



Exam : 070-214

**Title : Implementing and Administering Security
in a Microsoft Windows 2000 Network**

Ver : 11.01.2006

QUESTION 1:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain named Certkiller .com.

You have deployed a new Windows 2000 Server computer as a Web server in the perimeter network (also known as the DMZ). The Web server is not a member of Certkiller .com. A firewall between the network and the DMZ is configured to allow only HTTP traffic to be sent from the DMZ to the private network.

Your Web server administrator creates a security template named Webserver.inf that defines the default security settings required for the Web server. The security template settings must be enforced at the Web server and applied at regular intervals.

What should you do?

A. Make the Web server a member of the Certkiller .com domain and place the Web server computer account into a new organizational unit (OU).

Import the Webserver.inf security template to the Default Domain Policy.

B. Create a batch file that applies the security template by using the `secedit /configure /cfg Webserver.inf /db web.sdb` command.

In Scheduled Tasks, create a new task to run the batch file daily.

C. Apply the security template using the Security Configuration and Analysis console on the Web server.

Create a batch file that updates the security policy of the Web server by using the `secedit /refreshpolicy machine_policy /enforce` command.

In Scheduled Tasks, create a new task to run the batch file daily.

D. Import the Webserver.inf security template to the Local Computer policy of the Web server.

Create a batch file that updates the security policy of the Web server by using the `secedit /refreshpolicy machine_policy /enforce` command.

In Scheduled Tasks, create a new task to run the batch file daily.

Answer: C

Explanation:

We apply the security template using the Security Configuration and Analysis console. We then update the security policy at regular intervals using a scheduled task.

Incorrect Answers

A: We do not want to apply the Webserver.inf to all computers in the domain.

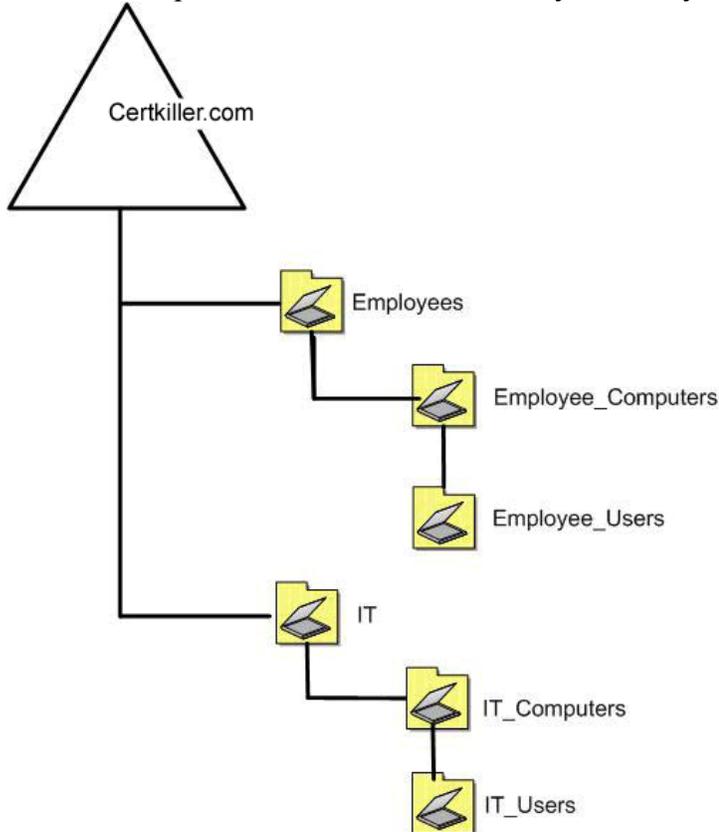
B: We do repeatedly have to apply the security template.

D: The initial template applied to a computer is called the Local Computer Policy. It is not a good practice to change this template.

QUESTION 2:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains two Windows 2000 domain

controllers and 500 Windows 2000 Professional computers.
The relevant portion of the Active Directory hierarchy is shown in the exhibit.



The user accounts for all administrators are located in the IT_Users organizational unit (OU). All other user accounts are located in the Employee_Users OU. The client computer accounts for the administrators' computers are located in the IT_Computers OU. All other client computer accounts are located in the Employee_Computers OU. Your company employs 10 security auditors to ensure that servers and client computers comply with the written security policy of Certkiller. You create a domain security group named Security_Audit. You add the computer accounts for each security auditor to this group.

You create several Group Policy objects (GPOs) and link them to the Employees OU. The GPOs configure security settings to enforce the written policy. The priority and configuration of each GPO are shown in the following table.

GPO name	Policy	Setting	Object with Read and Apply Group Policy Permissions	Priority	No Override
GPO1	Audit object access	Success and Failure	AuthenticateUsers Security_Audit	1	
GPO2	Audit logon	Failure	Security_Audit	2	

	events				
GPO3	Audit account logon events	Success	AuthenticateUsers Security_Audit	3	X

You discover that the Security logs on many client computers are full of successful object access events from the users of the client computers. You do not want users to be audited when they access files on their own computers. However, you want the security auditors to be audited when they access any file on any client computer. What should you do?

- A. Clear the No Override check box in GPO3.
- B. Remove the Authenticated Users group from the DACL for GPO1.
- C. Configure the policy settings for GPO3 so that success and failure events are audited.
- D. Configure the DACL for GPO1 so that the Authenticated Users group has Deny - Apply Group Policy permission.

Answer: B

Explanation:

By removing the Authenticated Users group from the DACL of GPO1, only members of the Security_Auditgroup would be audited for Object Access.

Incorrect Answers

A, C: GPO1 would still be applied, and object Access by the Authenticated Users group would still be audited.

D: The auditors, like all users, belong to the Authenticated Users group. They would also be receive Deny - Apply Group Policy permission, and they would not be audited contrary to the requirements in this scenario.

QUESTION 3:

You are the network administrator for Certkiller . The network consists if a Windows 2000 Active Directory domain. The domain contains five Windows 2000 Server domain controllers and 50 Windows NT Workstation 4.0 computers.

You perform a clean installation of Windows 2000 Professional on four client computers.

You do not install Internet Information Services (IIS) on these computers.

The written security policy for Certkiller allows Windows 2000 Professional users to install and run IIS. Every computer running IIS must be configured to meet the written policy before the computer can be connected to Certkiller network.

You want to ensure that the written policy for IIS is enforced automatically if IIS is installed on a Windows 2000 Professional computer.

What should you do before the user receive their computers?

- A. On each Windows 2000 Professional computer, modify the Ocfilesw.inf security template to comply with the written policy.
- B. On each Windows 2000 Professional computer, modify the Setup Security.inf security template to comply with the written policy.
- C. On a reference computer, configure IIS permissions to comply with the written policy. In the local Group Policy editor, select Import current Authenticode Security information. Select the Export Browser Settings option and save the settings to a file. Place the file in Systemroot\System32 on each Windows 2000 Professional computer.
- D. On a reference computer, configure IIS permissions to comply with the written policy. In the local Group Policy editor, select Import current security zones settings. Select the Export List option and save the list to a file. Place the file in Systemroot\System32 on each Windows 2000 Professional computer.

Answer: C

Explanation:

You can use Authenticode to designate software publishers and credentials agencies as trustworthy. You can also import these settings from your computer. If you want to modify the settings that you will apply to your users' computers, click Import current Authenticode security information, and then click Modify Settings.

Authenticode allows administrators to designate software publishers and credentials agencies as trustworthy. These settings can also be imported from the administrator's computer. Click Import current Authenticode information, and then click Modify Settings to modify the settings that will apply to users' computers.

Incorrect Answers

A: It would be a daunting administrative task to reconfigure each client computer manually. Furthermore, the OCFilesw.inf file defines Optional component file security for Professional.

B: It would be a daunting administrative task to reconfigure each client computer manually. Furthermore, the secure templates (secure*.inf) implement recommended security settings for all security areas except files, folders, and registry keys.

D: IIS security does not primarily concern accessing secure sites.

QUESTION 4:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 2,000 portable computers that run Windows XP Professional. All portable computers use Microsoft Internet Explorer as their only Web browser.

When you work from home, your portable computer automatically dials in to Certkiller network so that you can administer network resources remotely. The written security policy for Certkiller requires stricter security zone and privacy settings for all portable computers. You configure your portable computer to comply with the written policy. You create a Group Policy object (GPO) named SetSecurity and link it to the domain. You import the connection settings from your computer to the Security Zones and

Content Ratings policy in SetSecurity.

Now, when other users work from home, they report that their computers attempt to dial in to Certkiller network automatically. However, the connections fail because only administrators have dial-up permissions to Certkiller network.

You need to restore the dial-up configuration for other users to its previous state, while continuing to enforce the written security policy.

What should you do?

A. On your portable computer, open the Programs policy in the Internet Explorer maintenance section of the SetSecurity GPO, and select the option to import settings. Save the modified GPO.

B. On your portable computer, modify the Automatic Browser Configuration policy of the SetSecurity GPO so that automatic browser configuration is disabled. Save the modified GPO.

C. Delete, re-create, and then link the SetSecurity GPO to the domain by using a Windows XP Professional computer that has the same configuration as your portable computer.

D. Create a new user account in the domain.

Use the new account to log on to your portable computer.

Configure the settings to comply with the written policy, configure the dial-up configuration to not dial, and import those settings to the SetSecurity GPO.

Delete the new user account.

Answer: D

Explanation:

The administrator account was used when configuring the LapTop computers.

Administrators are allowed to connect remotely. We must therefore use a non-administrator user account when configuring the GPO that should be used on the LapTops.

Incorrect Answers

A: An incomplete solution.

B: The Automatic Browser Configuration policy is used to automatically push the updated security zone settings to each user's desktop computer, enabling the administrator to manage security policy dynamically across all computers on the network.

C: We need to configure the template with a NON admin account

QUESTION 5:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains domain controllers that run either Windows 2000 Sever or Windows NT Server 4.0.

You need to modify a registry entry on all domain controllers. You create an administrative template that contains the registry entry. You need to apply the template only to each domain controller every time it is restarted.

What must you do to achieve this goal? (Each correct answer presents part of the solution. Choose two)

A. Import the administrative template to the Default Domain Policy Group Policy object (GPO) and then configure the registry entry in the template.

B. Import the administrative template to the Default Domain Controllers Policy Group Policy object (GPO) and then configure the registry entry in the template.

C. Import the administrative template to the local Group Policy of the domain controller that runs the PDC Emulator and then configure the registry entry in the template.

D. Import the administrative template to a system policy, configure the template, and save it as a file named Ntconfig.pol.

Place the Ntconfig.pol file in the Policies folder under the Sysvol share.

Configure the Lbridge.cmd utility.

E. Import the administrative template a system policy, configure the template, and save it as a file named Ntconfig.pol.

Place the Ntconfig.pol file in the Netlogon share on the Windows NT 4.0 export server.

Configure the Lbridge.cmd script.

F. Import the administrative template to a system policy, configure the template, and save it as a file named Ntconfig.pol.

Place the Ntconfig.pol file in the Netlogon share on a Windows 2000 domain controller.

Configure the Lbridge.cmd script.

Answer: B, D

Explanation:

B: The Default Domain Controllers Policy Group Policy object (GPO) applied to all Windows 2000 Domain controllers. We use it to make the appropriate configuration.

D: The Windows NT system policy file, Ntconfig.pol, should be placed on the SYSVOL on a Windows 2000 Domain controller.

Note: A concern in a mixed environment is keeping the NETLOGON shares consistent. You have to remember to place a copy of Config.POL (for Windows 9x clients) and NTConfig.POL (for NT clients) in SYSVOL\SYSVOL\DomainName\Scripts folder which is shared as NETLOGON on Windows 2000 domain controllers. Windows NT LanMan Directory Replication can not be configured to replicate with Windows 2000 File Replication Service, so until you migrate completely to Windows 2000 with AD, you'll have to remember to keep *.POL files in both environments synchronized. You can use Microsoft provided LBridge.cmd script to copy the data from Windows 2000 Based DC to a Windows NT 4.0 BDC configured as an export server.

Reference:

HOW TO: Use Lbridge.cmd to Replicate System Policies Between Windows 2000 and Windows NT 4.0 Domain Controllers

Incorrect Answers

A: It should only be applied to domain controllers, not to every computer in the domain.

C: The PDC emulator cannot be helpful in replicating the configuration to the Windows NT domain controller.

- E: We must replicate the Ntconfig.pol file from a Windows 2000 Domain controller.
F: The Netlogon share on a Windows 2000 domain controller is not used for replication.
-

QUESTION 6:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 50 Windows NT Workstation 4.0 computers and 50 Windows 2000 Professional computers. Some Windows 2000 Professional computers run Internet Services (IIS) and host a Web site for the employees who use the computers.

You replace all Windows NT Workstation computers with new Windows 2000 Professional computers. You want to ensure that all client communication between all Windows 2000 computers is digitally signed. However, you want all client computers to be able to access the Web site on each Windows 2000 Professional computer.

You create a custom security template. You need to configure and apply the template to the appropriate client computers.

What two actions should you take? (Each correct answer presents part of the solution. Choose two)

- A. Apply the template to all Windows 2000 Professional computers.
- B. Apply the template only to Windows 2000 Professional computers not running IIS.
- C. Configure the template to enable the Digitally Sign Client Communication (always) policy.
- D. Configure the template to enable the Digitally Sign Server Communication (always) policy.
- E. Configure the template to enable the Digitally Sign Client Communication (when possible)policy.
- F. Configure the template to enable the Digitally Sign Server Communication (when possible)policy.

Answer: A, C

Explanation:

We want to implement the highest possible security !! therefor we apply the template to ALL clients pc's and we implement the Digitally Sign Client Communication (always) policy.

QUESTION 7:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 50 Windows NT Workstation 4.0 computers and 50 Windows 2000 Professional computers. You replace all Windows NT Workstation computers with Windows 2000 Professional computers.

You create an organizational unit (OU) named Workstations. You move all the Windows 2000 Professional computers into the Workstations OU. You create a Group Policy object (GPO) named Software_settings and link it to the Workstation OU.

You configure the Software_settings GPO to distribute an application that is not certified for Windows 2000. Users report that they cannot save preferred settings in the application, which uses the systemroot directory. However, this application functioned correctly when it was installed on Windows NT Workstation computers.

You want to ensure that users can save the preferred settings of the application. What should you do?

- A. Edit the Software_settings GPO and import the Defltwk.inf security template.
- B. Edit the Software_settings GPO and import the Compatws.inf security template.
- C. Edit the Software_settings GPO and enable the Disable legacy run list policy.
- D. Edit the Software_settings GPO and disable the Set Windows File Protection scanning policy.

Answer: B

Explanation:

By lowering the security levels on specific files, folders, and registry keys that are commonly accessed by applications, the compatible templates allow most applications to run successfully.

Incorrect Answers

A: Windows 2000 includes Security Configuration templates that contain the default settings for NTFS permissions, registry permissions, default user rights, and so on. Defltwk.inf is used on Windows 2000 Professional computers. By applying this security template to computers it ensure that they would receive the same security settings as the cleanly installed computers. However, the computers in this scenario are already cleanly installed, so there would be no change of security permission.

C: Enabling the Disable legacy run list would prevent listed legacy program from running.

D: The Set Windows File Protection scanning policy determines when Windows File Protection scans protected files. This policy directs Windows File Protection to enumerate and scan all system files for changes.

QUESTION 8:

You are the network administrator for Certkiller . The network contains 3,000 Windows NT Workstation 4.0 computers. All the computers run a custom software application that requires customized security settings. Each computer contains the correct security settings to run the application.

You upgrade one of the computers to Windows 2000 Professional by running Setup from a network distribution shared folder. The upgrade completes successfully, but the custom application will not run. You discover that the upgrade process overwrote the computer's customized security settings.

You need to ensure that future upgrades to Windows 2000 Professional will not overwrite the customized security settings.

What should you do?

- A. Apply the Compatws.inf security template to each computer after it is upgraded to Windows 2000 Professional.
- B. Configure a post-installation batch file that applies the Dwup.inf security template by running the secedit command.
- C. Modify the Dwup.inf security template in the Windows 2000 Professional distribution shared folder to include the customized security settings.
- D. Customize the security settings on the upgraded Windows 2000 Professional computer.
Use the Security Configuration and Analysis console to export the security settings to a security template named Upgrade.inf.
Place the template in the Windows 2000 Professional distribution shared folder.
- E. Modify the default Hisecws.inf security template to include the customized security settings.
Save the modified template in the Windows 2000 Professional distribution shared folder.

Answer: C

Explanation:

Windows 2000 uses the following security templates to apply security settings during the upgrade process:

1. Dwup.inf (for Windows 2000 Professional upgrades)
2. Dsup.inf (for Windows 2000 Server upgrades)

To prevent the upgrade process from modifying custom security settings, you can modify these text-based templates to ignore the specific folders, files, or registry keys that contain custom security settings. The modified Dwup.inf is saved in the Distribution folder and will be applied to all future upgrades.

Note: The Windows 2000 upgrade process applies Windows 2000 default security settings to registry keys and file system objects. This process overwrites any custom permissions that you previously defined. If the Windows 2000 default security settings are in conflict with custom permissions, programs that rely on the custom permissions may not work properly.

Reference:

HOW TO: Prevent Windows 2000 Upgrade from Modifying Custom Security, Microsoft Knowledge Base Article - Q260242

Incorrect Answers

- A: The Compatws.inf security template only makes Windows 2000 Professional computer compatible with the Windows NT 4.0 default security settings. However, in this scenario we must ensure that customized security settings are preserved.
- B: We must customize the Dwup.inf security template.
- D: The Upgrade.inf security template would not be applied to the upgraded computers.
- E: The modified Hisecws.inf security template would not be applied to the upgraded computers.

QUESTION 9:

You are the network administrator for Certkiller . The network consists of a Windows

2000 Active Directory domain. The network contains two Windows 2000 Server computers configured as domain controllers and 1,500 Windows 2000 Professional client computers.

Your manager wants you to ensure that your domain Account Policies are no less secure than the Account Policies of the Securedc.inf template. You run the Security Configuration and Analysis console on a network domain controller, and you use the Securedc.inf template to analyze the computer.

You review the Account Lockout Policy portion of the analysis. The relevant portion of the analysis is shown in the following table.

Policy	Database setting	Computer setting
Account lockout duration	30 minutes	0
Account lockout threshold	5 invalid logon attempts	3 invalid logon attempts
Reset account lockout counter after	30 minutes	20 minutes

Your manager does not want to weaken the existing security. You must increase the security of the Account Lockout Policy in all areas in which it is less restrictive than the Securedc.inf template.

What should you do?

- A. Import the Securedc.inf template into the Domain Security Policy.
- B. Import the Securedc.inf template into the Domain Controller Security Policy.
- C. Create a new security template with an Account lockout duration of 0 minutes, and Account lockout threshold of 3 invalid logon attempts, and a Reset account lockout counter after policy of 30 minutes.
Import the new template into the Domain Security Policy.
- D. Create a new security template with an Account lockout duration of 30, an Account lockout threshold of 3 invalid logon attempts, and a Reset account lockout counter policy of 30 minutes.
Import the new template into the Domain Controller Security Policy.

Answer: C

Explanation:

The Account lockout duration policy determines the number of minutes a locked out account remains locked out before automatically becoming unlocked. The range is 1 to 99999 minutes. You can specify that the account will be locked out until an administrator explicitly unlocks it by setting the value to 0.

The Account lockout threshold determines the number of failed logon attempts that will cause a user account to be locked out. A locked out account cannot be used until it is reset by an administrator or the account lockout duration has expired. You can set values

between 1 and 999 failed logon attempts, or you can specify that the account will never be locked out by setting the value to 0.

By default, this setting is disabled in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers.

The Reset account lockout counter after policy determines the number of minutes that must elapse after a failed logon attempt before the bad logon attempt counter is reset to 0 bad logons. The range is 1 to 99999 minutes.

By default, this policy is not defined, since it only has meaning when an Account lockout threshold is specified

When we merge two security templates, by importing the 2nd template, the 2nd imported template takes precedence when there is contention. As we want maximum security we need to create a custom security template which only strengthens security on all policies. Note: You can merge several different templates into one composite template, which can then be used for analysis or configuration of a system, by importing each template into a working database. The database merges the various templates to create one composite template, resolving conflicts in order of import; the last one imported takes precedence when there is contention.

The Best solution is this

Policy	Setting
Account lockout duration	0 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

Incorrect Answers

A, B: The Securedc.inf security template would take precedence when there is contention. It would allow 5 invalid login attempts, which would lower security.

D: We want an Account lockout duration of 0 (admin will unlock), not 30 minutes.

QUESTION 10:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain and includes 1, 000 Windows XP Professional client computers. All client computers are members of the domain. The domain accounts for all client computers are located in the organizational units (OUs) of the departments that own the computers. The domain also includes 100 Windows 2000 Server computers. The computer accounts for all servers are located in an OU named Servers.

All client computers are configured with a single hard disk. The hard disk is configured as two logical volumes named C and D. The C drive contains only the operating system files. The D drive contains all user data and application files. Both drives are formatted to use NTFS.

The written security policy for Certkiller requires custom NTFS permissions on the root of the D drive for all client computers. Previously, these permissions were

manually applied by an administrator before new computers were delivered to users. However, new computers are now being added at a rate of 100 or more per month. Computers ordered from the manufacturer contain different hardware. You want to ensure that new client computers can be automatically configured with the correct NTFS permissions for the root of drive D. However, you do not want your solution to affect any of the servers in the domain. What should you do?

- A. Create a Microsoft Visual Basic Scripting Edition (VBScript) script that assigns the correct NTFS permissions to the root of drive D.
Create a new Group Policy object (GPO) and link it to the domain.
Configure the GPO to run as a startup script.
- B. Create a startup script that runs the cacls.exe command to apply the correct NTFS permissions to the root of drive D.
Create a new Group Policy object (GPO) and link it to each departmental OU.
Configure the new GPO to run the startup script.
- C. Create a security template that assigns the correct NTFS permissions to the root of drive D.
Import the template into a Group Policy object (GPO) and link the GPO to each departmental OU.
- D. Create a security template that assigns the correct NTFS permissions to the root of Drive D.
Analyze the template, configure the correct NTFS permissions for the root of drive D, and save the security database.
Copy the security database to a folder named C:\Windows\Security on each new client computer.

Answer: C

Explanation:

We create a security template with the appropriate NTFS permissions, import the security template into a GPO, link to GPO to each departmental OU. This ensures that the computers will be configured with the correct NTFS permissions.

Incorrect Answers

- A: The startup script would run in the security context of the user, and it would not be allowed to apply these changes.
- B: The cacls.exe utility displays or modifies access control lists (ACLs) of files. However, the startup script would run in the security context of the user, and it would not be allowed to apply these changes.
- D: Moving the security database to the C:\Windows\Security directory would not accomplish much. We should use a GPO instead to apply the NTFS permissions.

QUESTION 11:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 10 Windows 2000 domain

controllers, 100 Windows 2000 Professional client computers, and 500 Windows NT Workstation 4.0 computers.

You create an organizational unit (OU) named Client_Comps. You move all the client computer accounts in the network to this OU. Then, you create a Group Policy object (GPO) named CK1 and link it to the Client_Comps OU. You import the Securews.inf security template to CK1 .

You install Windows 2000 Professional on all client computers. You verify that each client computer applies CK1 .

Users report that an application does not run on the Windows 2000 Professional computers. You discover that the application stores user data in the program files folder structure. This application used to run on the Windows NT Workstation 4.0 computers.

You need to ensure that the application can run on Windows 2000 Professional computers while maintaining the security settings in Securews.inf. You also need to maintain security on the other computers and domain controllers in the domain.

What should you do?

- A. Import the Compatws.inf security template to CK1 .
- B. Configure CK1 so that it applies only the settings from Defltwk.inf security template.
- C. Create a new GPO and link it to the domain.
Import the Defltwk.inf security template to the new GPO.
- D. Create a new security template that merges the Securews.inf template and the Compatws.inf template.
Import the new template to the Default Domain Policy GPO.

Answer: A

Explanation:

We should reduce the security constraints for the Windows 2000 Professional computers. We accomplish this by applying the Compatws.inf security template to CK1 . CK1 will be applied to all computers in the Client_Comps OU which is including all Windows 2000 Professional computers.

Incorrect Answers

B: We still must apply the Securews.inf security template.

C: We do not want the Defltwk.inf security template applied to all computers in the domain, just to the Windows 2000 Professional computers.

D: We do not want to apply the merged security template to all computers in the domain, only the Windows 2000 Professional computers.

QUESTION 12:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 10 Windows 2000 domain controllers, 400 Windows 2000 Professional computers, and 400 Windows 98 computers.

You create an organizational unit (OU) named Client_Comps. You move all

Windows 2000 client computer accounts to this OU. You create a Group Policy object (GPO) named GPO1 and link it to the Client_Comps OU. You import the Securews.inf security template to GPO1.

The Windows 98 computers contain security settings by means of a system policy. You upgrade the Windows 98 computer to Windows 2000 Professional. You place the computer account for each upgraded client computer in the Client_Comps OU. You discover that some security settings that were applied from the system policy are still applied to the upgraded client computers. These security settings are creating problems for users.

You try to reconfigure these security settings by using GPO1, but the options are not available. You need to reconfigure the security settings on the upgraded client computers.

What should you do?

- A. Import the Compatws.inf security template to GPO1.
- B. Run the Security Configuration and Analysis tool on each of the upgraded client computers.
Analyze and configure the computers by using the Securews.inf template.
- C. Run the `secedit /refreshpolicy machine_policy` command on all the upgraded client computers.
- D. Create a custom administrative template that reconfigures the security settings and add it to GPO1.

Answer: D

Explanation:

We should make a custom administrative template to reconfigure the upgraded security settings. We should then add it to GPO1.

Incorrect Answers

A: Importing Compatws.inf into the GPO would have a negative impact on the security configuration. We cannot allow it.

B: As we are unable to apply the Securews.inf security template through the GPO we could explicitly apply it through the Security Configuration and Analysis tool. This would be a heavy administrative burden however, we would have to perform this task on every upgraded PC.

C: The problem is not that GPO1 is not applied. The problem is that some old system policies are still in use.

QUESTION 13:

You are the network administrator Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains five Windows 2000 Server domain controllers, one Windows NT Server 4.0 BDC, 50 Windows NT Workstation 4.0 computers, and 50 Windows 2000 Professional computers. The network also contains 50 Windows 98 computers.

You upgrade the BDC to Windows 2000 Server and configure it as a member

server. You perform a clean installation of Windows 2000 Server on nine new computers and configure them as member servers.

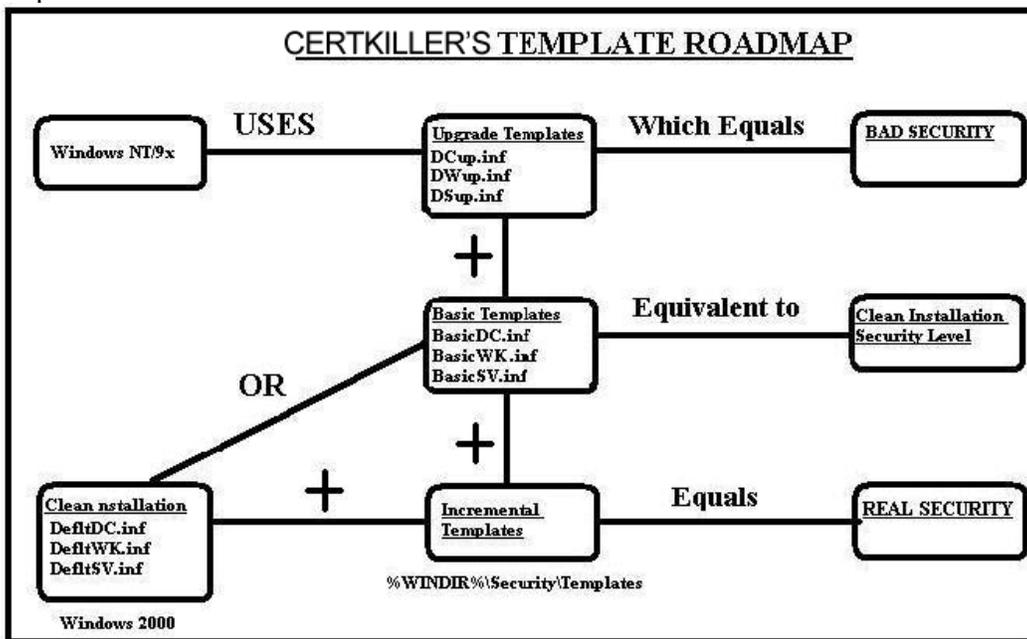
You want to ensure that the upgraded computer and the newly installed computers have the same security settings.

How should you configure the upgraded computer?

- A. Apply the Dcup.inf security template.
- B. Apply the Basicsv.inf security template.
- C. Analyze one of the cleanly installed Windows 2000 Server computers against the Dcup.inf security template.
Copy the resulting security database to the windir\security\templates folder of the upgraded computer.
- D. Analyze one of the cleanly installed Windows 2000 Server computers against the Basicsv.inf security template.
Copy the resulting security database to the windir\security\templates folder of the upgraded computer.

Answer: B

Explanation:



The default security templates (defltwk.inf, defltsv.inf, defltdc.inf) are not applied to computers that have been upgraded to Windows 2000 from earlier versions of Windows NT. To provide security settings that are equivalent to those of a clean installation of Windows 2000, you can use basic security templates. You can also use the basic security templates (basicwk.inf, basicsv.inf, basicdc.inf) to reapply default security settings. In upgraded machines, the default Windows 2000 permissions for file system, registry and service objects are also applied to upgraded machines using the following files: dwup.inf, dsup.inf, and dcup.inf (Windows NT 4.0 Domain Controller Upgrade Only), So this means that when upgrading, an additional INF file is used, Dcup.inf is used to

define Windows 2000-specific settings during the upgrade of a Windows NT 4.0-based domain controller.

Now to get to the same security level as the cleanly installed computers we need to apply the basicsv template. We can do this because the upgraded computer will be a member server.

Incorrect Answers

A: The Dcup.inf security template is already applied automatically during the upgrade process.

C,D: Copying the security database (*.sdb) to the %windir\Security\Templates Directory will do nothing. The file will not be used.

QUESTION 14:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 50 Windows NT Workstation 4.0 computers and 50 Windows 2000 Professional computers.

You create an organizational unit (OU) named Desktops. You upgrade 25 of the Windows NT Workstation computers to Windows 2000 Professional. On the remaining 25 Windows NT Workstation computers, you perform a clean installation of Windows 2000 Professional.

You place the computer accounts for all upgraded and newly installed Windows 2000 Professional computers in the Desktop OU. You customize the security on each Windows 2000 Professional computer by adding several domain security groups to the local Administrators group.

You want to ensure that the upgraded computers and the newly installed computers have the same security settings. You also want to maintain the customized security settings.

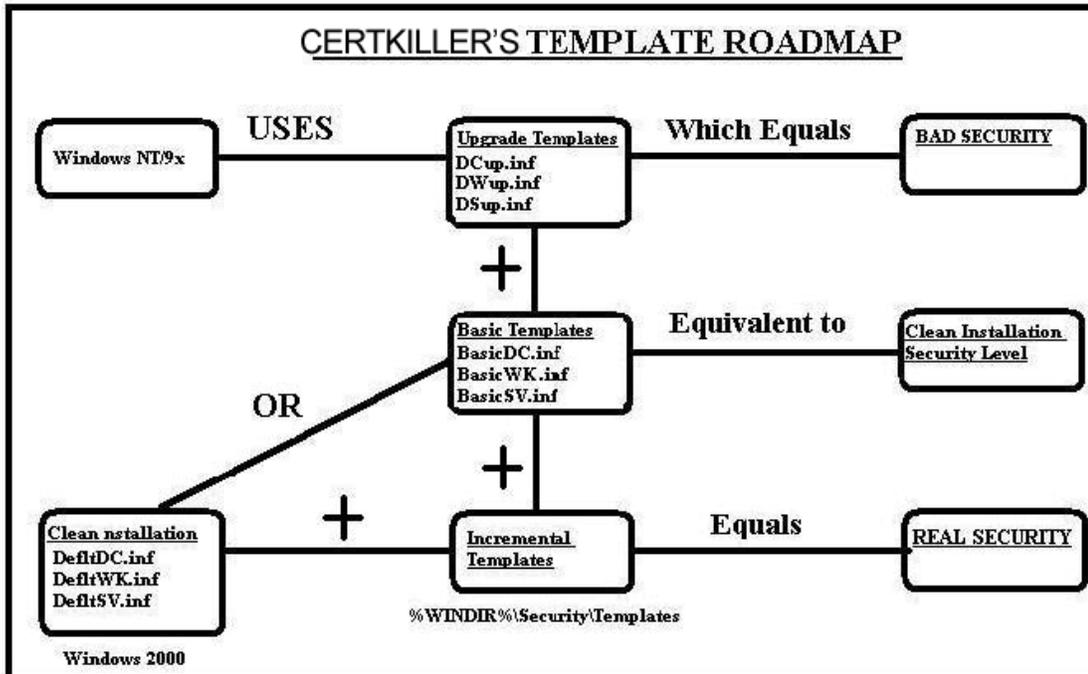
How should you configure each upgraded computer?

- A. Apply the Defltwk.inf security template.
- B. Apply the Basicwk.inf security template.
- C. Run the secedit /validate Basicwk.inf command.
- D. Run the secedit /validate Defltwk.inf command.

Answer: B

Explanation:

Windows 2000 includes Security Configuration templates that contain the default settings for NTFS permissions, registry permissions, default user rights, and so on.



Defltwk.inf

The default security setting of Windows 2000-based computers provides a significant increase in security over previous versions of Microsoft Windows NT(r). The settings are applied by using predefined default security templates. These templates provide a secure system from the outset. No additional configuration is required after installation.

Windows 2000 default security settings are applied only to Windows 2000 systems that have a clean installation to an NTFS file system partition. The security template used on a Windows 2000-based computer depends on the type of Windows 2000 installation selected. The template will vary based on whether the Windows 2000-based computer is running Windows 2000 Professional, running Windows 2000 Server, or functioning as a domain controller.

Default Security Templates Applied to All New Windows 2000 Installations Except:

- * Upgrades from Windows NT 4.0
- * FAT File System-only Computers

Basicwk.inf

To provide security settings that are equivalent to those of a clean installation of Windows 2000, you can use basic security templates. You can also use the basic security templates to reapply default security settings. These basic security templates specify default Windows 2000 security settings for all security areas with the exception of User Rights and Groups. These security settings ensure that existing group memberships and defined user rights are not modified.

The question states that we need to reconfigure the upgraded computers and we should not replace the group membership, so we need to apply basicwk.inf

Reference:

Moc - Windows 2000 Network Security Design (70-220) (Course 2150a) Page 5-11

Incorrect Answers

A: We need to reconfigure workstations that were upgraded from NT4 to windows 2000

so we need basicws.inf.

C, D: The secedit /validate command validates the syntax of a security template you want to import into a database for analysis or application to a system. However, it does not apply the security template.

QUESTION 15:

You are the network administrator for Certkiller . All servers and client computers on the network are running Windows 2000. A Windows 2000 Server computer named Mainfiles hosts two network printers: AllPrint and ATPrint.

All required audit policies are enabled. AllPrint uses a print device on LPT1. AllPrint allows the Everyone group Print permissions. More than 100 users successfully send print jobs to AllPrint daily. ATPrint uses a print device on LPT2. Both printers on Mainfiles use the default print queue location.

Your manager wants to minimize the number of users who print to ATPrint. In preparation for this action, your manager wants a list of the people who print documents on ATPrint over the next two days. Your manager does not want the list to include users who also print to AllPrint. You want to generate this list with the least amount of administrative effort.

What should you do?

- A. Configure the SACL on ATPrint to record the success of Print and Read Permissions for the Everyone group.
- B. Configure the SACL on ATPrint to record the failure of Print and Read Permissions for the Print Operators global group.
- C. Configure the SACL on the printer queue directory of Mainfiles to record the success of Read Permissions for the Everyone group.
- D. Configure the SACL on the printer queue directory file on Mainfiles to record the failure of Read Permissions for the Print Operators global group.

Answer: A

Explanation:

Auditing can be enabled for all objects in a Windows 2000-based network with a system access control list (SACL). A SACL contains a list of users and groups for which actions on the object are to be audited. Almost any object that a user can manipulate in Windows 2000 has a SACL. This includes files and folders on NTFS file system drives, printers and registry keys. A SACL is comprised of access control entries (ACEs). Each ACE contains three pieces of information:

- * The security principal to be audited.
- * The specific access types to be audited, called an access mask.
- * A flag to indicate whether to audit failed access, successful access, or both.

If you want events to appear in the security log, you must first enable Auditing for Object Access and then define the SACL for each object you wish to audit.

We want to audit ATPrint for the everyone group.

Reference:

<http://www.microsoft.com/technet/security/prodtech/win2000/secwin2k/09detect.msp>

Incorrect Answers

B: We want to audit successful print jobs, not failed ones.

C, D: The print queue does not have to be audited.

QUESTION 16:

You are the network administrator for Certkiller . The network contains a Windows 2000 Server named Certkiller 1. Certkiller 1 is configured only as a file server.

During a security audit on Certkiller 1, you discover that the Security log contains the following event:

Source: Security

Category: Account Management

Type: Success

Event ID: 627

User: NT AUTHORITY\SYSTEM

Description: Change Password Attempt:

Target Account Name: TsInternetUser

Target Domain: Certkiller

Target Account ID: Certkiller 1\
TsInternetUser

Caller User Name: Certkiller 1\$

Caller Domain: Certkiller

Caller Logon ID: (0x0, 0x3E7)

Privileges:

This event repeats every day. The written security policy for Certkiller prohibits the use of local user accounts on company file servers.

You need to ensure that Certkiller 1 complies with the written policy.

What should you do?

- A. Uninstall Terminal Services Licensing from Certkiller 1.
- B. Disable auditing of successful security events on Certkiller 1.
- C. Reset the password for the Certkiller 1\TsInternetUser user account.
- D. Remove all user accounts except the Administrator account from the local Users group on Certkiller 1.
- E. Configure the TsInternetUser account so that the user cannot change the account password.

Answer: D

Explanation:

The modification of a password by someone other than the user can indicate that an account has been taken over by another user. Look for Event IDs 627 and 628 which indicate that a password change is attempted and is successful. Review the details to determine whether a different account performed the change, and whether the account is a member of the help desk or other service team that resets user account passwords.

Reference:

<http://www.microsoft.com/technet/security/prodtech/win2000/secwin2k/09detect.msp>

QUESTION 17:

You are the administrator of a Windows 2000 network at Certkiller Inc. The network consists of a Windows 2000 forest with 12 domains. The domains contain Windows NT Workstation 4.0 client computers, Windows 2000 Professional client computers, and Windows 2000 Server computers. All domain controllers are Windows 2000 based. Users report that on the Windows logon screen of the Windows NT Workstation 4.0 client computers, only two or three names are listed in the domain drop-down list. If their user domain name is not listed, they cannot log on to their domain on these client computers. On the Windows 2000 Professional client computers, all 12 domains are listed in the domain drop-down list.

You want to ensure that users from all 12 domains can log on to their domain on all of the Windows NT Workstation 4.0 client computers.

What should you do?

- A. Configure a User Principal Name (UPN) for all user accounts in the domains.
- B. Reset the machine account passwords of all the Windows NT Workstation 4.0 client computers.
- C. Disable the use of LAN Manager (LM) authentication on all the Windows NT Workstation 4.0 client computers.
- D. Switch all domains from Windows 2000 mixed mode to Windows 2000 native mode.

Answer: A

Explanation:

Some of the domain names might not be compatible with the down-level Windows NT 4.0 naming convention. We should configure a User Principal Name (UPN) for all user accounts in the domains. . " If the user logs on with his or her User Principal Name (UPN), the down-level name defined in Active Directory for that account is used.

Note: When a user logs on to a Windows 2000-based computer, the name of the folder that is created is derived from the user ID, and if necessary, suffixed with the name of the local computer or domain, whichever is applicable to the user logging on. For example, if the down-level name is "MYDOMAIN\joesmith," the user ID is "joesmith." If the user logs on with his or her User Principal Name (UPN), the down-level name defined in Active Directory for that account is used.

Reference:

User Profile Storage in Windows 2000, Microsoft Knowledge Base Article - Q228445

Incorrect Answers

- B: The is not an account policy problem.
- C: This is not a authentication problem.
- D: There is no need to switch to native mode-

QUESTION 18:

You are the administrator of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Professional client computers and Windows 2000 Server computers. The domain has five Windows 2000 domain controllers. All computers are in the same site.

A user named Jack reports that he receives an access-denied error message when he attempts to connect from his Windows 2000 Professional client computer to a share named Budget on a Windows 2000 Server computer named Certkiller 1. She can successfully connect to other shares on Certkiller 1.

Only the Managers group is allowed to connect to the Budget share on Certkiller 1. You immediately discover that Jack should be a member of the Managers group but she is not. You add Jack's user account to the Managers group and wait 15 minutes.

You want to ensure that Jack can successfully connect to the Budget share on Certkiller 1. What should you do?

- A. Instruct Jack to log off and log on to her Windows 2000 Professional computer again.
- B. On Certkiller 1, run the net use command to delete all connections to Jack's computer.
- C. On Certkiller 1, use the Computer Management console to disconnect all sessions that are connected from Jack's computer.
- D. Use the Active Directory Sites and Services console to force replication on the five domain controllers.

Answer: A

Explanation:

To ensure that the membership of the Managers apply Jack should log off and log on again. Then she will get a new security token that allows her to access the share.

QUESTION 19:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 domain controllers, Windows 2000 Professional computers, and Windows XP Professional computers.

You need to administer Group Policy objects (GPOs) for Certkiller network from a Windows XP Professional computer. On this computer, you install Adminpak.msi and then create a GPO named CK1 . You link CK1 to the domain. In the security settings section of CK1 , you configure multiple polices and document all settings.

Another administrator named Jack needs to administer the GPOs for Certkiller network from a Windows 2000 Professional computer. When she opens CK1 , she cannot see all of the security settings that you documented.

Jack needs to be able to administer the GPOs and see all security settings.

What should you do?

- A. Add Jack's user account to the Group Policy Creator Owners group.
- B. Instruct Jack to administer the GPOs from a Windows XP Professional computer.

C. Instruct Jack to administer the GPOs from the domain controller that contains the PDC Emulator.

D. Copy the Windows XP administrative template to the Templates folder on Jack's Windows 2000 Professional computer.

Answer: A

Explanation:

Jack needs more permissions to enable her to edit the GPO. Specifically, her user account needs to be a member of the Group Policy Creator Owners group.

Reference:

Organizational Unit Controller Cannot Edit Group Policy Objects, Microsoft Knowledge Base Article - Q233548

How to Install the Remote Server Administration Tools in Windows 2000, Microsoft Knowledge Base Article - Q216999

Incorrect Answers

B: There is no specific advantage regarding remote registry administration of using a Windows XP Professional computer compared to a Windows 2000 Professional for

C: Jack would still not be able to edit the GPO. Her user account does not have the proper permissions.

D: It is not necessary to copy administrative templates.

QUESTION 20:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain named Certkiller .msft.

The IT manager for the sales department wants to enforce a minimum password length of eight characters. The IT managers for the remaining departments agree that they want a minimum password length of six characters.

The network currently enforces a six-character minimum password length. You must develop a solution that enforces the required eight character minimum password settings for sales department users domain accounts.

What should you do?

A. Create an organizational unit (OU) named Sales and move sales department user accounts into the new OU.

Create a Group Policy object (GPO) and link it to the Sales OU.

Configure the GPO to enforce the eight-character minimum password length.

B. Create an organizational unit (OU) named Sales and move sales department computer accounts into the new OU.

Create a Group Policy object (GPO) and link it to the Sales OU.

Configure the GPO to enforce the eight-character minimum password length.

C. Create a new child domain named sales. Certkiller .msft and move all sales department user accounts to the sales. Certkiller .msft domain.

Configure the Default Domain Policy in the sales. Certkiller .msft domain to enforce an eight-character password.

D. Create a new child domain named sales. Certkiller .msft and move all sales department computer accounts to the sales. Certkiller .msft domain.
Configure the Default Domain Controllers Policy in the sales. Certkiller .msft domain to enforce an eight-character password.

Answer: C

Explanation:

Account policies can only be applied at domain level: the Default Domain Policy. If we want two different account policies we need two domains.

Incorrect Answers

A, B: Account policies should only be used at Domain level, not at OU level.

D: We should apply the account policy to the Default Domain Policy, not the Default Domain Controllers Policy.

QUESTION 21:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The network contains two Windows 2000 Server computers configured as domain controllers and 1,500 Windows 2000 Professional client computers.

Certkiller has three departments: research, sales, and operations. Each department has a separate organizational unit (OU) in the domain that contains all user and group accounts for that department.

The written security policy for Certkiller concerning the Account Lockout Policy specifies that users entering an invalid password more than three times in 24 hours must be locked out until the administrator unlocks their accounts.

A user from the Research OU reports that he accidentally locked out his domain account before he went on a week long vacation, but now he can log on using his domain account. You learn that no administrator unlocked his account.

You review the Account Lockout Policy portion of the security template for the organization. The relevant settings of the security template are shown in the following table.

Policy	Computer settings
Account lockout duration	1,440 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	1,440 minutes

You must ensure that the Account Lockout Policy complies with the written policy. What should you do?

A. Set the Account lockout duration policy on the security template to 0 minutes. Import the template to the Domain Security Policy.

B. Configure the Account lockout duration policy on the security templates as Not defined.

Import the template to the Domain Security Policy.

C. Create a new Group Policy object (GPO) and link it to the Research OU.

Set the Reset account lockout counter after policy on the security template to 0 minutes.

Import the template to the new GPO.

D. Create a new Group Policy object (GPO) and link it to the Research OU.

Configure the Reset account lockout counter after policy on the security templates as Not defined.

Import the template to the new GPO.

Answer: A

Explanation:

The Account lockout duration policy determines the number of minutes a locked out account remains locked out before automatically becoming unlocked. The range is 1 to 99999 minutes. You can specify that the account will be locked out until an administrator explicitly unlocks it by setting the value to 0.

The Account lockout threshold determines the number of failed logon attempts that will cause a user account to be locked out. A locked out account cannot be used until it is reset by an administrator or the account lockout duration has expired. You can set values between 1 and 999 failed logon attempts, or you can specify that the account will never be locked out by setting the value to 0.

By default, this setting is disabled in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers.

The Reset account lockout counter after policy determines the number of minutes that must elapse after a failed logon attempt before the bad logon attempt counter is reset to 0 bad logons. The range is 1 to 99999 minutes.

By default, this policy is not defined, since it only has meaning when an Account lockout threshold is specified.

So the correct Settings should be:

Account lockout duration	0
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	1,440 minutes

Reference:

Microsoft Account Lockout Whitepaper & Windows 2000 Server Resource Kit

QUESTION 22:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain includes two organizational units (OU) named Manufacturing and Sales. The network contains two Windows 2000 Server computers configured as domain controllers and 1,500 Windows 2000 Professional client

computers. All user accounts are located in the Manufacturing OU and Sales OU. Your manager wants you to ensure that the domain Account Policies are no less secure than the Account Policies in the Securedc.inf template. You run the Security Configuration and Analysis console on a network domain controller, and you use Securedc.inf to analyze the computer.

You review the Password Policy portion of the analysis, which the following table shows.

Policy	Database setting	Computer setting
Enforce Password history	24 passwords remembered	1 password remembered
Maximum password age	42 days	0
Minimum password age	2 days	4 days
Minimum password length	8 characters	8 characters
Password must meet complexity requirements	Enables	Enabled
Store password using reversible encryption	Disabled	Enabled

Your manager does not want to reduce the existing security level. You must increase the security of the Password Policy in all areas in which it is less restrictive than the Securedc.inf template.

What should you do?

- A. Import Securedc.inf template into the Domain Security Policy.
- B. Create a new Group Policy object (GPO) and link it to the Sales and Manufacturing OUs.
Import the Securedc.inf template into the new GPO.
- C. Create a new security template.
Set Enforce password history to 24 passwords, Maximum password age to 42 days, and Minimum password age to 4 days.
Import the new template to the Domain Security Policy.
- D. Create a new Group Policy object (GPO) and link it to the Sales and Manufacturing OUs.
Create a new security template.
Set Enforce password history to 24 passwords, Maximum password age to 0, and Minimum password age to 4 days.
Import the new template to the new GPO.

Answer: C

Explanation:

We must create a new security template that is at least restrictive as the current settings. This ensures that security only improves and not decreases.

Incorrect Answers

A: When merging security templates the last one imported, Securedc.inf, takes precedence when there is contention. Importing the Securedc.inf security templates would therefore decrease Minimum password age and disable Store password using reversible encryption. This is not acceptable.

B, D: Windows 2000 only allows one domain account policy: the account policy applied to the root domain of the domain tree.

QUESTION 23:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain that has three domain controllers. All computer accounts are in the Computers container. The network has 900 Windows 2000 Professional client computers.

The written security policy requires that logons from domain accounts be audited. The Domain Controller Security Policy audit settings are in their default state. You do not want to audit logon attempts that use local user accounts on client computers or member servers.

You need to configure audit settings to comply with the written security policy.

What should you do?

- A. Run the secedit command to apply the Defaultdc.inf template to the domain controllers.
- B. Run the secedit command to apply the Basicdc.inf template to the domain controllers.
- C. Configure the Audit logon events policy for success and failure in the Local Security Policy of each domain controller.
- D. Configure the Audit account logon eventspolicy for success and failure in the Domain Controller Security Policy.

Answer: D

Explanation:

Audit logon events - Determines whether to audit each instance of a user logging on, logging off, or making a network connection to this computer.

If you are auditing successful Audit account logon events on a domain controller, then workstation logons do not generate logon audits. Only interactive and network logons to the domain controller itself generate logon events. In short, "account logon events" are generated where the account lives. "Logon events" are generated where the logon occurs.

Audit account logon events - Determines whether to audit each instance of a user logging on or logging off of another computer where this computer was used to validate the account.

Reference :

Windows 2000 Resource Kit Group Policy Help

Incorrect Answers:

A,B: The Defaultdc.inf and Basicdc.inf do nothing with auditing

C: Audit logon events Determines whether to audit each instance of a user logging on, logging off, or making a network connection to this computer.

QUESTION 24:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

Certkiller runs a distributed database application on five Windows 2000 member servers. The five database servers, together with other Windows 2000 Server computers, are in an organizational unit (OU) named Servers. The servers located in the Servers OU must not be moved to other OUs

You want to track when any of the five database servers is shut down or restarted. You create a new Group Policy object (GPO) named Uptime and link it to the Servers OU. You need to configure the Uptime GPO to allow the five database servers to track when they are shut down or restarted.

What should you do?

- A. Configure the Uptime GPO to grant the Profile system performance right to the five database servers.
- B. Configure the Uptime GPO to grant the Generate security audits right to the five database servers.
- C. Configure the Uptime GPO to enable the Audit access of global system objects policy. Configure the permissions of the GPO to apply only the five database servers.
- D. Configure the Uptime GPO to enable the Audit system events policy. Configure the permissions of the GPO to apply only to the five database servers.

Answer: D

Explanation:

By configuring the Uptime GPO to enable the Audit system events policy and configuring the permissions of the GPO to apply only to the five database servers, we can allow the five database servers to monitored when they are shut down or restarted.

QUESTION 25:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

The written security policy for Certkiller requires that passwords of domain user accounts must be changed every 30 days. You configure a password expiration of 30 days. You also configure a warning message to appear, prompting the user to change the password seven days before it expires.

You want to track when users change their domain passwords.

What should you do?

- A. In the Default Domain Policy Group Policy object (GPO), grant the Domain Users group the Generate security audits user right.
- B. In the Default Domain Policy Group Policy object (GPO), grant the Domain Users group the Audit the access of global system objects user right.
- C. In the Default Domain Controllers Policy Group Policy object (GPO), enable the Audit account management policy to log successful events.
- D. In the Default Domain Controllers Policy Group Policy object (GPO), enable the Audit logon events and the Audit account logon events policies to log successful events.
- E. In the Default Domain Controllers Policy Group Policy object (GPO), enable the Audit privilege use policy to log successful events.

Answer: C

Explanation:

Audit account management determines whether to audit each event of account management on a computer. Examples of account management events include:

- * A user account or group is created, changed, or deleted
- * A user account is renamed, disabled, or enabled
- * A password is set or changed

>

In this situation we want to track when users change their password.

QUESTION 26:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

You want to track all events of users logging on to and logging off the network in the event logs on the Windows 2000 domain controllers. All users use their domain user account to log on to the network from Windows 2000 Professional client computers in the domain.

In the Default Domain Controllers Policy Group Policy object (GPO), you enable the Audit logon events policy to log successful events. Two weeks later, you notice that no logon events appear in the event logs on the Windows 2000 domain controllers. The logon events are also not listed in the event logs on the Windows 2000 Professional client computers.

You want to ensure that all logon and logoff events are recorded in the event logs on Windows 2000 domain controllers.

What should you do?

- A. In the Default Domain Policy GPO, enable the Audit account management policy to log successful events.
- B. In the Default Domain Policy GPO, enable the Audit account logon events policy to log successful events.

C. In the Default Domain Controllers Policy GPO, enable the Audit account logon events policy to log successful events.

D. In the Default Domain Controllers Policy GPO, enable the Enforce password history policy.

Answer: C

Explanation:

We need to enable the Audit account logon events policy to log successful events for the Default Domain Controllers Policy GPO.

Incorrect Answers

A: Audit account management - Determines whether to audit each event of account management on a computer. Examples of account management events include:

- * A user account or group is created, changed, or deleted

- * A user account is renamed, disabled, or enabled

- * A password is set or changed

B: Audit account logon events - Determines whether to audit each instance of a user logging on or logging off of another computer where this computer was used to validate the account.

For domain controllers, this policy is defined in the Default Domain Controllers Group Policy object (GPO). The default setting is No auditing.

We want to monitor logon attempts on the domain (the domain controllers), not on the local workstations.

D: Enforce password history - Determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords.

By default, this setting is defined in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers with a value of 1.

QUESTION 27:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 50 Windows 2000 Server computers. One of these computers is named Certkiller 1 and is managed by Certkiller research department. Certkiller 1 is the only computer in the Research organizational unit (OU).

The research department employs a new user, Mr Bill, to administer Certkiller 1. Bill's domain user account is a member of the local Administrators group on Certkiller 1.

An employee in the research department reports that the files are being deleted from Certkiller 1. The employee suspects that a new software application being tested on Certkiller 1 might be deleting the files. The software application runs as a service by using a dedicated domain user account. The manager of the research department suspects that Bill might be deleting files accidentally.

You need to enable auditing to discover how the files are being deleted. You need to ensure that the auditing has no impact on other company computers.

What should you do first?

- A. Log on to Certkiller 1 as a member of the Domain Admins group and enable auditing of object access.
- B. Create a Group Policy object (GPO) and link it to the domain. Configure the GPO to enable auditing if object access.
- C. Create a Group Policy object (GPO) and link it to the Research OU. Configure the GPO to enable auditing of object access. Configure auditing of successful file deletions on Certkiller 1.
- D. Log on to Certkiller 1 by using the local Administrator account. Enable auditing of object access and use of privilege auditing.

Answer: C

Explanation:

We must enable auditing and specify which event or events we want to audit (successful file deletions).

Incorrect Answers

A, D: We must specify the kind of object access we want to audit. In this scenario we want to audit successful file deletions.

B: We only want to enable auditing on Certkiller 1 not to all computers in the domain.

QUESTION 28:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The network also contains 1,500 Windows 2000 Professional client computers.

The written security policy for Certkiller requires that failed domain logon attempts be tracked. You enable failure auditing on the Audit logon events setting in the Domain Controller Security Policy. You then use the Terminal Services client to connect to Certkiller 1 to verify that an incorrect user name or password results in a logged event. You attempt to log on from one of the client computers by using several incorrect user names and passwords. You examine the Security log on Certkiller 1 and find that no new events appear in the log.

You must ensure that the written policy regarding logon attempts is enforced.

What should you do?

- A. Enable Failure auditing for the Audit object access policy in the Domain Security Policy.
- B. Enable Failure auditing for the Audit account logon events policy in the Domain Controller Security Policy.
- C. Enable Failure auditing fir the Audit directory service access policy in the Domain Controller Security Policy.
- D. Enable Failure auditing for the Audit process tracking policy in the Domain Security Policy.

Answer: B

Explanation:

The Audit account logon events category captures authentication events in centralized locations on the domain controllers, while the Audit logon events audit category is used to track local logon events on your server or workstation.

QUESTION 29:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. Files are being deleted from several domain file servers. You enable auditing on the servers.

The audit logs indicate that the files are being deleted by a domain account named XPSFCEC from a Windows XP Professional computer named CK1 . Usually, the XPSFCEC user account is used by several company applications that run as services. However, written security policies for Certkiller do not allow XPSFCEC to be used on client computers.

You verify that the user of CK1 logs on by using a domain user account other than XPSFCEC. You examine the Security log on CK1 and find the XPSFCEC account referenced in the following event.

```
Event Type: Success Audit
Event Source: Security
Event Category: Detailed Tracking
Event ID: 600
Date: 07/14/2002
Time: 05:13:02
User: NT AUTHORITY\SYSTEM
Computer: CK1
Description:
  A process was assigned a primary token.
  Process ID: 2064
  Image File Name: C:\test\ Certkiller.exe
  User Name: XPSFCEC
  Domain: Certkiller.com
  Logon ID: (0x0, 0x1CBC6A)
```

You need to ensure that the XPSFCEC user account will no longer be used by software running on CK1 .

You need to ensure that Certkiller applications using the XPSFCEC account continue to operate.

What should you do?

- A. Disable the XPSFCEC user account.
- B. Change the password used by the XPSFCEC user account.
- C. On CK1 , configure Certkiller .exe to log on by using a user account other than XPSFCEC.
- D. Assign the Full Control - Denypermission to the XPSFCEC account for all files on each file server.
- E. Modify the Default Domain Policy Group Policy object (GPO) so that the XPSFCEC account does not have permission to create process tokens.

Answer: E

Explanation:

According to the exhibit a process was started on CK1. The user name XPSFCEC was used to start this process. We should prevent this account from creating process tokens.

Create a token object - Determines which accounts can be used by processes to create a token which can then be used to get access to any local resources when the process uses NtCreateToken() or other token-creation APIs.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

It is recommended that processes requiring this privilege use the LocalSystem account, which already includes this privilege, rather than using a separate user account with this privilege specially assigned.

Incorrect Answers

A: We cannot disable the XPSFCEC user account as it is still going to be used by applications.

B: Changing the password of XPSFCEC would require reconfiguration of any application that uses this service.

C: This would only prevent the problem for one particular application.

D: This prevents the deletion of files on the file servers. However, the XPSFCEC user account can still be used by software running on CK1.

QUESTION 30:

You are the network administrator for Certkiller. The network consists of a Windows 2000 Active Directory domain. The domain includes two Windows 2000 Server computers running as domain controllers, five Windows 2000 Server computers running as file servers, and 500 Windows 2000 Professional client computers.

All the domain controllers are in the Domain_Computers organizational unit (OU). The file servers are in an OU named Servers. The client computers are in an OU named Clients. The Domain_Computers OU is the parent OU to both the Servers OU and the Clients OU.

The written security policy for Certkiller requires that you track attempts to log on to a computer that use a local user account.

What should you do?

A. Create a security template that enables the Audit Account Logon Events policy for successful and failed attempts.

Create a Group Policy object (GPO) and link it to the domain.

Import the template into the new GPO.

B. Create a security template that enables the Audit Account Logon Events policy for successful and failed attempts.

Create a Group Policy object (GPO) and link it to the Servers OU.

Import the template into the new GPO.

C. Create a security template that enables the Audit Logon Events policy for successful

and failed attempts.

Create a Group Policy object (GPO) and link it to the Clients OU.

Import the template into the new GPO.

D. Create a security template that enables the Audit Logon Events policy for successful and failed attempts.

Create a Group Policy object (GPO) and link it to the Domain_Computers OU.

Import the template to the new GPO.

Answer: D

Explanation:

A Logon event occurs when a user logged on or logged off, or a user made or canceled a network connection to the computer. This includes attempts to log on a computer with a local user account. By linking the appropriately configured GPO to the Domain_Computers OU, it will be applied to both child OUs; the Server OU and the Clients OU. This ensures that all logon attempts on computers with local accounts are audited.

Reference:

HOW TO: Monitor for Unauthorized User Access in Windows 2000, Microsoft Knowledge Base Article - Q300958

Incorrect Answers

A: An Account Logon Event occurs when a domain controller received a request to validate a user account. However, we want to audit local login attempts, not domain logon attempts.

B: Client computers also have local account. The GPO must be applied to them as well.

C: Member servers also have local account. The GPO must be applied to them as well.

QUESTION 31:

You are the network administrator Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains a Windows XP Professional computer that is used by an employee named Mr Bill. Bill logs on to his computer by using a domain user account and accesses documents located on company file servers.

During a routine security audit, you examine the event logs on Bill's computer and discover that the Security log contains hundreds of events indicating failed logons for the local Administrator account.

You refresh Security log and notice that hundreds of additional identical events are added to the log. You suspect that an unauthorized user is attempting to access Bill's computer by using the local Administrator account.

You need to protect Bill's computer from this attack while ensuring that Bill can continue to work.

What should you do first?

A. Instruct Bill to log off.

Disconnect Bill's computer from the network and instruct him to log on again.

B. On Bill's computer, change the name of the local Administrator account to

XPLocalAdmin1.

C. On a domain controller, change the name of the domain Administrator account to CorpDomainAdmin1.

D. Instruct Bill to log on.

Log on to the computer as a domain administrator and disable Bill's user account.

Answer: B

Explanation:

Changing the name of the Local Administrator's account would increase security of the local computer.

Incorrect Answers

A: Disconnecting the computer from the network with increase security, but it would make Bill unable to use network resources.

C: It is not the Domain Administrator's account that is being attacked.

D: It is not Mr Bill's account that is being attacked.

QUESTION 32:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 10 organizational units (OUs), which represent Certkiller 's main office and its nine branch offices. Each company office contains a domain controller, servers, and client computers. Each OU contains the computer accounts for all computers, including the domain controller, in its associated company office.

You must ensure that all domain controllers have the same security settings, but you do not want to affect the security settings of the existing client computers. You create a security template named Dc_sec.inf that enables the required security settings.

What should you do next?

A. Import the security template to the Default Domain Policy Group Policy object (GPO).

Configure the DACL and the GPO so that only the Domain Controllers group has Read and Apply Group Policy permissions.

B. Import the security template to the Default Domain Controller Policy Group Policy object (GPO).

Configure the DACL on the GPO so that only the Domain Controllers group has Read and Apply Group Policy permissions.

C. Create a new Group Policy object (GPO) and link it to the domain.

Configure the DACL on each GPO so that only the Domain Controllers group has Read and Apply Group Policy permissions.

D. Create a new Group Policy object (GPO) and link it to the Domain Controllers OU. Configure the DACL on the GPO so that only the Domain Controllers group has Read and Apply Group Policy permissions.

Answer: A

Explanation:

The question states:

"The domain contain 10 OU's, which represent Certkiller 's main office and its nine branch offices. Each company office contains a domain controller, servers, and client computers. Each OU contains the computer accounts for all computers, including the domain controller, in it associated office."

So, this means that the domain controller account has been moved from the default Domain Controllers OU to an other OU. Thus the Default Domain Controller policy no longer applies to the domain controllers, because the Def. DC GPO is linked to the default domain controllers OU.

Now to let the policy apply to the DC's we have to either link a custom GPO with the security template imported to the OU's containing the DC computer accounts or import the security template in an existing GPO which is linked at an higher level. This scenario is described in answer A.

Incorrect Answers:

B: The DC's have been moved to another OU, so the default domain controller policy no longer applies to the DC's

C: Incomplete solution, we also need to import the security template

D: The DC's have been moved to another OU, so the default domain controller policy no longer applies to the DC's. Furthermore we also need to import the security template in the GPO.

QUESTION 33:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 500 Windows 2000 Professional computers and a Windows 2000 Server computer named Certkiller 1. Certkiller 1 runs Terminal Services in remote administration mode.

Certkiller 1 runs an order-processing application. Each user who needs to administer the application has a domain user account in a domain security group named App1. All members of App1 will use a Terminal Services client on their client computers to administer the application.

Members of App1 report that they can connect to Certkiller 1 by using the Terminal Services client, but they cannot log on by using Terminal Services. You need to configure these user accounts with the minimum permissions necessary to access Certkiller 1.

What should you do?

A. In the properties for each App1 user account, ensure that the Allow logon to terminal server check box is selected.

B. In the properties for each App1 user account, configure the Terminal Services user profile so that it has the same path as the user's Home folder.

C. Assign User Access permission to the Power Users in the Terminal Services Configuration snap-in.

D. Assign User Access permission to the App1 group in the Terminal Services

Configuration console.

Answer: A

Explanation:

To allow a user to log on to Terminal Services

1. Open Active Directory Users and Computers.
2. In the console tree, click Users.
3. Double-click the user for which you want to change settings.
4. On the Terminal Services Profile tab, select the Allow logon to terminal server check box, and then click Apply.

QUESTION 34:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The network contains two Windows 2000 Server computers configured as domain controllers and 1,500 Windows 2000 Professional client computers.

Certkiller has three departments: research, sales, and operations. Each department has a separate organizational unit (OU) in the domain that contains all user and group accounts for that department. Certkiller policy prevents configuration of Block Policy inheritance on the OUs.

You scan the domain controllers with the Microsoft Baseline Security Analyzer (MBSA) and receive the following message:

Computer is running with RestrictAnonymous = 0.

This level prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security.

Your manager tells you to use a security template to apply the MBSA-recommended setting to the domain controllers. You are not allowed to modify the configuration of other computers on the domain. You create a new security template based on the existing configuration of your domain controllers.

What should you do next?

A. In the template, set the Additional Restrictions for Anonymous Connections policy to No access without explicit anonymous permission.

Import this template into the Domain Controller Security Policy.

B. In the template, configure the Workstation service for Manual startup and deny Write access to the Anonymous Logon group.

Import this template in the Domain Controller Security Policy.

C. In the template, set the Additional Restrictions for Anonymous Connections policy to Do not allow enumeration of SAM accounts and shares.

Import this template into the Domain Security Policy.

D. In the template, configure the Workstation service for Manual startup and deny Read access to the Anonymous Logon group.

Import this template into the Domain Security Policy.

Answer: A

Explanation:

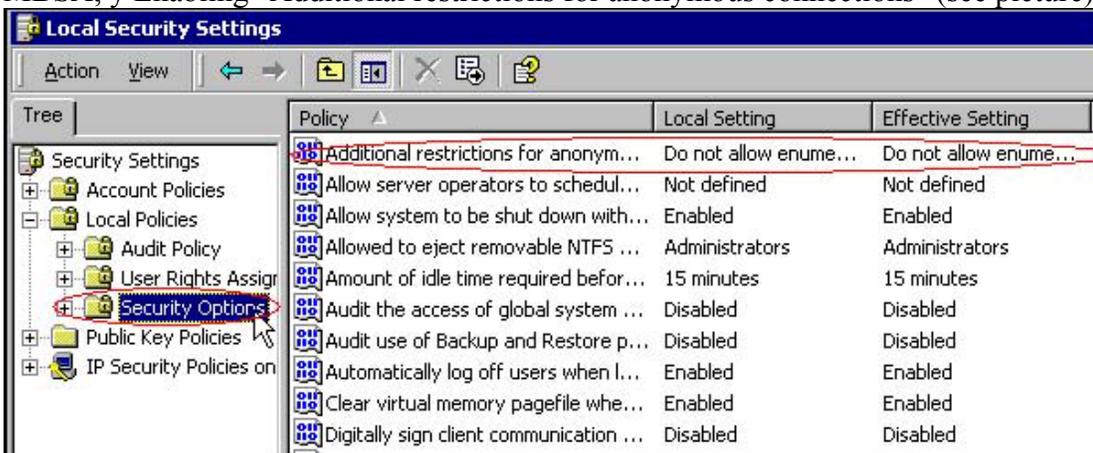
MBSA shows that the computer runs with RestrictAnonymous=0. The RestrictAnonymous numbers correspond to the following settings:

0 None. Rely on default permissions

1 Do not allow enumeration of SAM accounts and names

2 No access without explicit anonymous permissions

The RestrictAnonymous=0 setting is a security risk and it allow hackers to probe machine from the Internet for a list of the Users (SAM Accounts) and Shares (Shared folders and Printers). We can change this setting to 2, which is the recommendation from MBSA, y Enabling "Additional restrictions for anonymous connections" (see picture)..



And then set this policy to No access without explicit anonymous permission.

Note: Microsoft Baseline Security Analyzer (MBSA) scans for missing hotfixes and vulnerabilities in Windows, IIS, SQL Server, Internet Explorer, and MS Office.

Reference:

How to Use the RestrictAnonymous Registry Value in Windows 2000, Microsoft Knowledge Base Article - Q246261

Microsoft Baseline Security Analyzer (MBSA) Version 1.0 Is Available. Microsoft Knowledge Base Article - Q320454

Incorrect Answers

B, D: Manual startup of the workstation service would be awkward for the users. They would not be able to browse the network without this service.

C: This option would improve security, but security would be even better even we choose the No access without explicit anonymous permission. instead of Do not allow enumeration of SAM accounts and shares. This is also the recommendation of MBSA.

QUESTION 35:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 10,000 client computers and 50 Windows 2000 Server computers. One of the servers is named Certkiller 1. Certkiller 1

runs Microsoft Exchange Server 2000 and stored the mailboxes for all company users. All company users access e-mail by using Microsoft Outlook 2002.

The domain contains 8,000 contact objects. These objects represent individuals who work for customers of Certkiller .

A user receives an e-mail message from another company user named Bruno. The e-mail message contains a virus. Other users report that they have just received the same message from Bruno. You suspect that the message has been sent automatically to all recipients in the global address list (GAL).

You need to immediately prevent Certkiller 1 from automatically delivering the message to any additional recipients. You want to accomplish this task with the least amount of disruption to company users.

What should you do?

A. Stop all Exchange Server 2000 services.

Restore all Exchange Server 2000 information stores from the most recent backup.

Restart Certkiller 1.

B. Shut down Certkiller 1.

Modify the Active Directory permissions on all recipient objects so that only authenticated users have Read permission.

Restart Certkiller 1.

C. Disconnect Certkiller Internet connection.

Instruct all users to delete the infected e-mail message and ensure that all users comply.

Restore the Internet connection.

D. Disconnect Certkiller Internet connection.

Enable message tracking on Certkiller 1.

Locate and delete all copies of the message.

Restore the Internet connection.

Answer: D

Explanation:

By disconnecting the Certkiller Internet connection, enabling the message tracking on Certkiller 1, Locating and deleting all copies of the message and then restoring the Internet connection, we will be able to prevent Certkiller 1 from automatically delivering the message to any additional recipients.

QUESTION 36:

You are the network administrator for Certkiller . The network contains 5,000 Windows XP Professional computers and 2,000 Windows 2000 Professional computers.

Ten users report that their computers are infected with a virus. You discover that the virus attacks Internet Information Services (IIS), which is installed on half the computers on the network. Certkiller 's anti-virus software did not detect the virus. The software manufacturer wants you to find out which port the virus uses in its attacks.

You place an infected Windows 2000 Professional computer and an uninfected Windows XP Professional computer on an isolated network. You need to find out which port the

virus uses to attach the uninfected computer.

What should you do? (Each correct answer presents a complete solution. Choose two)

A. Enable auditing on the Windows XP Professional computer and configure auditing for all events.

Examine the events in Event Viewer.

B. Enable auditing on Windows 2000 Professional computer and configure auditing for all events.

Examine the events in Event Viewer.

C. Enable IIS logging on the Windows 2000 Professional computer.

Examine the log file in the Systemroot\System32\Logos\W3CSVC1 folder.

D. Enable the Internet Connection Firewall on the Windows XP Professional computer and enable logging.

Examine the Pfirewall.log file.

E. Enable Network Monitor on the Windows XP Professional computer and perform a capture.

Examine the events in the capture log.

Answer: C, D

Explanation:

Enabling the XP-Firewall and a look on the log file would help to see, on which port the virus comes in.

QUESTION 37:

You are the network administrator for Certkiller . The network consists if a Windows 2000 Active Directory domain. The domain contains a Windows 2000 Server computer named Certkiller 1. Certkiller 1 is a member of the domain.

Certkiller 1 hosts an accounting application named AccountingService that runs as a service. On Monday morning, users report that they cannot access AccountingService. You discover that AccountingService is stopped. You attempt to start the service but receive an error message indicating that the service cannot be started as the result of a logon failure.

You examine the Security log on a domain controller and discover the following event.

Event ID: 539 (0x021B)

Type: Failure Audit

Description: Logon Failure

Explanation: Account locked out

User Name: SVCACCTA Domain : Certkiller

Logon Type: 2 Logon Process: NETLOGON

Authentication Package: NTLM

Workstation Name: Certkiller 1

You need to ensure that AccountingService will start.

What should you do?

- A. Reset the password on the domain computer account for Certkiller 1.
 - B. Grant the Svcacct domain user account the Logon as a service domain user right.
 - C. Use the Netdom.exe command to reset Certkiller 1's domain computer account.
 - D. Change the password for the Svcacct domain user account.
- Reconfigure AccountingService to use the new password.
Unlock the Svcacct domain user account.

Answer: D

Explanation:

We should perform these steps to solve the problem:

- * Change the password for the affected domain user account.
- * Reconfigure AccountingService to use the new password.
- * Unlock the affected domain user account.

QUESTION 38:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain.
Bruno is an employee in the sales department. Bruno uses a Windows NT Workstation 4.0 computer named CK1 . CK1 is a member of the domain. Bruno receives a new Windows XP Professional computer named Client2, and CK1 is removed from the network. Bruno immediately reports that he cannot log on to Client2.
You examine the Security log on a domain controller and discover the following event.
Event ID: 533 (0x0215)
Type: Failure Audit
Description: Logon Failure

Explanation: User not allowed to logon at this computer
User name: BRUNO Domain: Certkiller
Logon Type: 2 Logon Process: NETLOGON
Authentication Package: NTLM Workstation Name: CLIENT2
You need to ensure that Bruno can log on to Client2.
What should you do?

- A. Disable the computer account for CK1 .
 - B. Delete the computer account for CK1 .
 - Change the computer name for Client2 to CK1 .
 - C. Place the computer account for Client2 in the same organizational unit (OU) that contains the computer account for CK1 .
 - D. Connect CK1 to the network.
- Use the Files and Settings Transfer wizard to transfer Bruno's files and settings to Client2.
Remove CK1 from the network.

Answer: C

Explanation:

Event generated by as logon failure due to a user not allowed to logon at this computer.

Reference:

<http://www.eventid.net/display.asp?eventid=533>

QUESTION 39:

You are the network administrator for Certkiller . You manage three Windows 2000 Server computers. Two of these servers are configured as domain controllers, and the other is a member server named Certkiller 1.

Certkiller 1's computer account is an organizational unit (OU) named Secure. A Group Policy object (GPO) linked to the Secure OU has the Audit logon events policy assigned for both success and failure access. The Secure OU is configured to Block Policy inheritance.

The written security policy for Certkiller requires you to back up and clear the logs on Certkiller 1 monthly.

To back up and clear the event logs, you log on as Jack@ Certkiller .com. As you are archiving the Security log on Certkiller 1, you notice that the log has fewer events than usual. The first entry in the audit log is shown in the exhibit.

Event type: Success

Event source: Security

Event category: System Event

Event ID: 517

Description: The audit log was cleared.

Primary User Name: SYSTEM

Primary Domain: NT Authority

Primary Logon ID: (0x0, 0x3E7=

Client User Name: Nina

Client Domain: Certkiller

Client Logon ID: (0x0, 0x75D59)

You must ensure that company policy is enforced.

What should you do first?

- A. On Certkiller 1, change the CrashOnAuditFail registry value to 1.
- B. Deny the System group Full Control access of the Sysevent.evt file.
- C. Remove the user account Nina from all groups that allow administrative access to Certkiller 1.
- D. Configure Audit Policy of the GPO linked to Secure to Audit privilege user for the administrators group.
- E. Configure the system group for Read only permission to Systemroot\System32\Config folder on Certkiller 1.

Answer: C

Explanation:

The log shows that the user Nina has cleared the Audit log. We must prohibit her from doing so. This is achieved by removing her account for all groups that have administrative access to the computer.

Incorrect Answers

A: The CrashOnAuditFail registry value on applies after the system has crashed. It does not apply in this scenario.

B: Will not achieve much.

D: We do not more auditing.

E: Will not achieve much.

QUESTION 40:

You are an administrator of Certkiller 's Web servers. These servers run Windows 2000 Server and Internet Information Services (IIS). On each server, IIS is installed with the default settings. In addition to the default Web site, each server hosts four additional Web sites. Logging is enabled for all Web sites on all servers.

During the night, an Internet-based intruder accesses a Web server. The attacker gains access to the source code of several Microsoft Active Server Pages (ASP) Web pages on the default Web site and deletes several Web pages from the Default Web site. The other Web sites on the server are not affected.

The next morning, another administrator discovers the security breach. The administrator restores the Web pages and reconfigures each Web server to prevent future attacks.

You need to save all evidence of the attacker's activities for future research. You cannot remove the server from production.

What should you do?

A. Make a copy of the most recent log file from the the Systemroot\LogFiles\W3SVC1 folder.

B. Make a copy of the log files that are contained in each Systemroot\LogFiles\W3SVC* folder.

C. Back up the System State data to a backup file.

Then, copy that backup file to a secure server.

D. Back up the C:\Inetpub folder to a backup file.

Then, copy that backup file to a secure server.

Answer: A

Explanation:

The other web sites are not affected, therefore, we only need to inspect the Systemroot\LogFiles\W3SVC1 folder only

Reference: Chapter 10, Configuring and Using Auditing and the Event Logs, MCSE Implementing and Administering Security in a Windows 2000 Network Study Guide & DVD Training System

QUESTION 41:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains a Windows 2000 Server computer named Certkiller 1. Certkiller 1 is a member of the domain.

During a security audit on Certkiller 1, you discover that every five minutes, the Security log repeats the following two events.

Event Type: Error

Event Source: Userenv

Event Category: None

Event ID: 1000

Description: The Group Policy client-side extension Security was passed flags (17) and returned a failure status code of (1208).

Event Type: Warning

Event Source: SceCli

Event Category: None

Event ID: 1202

Description: Security policies are propagated with warning.

0x4b8 : An extended error has occurred. Please look for more

details in Troubleshooting section in Security Help.

You review Winlogon.file and discover the following error message.

Error 1332: No mapping between account names and security IDs was done. Cannot find Power Users.

You need to correct the condition that is causing these errors.

What should you do?

- A. Run the secedit command to refresh the Group Policy object (GPOs) on Certkiller 1.
- B. Ensure that the Net Logon service on Certkiller 1 is configured to start automatically.
- C. Remove all references to the Power Users group from the Local Security Policy on Certkiller 1.
- D. Configure Certkiller 1 with the correct IP addresses for the DNS servers on your network.

Answer: C

Explanation:

There seems to be a problem with references made to the Power Users Group.

Incorrect Answers

A: We do not use secedit.

B: This is not a problem with the Net Logon service

D: This is not the problem with the DNS server.

QUESTION 42:

You are the network administrator for Certkiller . The network consists of a main office, four branch offices, and one Windows 2000 Active Directory domain. Each office contains a Windows 2000 Server computer that is configured as a domain controller. The network also contains a Windows 2000 DNS server that requires secure updates.

Users in one branch office report that their client computers are slow logging on to the network each morning. You restart the domain controller in the office, but users report that the problem continues after the domain controller restarts. The domain controller in the office is a Windows 2000 Server computer named Certkiller 3. Certkiller 3 runs Terminal Services.

You connect and log on to Certkiller 3 by using Terminal Services and discover that the server takes a long time to process your logon. You open Task Manager and discover that the System Idle process on the server is receiving approximately 95 percent of the server's processor utilization.

You examine the System log on the server and discover the following entry.

Event Type: Error

Event Source: NETLOGON

Event Category: None

Event ID: 5775

Description:

Deregistration of the DNS record

'_kerberos._tcp.dc._msdcs. Certkiller .com. 600

IN SRV 0 100 88 " Certkiller 3. Certkiller .com.'

failed with the following error: DNS bad

key. Data: 0000: 39 23 00 00 9#..

You need to return the server to normal operating condition.

What should you do?

- A. Add an additional processor to Certkiller 3.
- B. Delete all DNS records created by Certkiller 3 on the DNS server and restart Certkiller 3.
- C. Ensure that the Kerberos Key Distribution Center service on Certkiller 3 is set to start automatically.
Restart Certkiller 3.
- D. Use the Active Directory Users and Computer console to delete and re-create the computer account for Certkiller 3.

Answer: B

Explanation:

This is a DNS problem. The DNS Service is unable to deregister a resource record. We resolve the problem by manually deleting all DNS records by Certkiller 3.

Note: The Netlogon 5775 error message is logged in the System event log when the Netlogon service on a domain controller cannot deregister an individual resource record. The event description contains the name of this resource record and other DNS parameters that are used for the deregistration attempt.

Incorrect Answers

- A: This is not a performance issue.
 - C: This is not a login problem, and is not affected by the Kerberos Key Distribution Center service.
 - D: The computer account does not cause this problem.
-

QUESTION 43:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain is configured to audit logon events.

Maria is a user in Certkiller sales department. On Monday, Marie goes on a one-week vacation. The next day, you discover that the Security log on each domain controller in the domain contains the following event:

Event ID: 529 (0x0211)

Type: Failure Audit

Description: Logon Failure

Explanation: Unknown user name or bad password

User Name: Maria Domain: Certkiller

Logon Type: 3 Logon Process: NETLOGON

Authentication Package: NTLM Workstation Name:

This event appears more than 100 times on Tuesday, and the event repeats approximately every minute.

You need to immediately prevent this security violation from occurring. You do not want to affect other network users.

What should you do?

- A. Disable the domain computer account for CK1 .
- B. Disable the domain user account for Maria.
- C. Stop the Net Logon service on all domain controllers.
- D. Delete the domain user account that is used by the user of CK1 .

Answer: B

Explanation:

We simply disable the user account. It will not affect the network users. Maria will not be affected as well, as she is on a one-week vacation.

QUESTION 44:

You are the administrator of a Windows 2000 Server computer named Certkiller 1.

Certkiller 1 is a file server used by all company employees.

One morning, users report that more than 500 files are missing from Certkiller 1. You examine the audit log on Certkiller 1 and discover that the files were deleted by a former employee named Jack, who was recently fired. Many deleted files are new and are not contained on any backup tapes.

Your legal department instructs you to preserve the evidence of Jack's access to

Certkiller 1. You need to ensure that as many deleted files as possible can be restored by using a disk sector editor. You also need to allow employees to access the remaining files.

What should you do?

- A. Remove Certkiller 1 from your network.
Create an exact image of Certkiller 1's hard drive.
Restore the image to a new file server.
- B. Restore as many deleted files as possible from backup tape.
Then, perform a full backup.
- C. Configure the event logs so that they do not overwrite events.
Then, stop the Server service.
- D. Save the event logs to a file.
Then, copy all files to another file server.

Answer: D

Explanation:

Saving the event logs preserves evidence of Jack's access to Certkiller 1.
Copying the files to another file server, ensures that they are available for other employees.

QUESTION 45:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.
One of the Windows 2000 member servers, Certkiller 1, runs Routing and Remote Access for Windows 2000. Users can dial into the Certkiller network from home by connecting to Certkiller 1.

The written security policy for Certkiller requires that all failed and successful access to Certkiller 1 be logged. You configure the Shut down system immediately if unable to log security audits policy setting for Certkiller 1.

Eight months later, Certkiller 1 suddenly displays the STOP error "STOP: C0000244 {Audit Failed}" and shuts down. The server operator for Certkiller 1 reports that he is unable to make Certkiller 1 work again.

You want to ensure that Certkiller 1 is operational again.

What should you do?

- A. Increase the Maximum security log sizeevent log policy for Certkiller 1.
Restart Certkiller 1.
- B. Enable the Overwrite events as neededoption for the Security event log on Certkiller 1.
Restart Certkiller 1.
- C. Log on to Certkiller 1.
Save and clear the Security log.
Set the CrashOnAuditFail registry value to 1.

Restart Certkiller 1.
D. Log on to Certkiller 1.
Change the audit policy so that system events are not audited.
Set the CrashOnCtrlScroll registry value to 1.
Restart Certkiller 1.

Answer: B

Explanation:

This problem occurs if the Security Log has reached the Maximum Log Size specified, and Event Log Wrapping is set for "Overwrite Events Older than (X) Days." This can also occur if "Do Not Overwrite Events" is selected. Because the Security Event Log is full, and the CrashOnAuditFail registry key is set, Windows NT generates a STOP 0xC0000244 blue screen error message and cannot log audit information.

To work around this problem, use one of the following options:

1. Set the Event Log Wrapping for "Overwrite Events as Needed." (This is B).
2. Decrease the amount of information being audited.
3. Increase the log file size and use a combination of the previous options listed above.
4. Disable auditing.

Reference:

STOP 0xC0000244 When Security Log Full, Microsoft Knowledge Base Article - Q232564

Incorrect Answers

A: Just increasing the Maximum security log size will not prevent the problem from reoccurring.

C: Saving and clearing the Security log are good steps. However, nothing is done to prevent this crash from reoccurring later. In fact, a CrashOnAuditFail registry value of 1 ensures that the system crashes when it is unable to audit events.

D: The written security policy requires auditing of login attempts.

QUESTION 46:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains two domain controllers, three Windows 2000 member servers, and 500 Windows 2000 Professional client computers. Users log off their client computers and shut down their systems at the end of each workday.

You want to install a new service pack on all the Windows 2000 computers on the network. You test the service pack on several computers. You then create a share on one of the servers and copy the appropriate service pack files to that share.

You want the service pack to automatically install when users turn on their computers.

What should you do?

A. Create a .zap file that calls a logon script that runs in the security context of the user. Configure the script to run the update.exe command with reference to computername variable.

Publish the .zap file to the users on the network.

B. Create a .zap file that calls a logon script that runs in the security context of the user. Configure the script to run the update.exe command with reference to username variable. Publish the .zap file to the users on the network.

C. Create a Group Policy object (GPO) and link it to the domain. Configure the GPO to assign to the users on the network a software installation package containing the new service pack .msi file.

D. Create a Group Policy object (GPO) and link it to the domain. Configure the GPO to assign to the computers on the network a software installation package containing the new service pack .msi file.

Answer: D

Explanation:

You can use the Software Installation and Maintenance feature in Windows 2000, which leverages Windows Installer Service and the Update.msi file to create a Windows Installer package that installs the service pack. Software Installation and Maintenance uses a Group Policy object (GPO) to deploy the package. Microsoft requires use of the "Machine Assigned" distribution method when using Update.msi.

Reference:

Microsoft Windows2000 Service Pack Installation and Deployment Guide

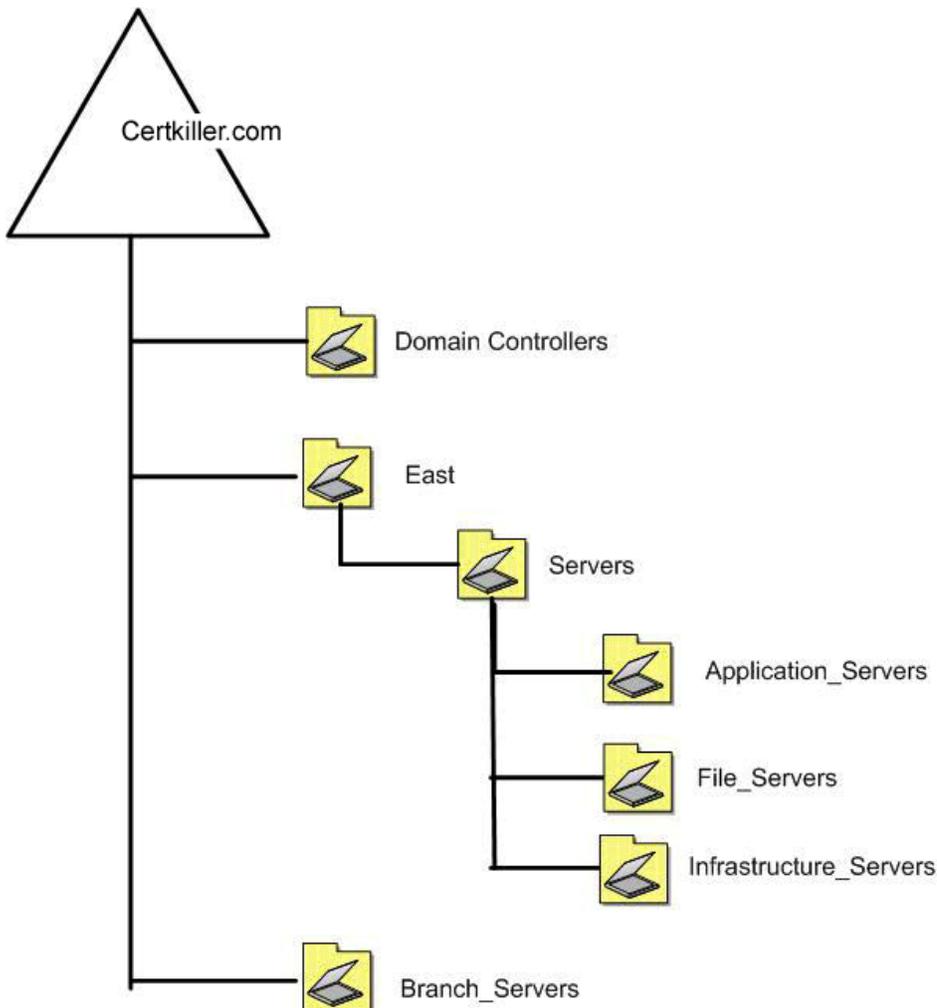
Incorrect Answers

A, B: .zap files are used to create non-Windows installer packages.

C: Microsoft requires use of the "Machine Assigned", not "User Assigned", distribution method when using Update.msi.

QUESTION 47:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains a Windows 2000 Server computer named Certkiller 1. Certkiller 1 is located in the File_Servers organizational unit (OU). The relevant portion of the Active Directory structure is shown in the exhibit.



At least one Group Policy object (GPO) is linked to the East OU and each of its child OUs. Each GPO contains one software deployment package in the computer configuration. The computer configuration section of each GPO also contains security settings.

You need to move Certkiller 1 to the Branch_Servers OU. The Branch_Servers OU has a GPO named BranchGPO linked to it. After the move, the security configuration for Certkiller 1 must remain unchanged. However, you do not want any software packages to affect Certkiller 1.

What should you do?

A. Add links from the GPOs that are linked to the East OU and its child OUs to the Branch_Servers OU.

B. Remove the links for all GPOs that are linked to the East OU and its child OUs. Link these GPOs to the domain.

C. Export the effective security policy settings from Certkiller 1 to a file named Certkiller 1.inf.

Move Certkiller 1 to the Branch_Servers OU and import the Certkiller 1.inf file to the BranchGPO.

D. Create a new security group named All_Servers in the File_Servers OU.

Add Certkiller 1 to the All_Servers group.

For each GPO that is linked to the East OU and its child OUs, configure the All_Servers group to have the Apply Group Policy and Read permissions.

Answer: C

Explanation:

We export the security policy settings into a file. We then move the computer to the Branch_Servers OU, and apply the saved security settings to the new OU.

Incorrect Answers

A: This ad hoc solution would not meet the requirements. The software packages would still affect Certkiller 1.

B: The software packages would still affect Certkiller 1.

D: We must move Certkiller 1 to the Branch_Servers OU. We cannot keep Certkiller 1 in the File_Servers OU.

QUESTION 48:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains computers that run Windows 2000 Server, Windows 2000 Professional, or Windows XP Professional.

The written security policy for Certkiller requires you to configure baseline security permissions for the HKEY_LOCAL_MACHINE portion of the registry on all computers in the domain. The client computers require a different baseline security configuration than the servers.

You create two organizational units (OUs): Clients and Servers. You move all computer accounts for the client computer to the Clients OU and all computer accounts for the servers to the Servers OU. You also create two Group Policy objects (GPOs): SecClients and SecServers. You link the SecClients GPO to the Clients OU and the SecServers GPO to the Servers OU.

You must ensure that the baseline security for the HKEY_LOCAL_MACHINE is deployed to the client computers and servers.

What should you do?

A. Create two security templates: one for client computers and one for servers.

Configure each template to include all registry entries defined in the baseline security policy.

Import the template for the servers into the Default Domain Policy GPO.

Import the template for the client computers to the Default Domain Policy GPO.

B. Create two security templates: one for client computers and one for servers.

Configure each template to include all registry entries defined in the baseline security policy.

Import the template for the servers to the SecServers GPO.

Import the template for the client computers to the SecClients GPO.

C. Create two custom administrative templates: one for client computers and one for servers.

Configure each template to include all registry entries defined in the baseline security policy.

Add the template for the servers to the Default Domain Policy GPO.

Add the template for the client computers to the Default Domain Policy GPO.

D. Create two custom administrative templates: one for client computers and one for servers.

Configure each template to include all registry entries defined in the baseline security policy.

Add the template for the servers to the SecServers GPO.

Add the template for the client computers to the SecClients GPO.

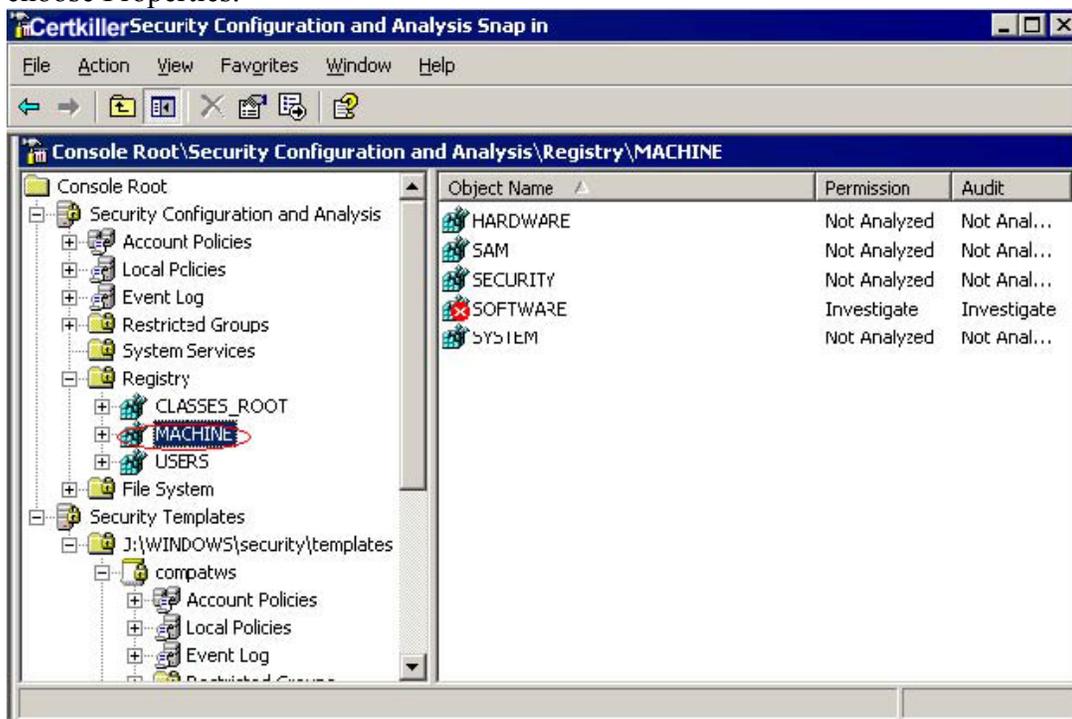
Answer: B

Explanation:

We must use two separate security templates, one for the client computers and for the servers. We configure each security template with the appropriate Registry permissions (see below). We then make sure that they are applied to the right computers by importing them into the SecServers GPO and SecClients GPO respectively.

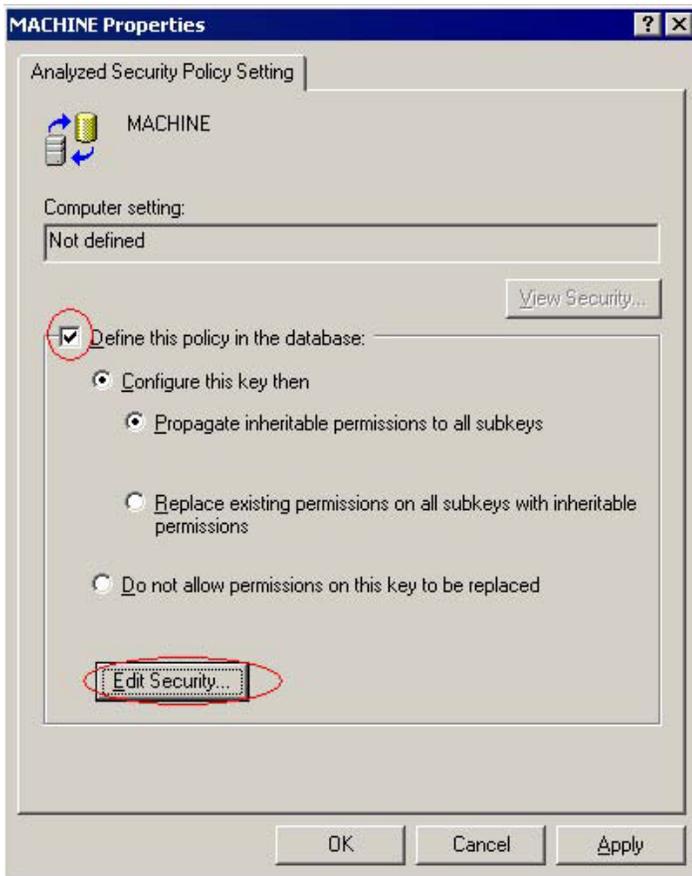
Procedure changing the permission of a Registry key with a security template:

1. Open the Security Configuration and Analysis Snap in,
2. Import a template.
3. Expand Registry, locate the appropriate Registry key. Right-click on the key and choose Properties.



4. Select Define this policy in the database.

5. Click Edit Security and set the appropriate permissions.



Note: A security template is a physical representation of a security configuration, a single file where a group of security settings is stored.

Incorrect Answers

A: We cannot apply both security templates to all computers in the domain.

C, D: A customer administrative template can be used to set specific registry values. However, it cannot be used to configure permission on specific keys of the Registry.

QUESTION 49:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 5,000 Windows XP Professional computers. All computers were purchased with Windows XP Professional already installed. All computers are configured by means of a Group Policy object (GPO) named Master, which is linked to the domain.

During the week, several viruses infect the network by means of incoming e-mail messages that contain Microsoft Visual Basic Scripting Edition (VBScript) files. The written security policy for Certkiller prohibits users from running Microsoft ActiveX scripts on any company computer.

You need to ensure that all company computers comply with the written policy. You want to accomplish this task in the least amount of administrative time.

What should you do?

A. In the computer configuration section of the Master GPO, create a new software restriction.

In the new restriction, remove the VBS and WSC file types from the File Types list.

B. In the computer configuration section of the Master GPO, create a new software restriction that includes has rules for C:\Windows\System32\Wscript.exe and C:\Windows\System32\Cscript.exe.

Configure the rules as Disabled.

C. Instruct all users to open the Tools menu in My Computer, select Folder Options, select the File Types tab, and then remove the VBS file type.

Write a VBScript file that sends you an e-mail message when it runs, and then send the script to all company users via e-mail.

D. Write a logon script that deleted the Wscript.exe file and the Cscript.exe file. Import the logon script into a GPO and link it to the domain.

Answer: D

Explanation:

We use a GPO that ensures that Wscript.exe and Cscript.exe is deleted. We apply the GPO to the domain. This will ensure that running Microsoft ActiveX scripts is disabled.

Note: The vbscripting threat can be blocked by disabling the Windows Scripting Host which is the agent that executes the .vbs files. There are several methods which are compatible for Windows NT / Windows 2000 and Windows XP:

Rename or delete the WSH executable : wscript.exe,

Its normally found in the system32 folder. (this is the idea of D)

Block WSH from executing .vbs files by removing the file association

Right-click My Computer

Select Open from the menu

Select the View tab

Select Options

Open the File Types tab

Select VBScript Script File from the list of file types

If its not there, then WSH is not installed or has been disabled. If its there

Click on the Remove button to remove the ability of WSH to run .vbs scripts.

(this is C),

Dynamically disable / enable WSH using third party software such as Symantec's Noscript.exe freeware program.

Disable scripts using third party software such as AnalogX Script Defender program.

Incorrect Answers

A: These steps would not prevent Microsoft ActiveX scripts from being run.

B: This will not work.

C: This method would work. However, we cannot trust the users to perform this fairly complicated maneuver.

QUESTION 50:

You are the network administrator for a branch office of Certkiller . All computers on the

network are members of a Windows 2000 Active Directory domain. Certkiller has one domain administrator at the main office.

An organizational unit (OU) named Branch1 corresponds to your branch office. An OU named Files is under the Branch1 OU. All user accounts, computer accounts, printer objects, and shared resources of your branch office are in the Branch1 OU.

Three Windows 2000 Server computers are configured as file servers named Certkiller 1, Certkiller 2, and Certkiller 3. The computer accounts for these servers are in the Files OU. The domain administrator has delegated to you full control of Branch1 and all its subordinate OUs. You are granted the ability to create and link Group Policy object (GPOs).

An Audit Policy is not defined for any GPO that is linked to the domain. Auditing of Read permissions, both success and failure, is enabled for the Everyone group on all folders and files on the file servers to which users have access.

You configure the SACL on each folder that your manager is concerned about to audit success and failure of Read access for the Everyone group. Corporate management wants you to log all user access to files or folders on only the file servers in your branch office. What should you do?

- A. Create a Group Policy object (GPO) and link it to the Files OU. Configure the GPO to enable both the success and failure of the Audit logon events policy.
- B. Create a Group Policy object (GPO) and link it to the Files OU. Configure the GPO to enable both the success and failure of the Audit object access policy.
- C. Ask the domain administrator to create a Group Policy object (GPO) and link it to the domain. Configure the GPO to enable both the success and failure of the Audit logon events policy.
- D. Ask the domain administrator to create a Group Policy object (GPO) and link it to the domain. Configure the GPO to enable both the success and failure of the Audit object access policy.

Answer: B

Explanation:

We must enable auditing of object access. We should only enable auditing of file servers in the branch office. We should therefore configure a GPO to audit object access and link the GPO to the Files OU, which contains the Branch office file servers.

Note: SACL = System Access Control List

Incorrect Answers

A, C: We are not interested in auditing logon events.

D: We should not enable auditing of object access for the whole domain. We only need to configure auditing at the appropriate OU level.

QUESTION 51:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains four Windows 2000 domain controllers, 200 user accounts, and 225 computer accounts.

Approximately five percent of the domain accounts are not used on a regular basis. However, you do not know which accounts are currently active and which ones are no longer used.

You back up the System State data of each domain controller to tape every night. The tapes are stored at an offsite facility. One morning, the manager of the offsite facility reports that four recent backup tapes are missing. He suspects that the tapes were stolen by a former employee.

You need to ensure that the information on the backup tapes cannot be used to compromise the security principals in the domain. You have access to a library of scripts written in Microsoft Visual Basic Scripting Edition (VBScript), which might help you accomplish this task.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

- A. Run a script that configures all user and computer account passwords as expired.
- B. Run a script that configured all user accounts so that users must change their passwords the next time they log on.
- C. Run a script that disables all user accounts.
Instruct users to contact Certkiller help desk to re-enable their accounts.
- D. Run a script that registers Passfilt.dll
- E. Modify the domain account policies so that the password history contains the last 20 passwords.
- F. Modify the domain account policies to include a longer minimum password length and a maximum password age of five days.

Answer: C, F

Explanation:

C: This is a drastic measure. However it seems that it is required in this scenario.

F: We should ensure that we have a strong account policy regarding password complexity.

Incorrect Answers

A: This measure would make the situation complicated.

B: 5 % of the user accounts are not used on a regular basis. This method would not address these user accounts.

D: Microsoft Windows NT 4.0 Service Pack 2 introduces a new DLL file (Passfilt.dll) that lets you enforce stronger password requirements for users. Passfilt.dll provides enhanced security against "password guessing" or "dictionary attacks" by outside intruders. The functionality described above for Windows NT 4.0 has been moved into the operating system security components for Windows 2000 and Windows XP. Strong password enforcement can be enabled on Windows 2000 and Windows XP using the

system administration tools.

E: A password history that remember the last 20 password would increase security. However, it is not best way to improve security.

QUESTION 52:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain, 20 Windows 2000 Server computers, 500 Windows XP Professional computers, and 4,000 Windows Professional computers. All computer accounts are located in the DomainComputers organizational unit (OU).

You receive a new Windows 2000 service pack. You need to ensure that the service pack will be deployed to all Windows 2000 computers. You do not want the service pack deployed to Windows XP Professional computers.

What should you do?

A. Create a child OU named XPro under the DomainComputers OU.

Place the computer account for each Windows XP Professional computer in the XPro OU.

Create a Group Policy object (GPO) and link the GPO to the domain.

Configure the GPO to assign the service pack in the computer configuration section.

B. Create a child OU named XPro under the DomainComputers OU.

Place the computer account for each Windows XP Professional computer in the XPro OU.

Create a Group Policy object (GPO) and link the GPO to the DomainComputers OU.

Configure the GPO to assign the service pack in the user configuration section.

C. Create a child OU named Win2000Pro under the DomainComputers OU.

Place the computer account for each Windows 2000 computer in the Win2000Pro OU.

Create a Group Policy object (GPO) and link the GPO to the Win2000Pro OU.

Configure the GPO to assign the service pack in the user configuration section.

D. Create a child OU named Win2000Pro under the DomainComputers OU.

Place the computer account for each Windows 2000 computer in the Win2000Pro OU.

Create a Group Policy object (GPO) and link the GPO to the Win2000Pro OU.

Configure the GPO to assign the service pack in the machine configuration section.

Answer: D

Explanation:

We must put the Windows 2000 computers into a separate OU. We must create a GPO that deploys the service pack by assigning it to computers. The GPO is linked to the new OU..

Incorrect Answers

A: If we apply the GPO to domain it would affect all computers.

B: We need to create a OU for the Windows 2000 computers, not for the Windows XP computers.

C: We must assign the service pack to computers, not to users.

QUESTION 53:

You are the network administrator for your Certkiller . The network consists of a Windows 2000 Active Directory domain. The network contains two Windows 2000 Server computers configured as domain controllers and 1,500 Windows Professional client computers.

You place three client computers in a public waiting area for guests. You create an organizational unit (OU) named Public and move the three client computer accounts into it.

You create a Group Policy object (GPO) named Publock. You enable several restrictions for the desktop, Start menu, and Taskbar in the Publock GPO.

You need to ensure that all settings in the Publock GPO are applied to any user who logs on to the three client computers in the public waiting area.

What should you do?

- A. Configure Block Policy inheritance on the Public OU.
- B. Configure the Publock GPO to enable User Group Policy loopback processing mode in Replace mode.
- C. Modify the DACL of the Publock GPO and give the Everyone group Read and Apply Group Policy permissions.
- D. Select the Disable User Configuration settings option on the Publock GPO. Configure the Deny access to this computer from the network policy in the computer configuration section of the GPO.

Answer: B

Explanation:

Applies alternate user policies when a user logs on to a computer affected by this policy.

This policy directs the system to apply the set of Group Policy objects for the computer to any user who logs on to a computer affected by this policy. It is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user policy based on the computer that is being used.

By default, the user's Group Policy objects determine which user policies apply. If this policy is enabled, then, when a user logs on to this computer, the computer's Group Policy objects determine which set of Group Policy objects applies.

To use this policy, select one of the following policy modes from the Mode box:

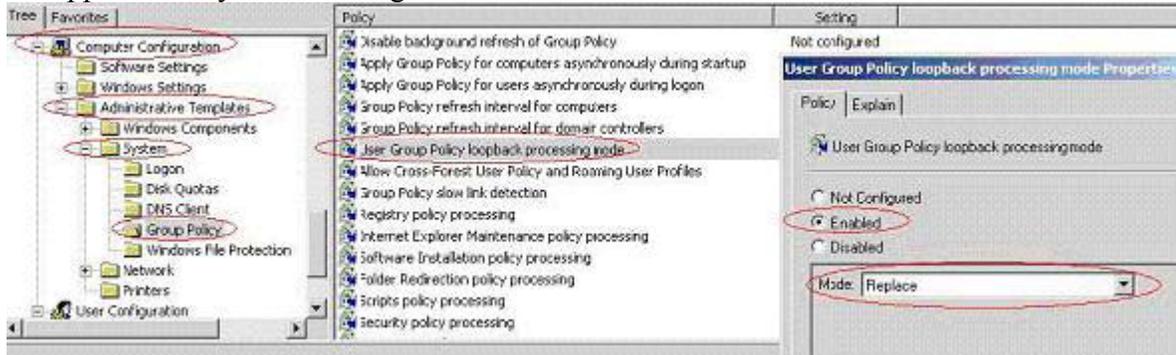
-- "Replace" indicates that the user policies defined in the computer's Group Policy objects replace the user policies normally applied to the user.

-- "Merge" indicates that the user policies defined in the computer's Group Policy objects and the user policies normally applied to the user are combined. If the policy settings conflict, the user policies in the computer's Group Policy objects take precedence over the user's normal policies.

If you disable this policy or do not configure it, the user's Group Policy objects determines which user policies apply.

Note: This policy is effective only when both the computer account and the user account are in Windows 2000 domains.

The Group Policy loopback feature is used to apply Group Policy Objects (GPOs) that depend only on which computer the user logs on to. This would ensure that Publock GPO are applied to any user who logs on.



Reference:

Loopback Processing of Group Policy, Microsoft Knowledge Base Article - Q231287

Incorrect Answers

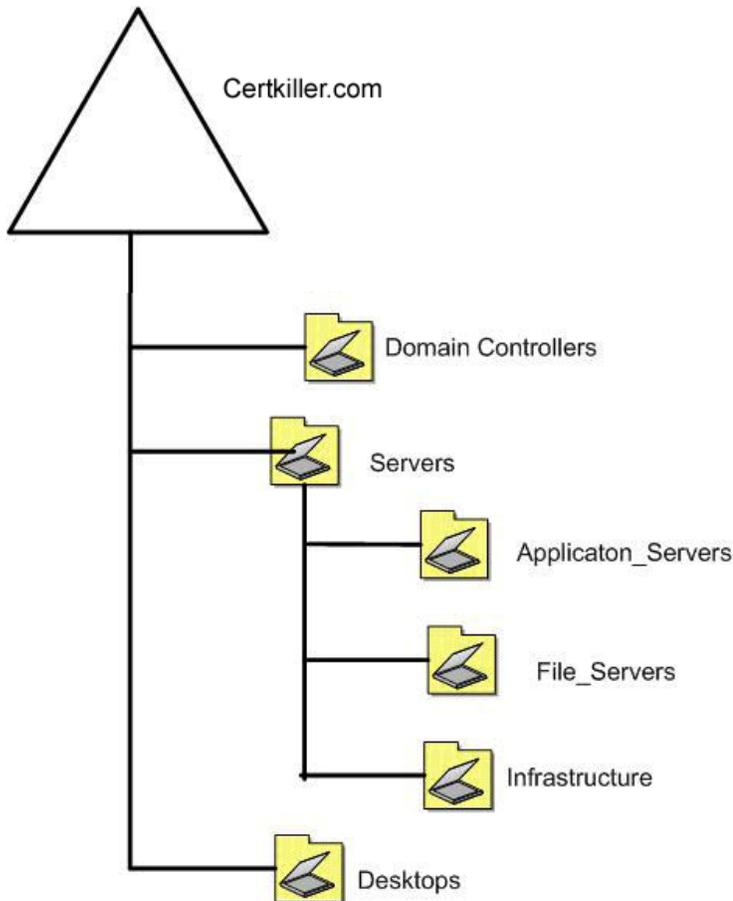
A: Block Policy inheritance would not be useful.

C: Read and Apply Group Policy permissions would ensure that GPO would be applied to the Everyone group. This is not helpful in this scenario.

D: Other user-specific GPOs could be applied to the computer.

QUESTION 54:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain named Certkiller .com. Certkiller 's Active Directory organizational unit (OU) structure is based on the defined server roles. The relevant portion of the Active Directory structure is shown in the exhibit.



The IT manager wants you to develop a standardized security baseline that implements NTFS and registry permissions that conform with the written security of Certkiller for servers. The servers that require the security baseline settings include application servers, file servers, and infrastructure servers.

You decide to use security template to define the baseline security settings. You define the following security templates:

1. A security template named Default.inf that includes the required NTFS and registry permissions for Windows 2000-based servers in Certkiller .
2. Individual security template that define role-specific security settings.

There is one security template for each server role in Certkiller .

What strategy should you use to deploy the security templates?

- A. Create a Group Policy object (GPO) and link it to the domain.
Import the Default.inf security template to the new GPO.
Import the role-specific security templates to individual GPOs linked to the Servers OU.
- B. Create a Group Policy object (GPO) and link it to the Servers OU.
Import the Default.inf security template to the new GPO.
Import the role-specific security templates to individual GPOs linked to the Servers OU.
- C. Create a Group Policy object (GPO) and link it to the domain.
Import the Default.inf security template to the new GPO.
Import the role-specific security templates to GPOs linked to each role-specific OU.
- D. Create a Group Policy object (GPO) and link it to the Servers OU.

Import the Default.inf security template to the new GPO.
Import the role-specific security templates to GPOs linked to each role-specific OU.

Answer: D

Explanation:

The Default.inf template should be applied through a GPO at the Servers OU to ensure that all servers use this template. The individual GPOs should be linked to each-role-specific OU.

Incorrect Answers

A, C: We don't want to apply the Default.inf to the Desktop computers. We should not apply it at the domain level.

B: The individual GPOs should be linked to each-role-specific OU, not to the Servers OU where they would be applied to all servers.

QUESTION 55:

You are the administrator of a Windows 2000 network. The network consists of a Windows 2000 Active Directory domain named Certkiller .com. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers. The client computers are in an organizational unit (OU) named Clients. You use Group Policy objects (GPOs) to administer the configuration of the Windows 2000 Professional client computers.

To increase the security of the client computers, you want to ensure that the configuration settings in the client computers are always corrected whenever a user changes these settings manually.

What should you do?

A. Configure the Task Scheduler on the client computers to periodically run the secedit /refreshpolicy machine_policy and the secedit /refreshpolicy user_policy commands.

B. Configure the Default Domain Group Policy object (GPO) to enable Group Policy refresh interval for computers settings and a Group Policy refresh interval for users setting.

C. Create a GPO and link it to the Domain Controllers OU.

Configure the GPO to enable the User Group Policy loopback processing mode in merge mode.

D. Create a GPO and link it to the Clients OU.

Configure the GPO to enable the settings to process policies even if the GPOs have not changed.

E. Create a GPO and link it to the Clients OU.

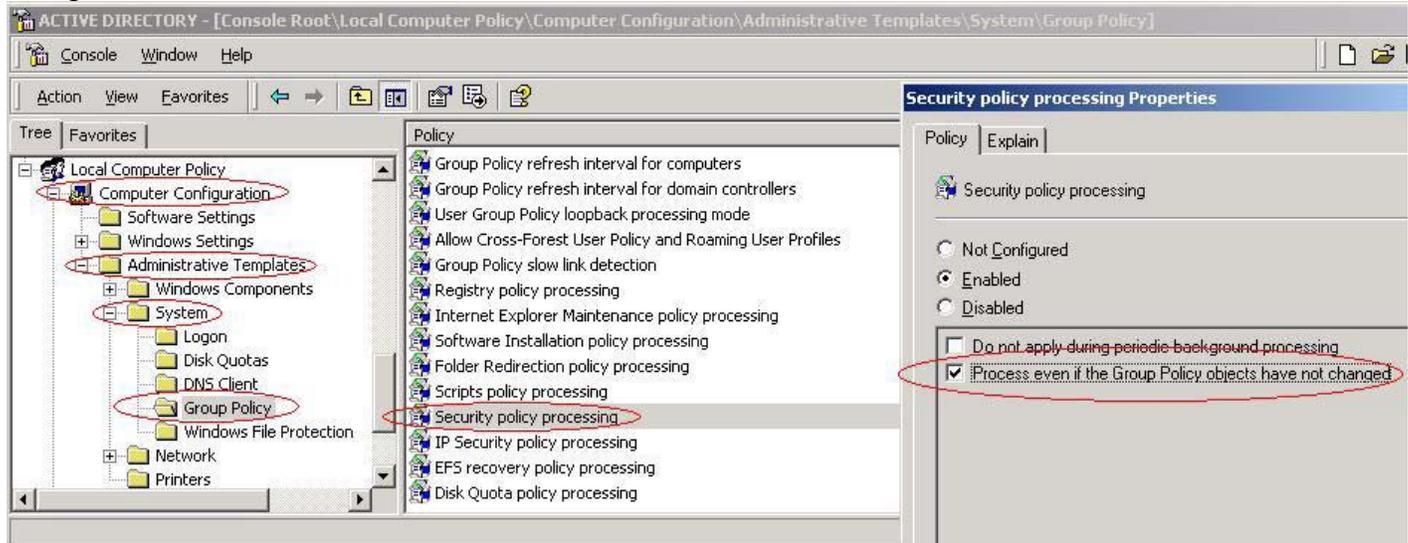
Configure the GPO to disable the Enforce Show Policies Only setting.

Answer: D

Explanation:

The "Process even if the Group Policy objects have not changed" option updates and

reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.



Reference:

HOW TO: How to Modify the Default Group Policy Refresh Interval, Microsoft Knowledge Base Article - Q203607

Incorrect Answers

A: This is an awkward indirect way of applying security templates. Also most of the time users do not have enough permissions to use the secdit command.

B: The Group Policy refresh interval for computers is used to modify the refresh and offset intervals settings. Is not used to enable a setting.

C: Loopback processing mode is used to establish machine-specific settings, so that the computer's client settings take precedence. It does not fit in this scenario.

E: The Enforce Show Policies Only policy prevents administrators from viewing or using Group Policy preferences. If we disable it administrators will be able to view and use Group Policy preferences. This does not address the problem at hand.

QUESTION 56:

You are a network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The network contains 100 Windows 2000 Server computers that are configured as file servers and 5 Windows 2000 Server computers that are configured as application servers.

The written security policy for Certkiller requires customized file security settings for all file servers. You create a security template named Files.inf and configure the template to contain settings that comply with the written policy. You create a Group Policy object (GPO) named FileServerSec and link it to the FileServers organizational unit (OU). You import the Files.inf security template to the FileServerSec GPO.

The next day, you discover that another administrator accidentally linked the FileServerSec GPO to an OU named AppServers. AppServers contains application

servers used by all company employees. As a result, no users can access the application servers. The administrator had already unlinked the GPO from the AppServers OU, but the application servers are still not functioning correctly. You need to restore functionality to the application servers. What should you do?

- A. Remove each application server from the domain, and then add the server to the domain.
- B. Create a GPO and link it to the AppServers OU. Then, import the Defltsv.inf security template to the new GPO.
- C. Use the Security Configuration and Analysis console on each application server to import Files.inf and run an analysis. Clear the check box for each policy that the analysis shows is applied.
- D. On each application server, run the `secedit /refreshpolicy machine_policy /enforce`.

Answer: D

Explanation: If you unlink a GPO, all of the sites, the domains, and the organizational units to which the GPO is linked no longer have those Group Policy settings applied to them. We use `secedit` to make sure that the current Group Policies are applied.

Reference:

HOW TO: Administer GPOs in Windows 2000, Microsoft Knowledge Base Article - Q322143

Using Secedit.exe to Force Group Policy to Be Applied Again, Microsoft Knowledge Base Article - Q227448

Incorrect Answers

- A: Removing and adding the servers from the domain would not do much good.
- B: The Defltsv.inf security template restores the default settings for NTFS permissions, registry permissions, default user rights, etc. It is not necessary to use it however. We only need to re-evaluate and apply the group policies.
- C: This would be an awkward and time consuming process.

QUESTION 57:

You are a network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 3,000 Windows 2000 Professional computers and an organizational unit (OU) named Research. The Research OU contains a child OU named Managers.

You move the computer accounts for all managers' computers in the research department to the Managers OU. You move the computer accounts for all other research department employees' computers to the Research OU.

The security administrators for Certkiller provide a new security template that must be applied to all computers in the research department, including the computers used by department managers. You create a Group Policy object (GPO) named Sec CertK Template and link it to the Research OU. Sec CertK Template is configured

with the default permission. You import the security template to the Sec CertK Template GPO. No other custom GPOs are currently used in your domain.

The Sec CertK Template GPO is correctly applied to the computers in Research OU. However, you discover that the computers used by research department managers are not being affected by the new security template. You need to ensure that the template is applied to all computers in the research department.

What should you do? (Each correct answer presents a complete solution. Choose two)

- A. Link the Sec CertK Template GPO to the Managers OU.
- B. On all of the computers used by research managers, run the `secedit /refreshpolicy machine_policy` command.
- C. Move all research department user accounts to the Research OU.
- D. In the properties of the Sec CertK Template GPO, select the No Override check box.
- E. Grant the Domain Users group Full Control permission for the Sec CertK Template GPO.

Answer: B, D

Explanation:

D: We ensure that the GPO is applied by selecting No Override.

B: We make sure that the updated policy is applied with the `secedit /refreshpolicy machine_policy` command.

Incorrect Answers

A: The Managers OU is a child to the Research OU. Any GPO that is applied to the Research OU is also applied to the Managers OU. It is not necessary to link the GPO to both OUs. This would be considered a bad practice. Furthermore, most likely this would not help.

C: Moving would not address the problem and it is a bad practice not to use the OU structure.

E: Users do not need Full Control permission to the GPO. Furthermore, full permission would not address the problem.

QUESTION 58:

You are the network administrator for Certkiller. The network consists of a Windows 2000 Active directory domain. The domain contains a Windows 2000 Server computer named Certkiller 1 that is running Microsoft SQL Server. The domain also contains an organizational unit (OU) named CertK. Certkiller is the CertK OU. The written security policy for Certkiller requires that you create all Group Policy objects (GPOs) for the domain.

The administrator for the CertK OU is named Jack. Jack is responsible for the user accounts and computer accounts in the OU. Jack submits a list of configurations that he wants to be applied to Certkiller in the CertK OU by means of a GPO. You create a GPO that complies with Jack's request.

You want to give Jack the ability to link the GPO to the CertK OU, but you need to

ensure that Jack cannot create GPOs.
What should you do?

- A. Add Jack's user account to the Group Policy Creator Owners group.
- B. Run the Delegation of Control wizard on the CertK OU and assign Jack's user account the Manage Group Policy links task.
- C. Move Jack's user account to the North OU.
- D. Configure the permissions on the GPO so that Jack's account has Read and Apply Group Policy permissions.

Answer: B

Explanation:

The Manage Group Policy links common task common task assigns the delegate(s) the permission to edit, add or delete Group Policy links of the selected Organizational Unit. We use the Delegation of Control wizard to assign the appropriate permissions to Bruno.

Reference:

Step-by-Step Guide to Using the Delegation of Control Wizard

HOW TO: Delegate Authority for Editing a Group Policy Object (GPO), Microsoft Knowledge Base Article - Q221577

Incorrect Answers

A: As a member of the Group Policy Creator Owners Bruno would be able to create GPOs.

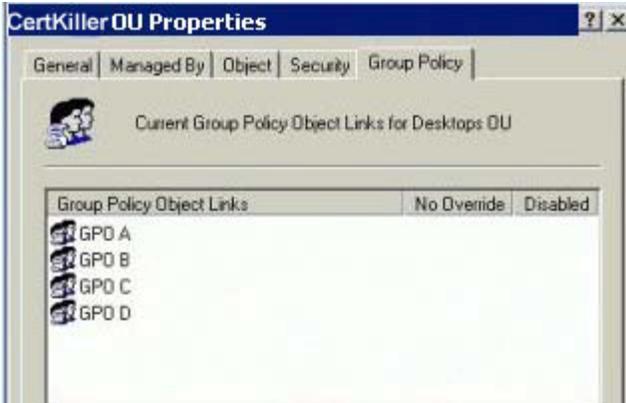
C: Moving the user account to the OU would not automatically give the user account any permissions or rights.

D: Read and Apply Group Policy permissions would ensure that GPOs in the OU would apply to Bruno. However, it would allow Bruno to link GPOs to the OU.

QUESTION 59:

You are the network administrator for Certkiller International. The network consists of a Windows 2000 Active Directory domain. The domain contains five Windows 2000 Server domain controllers and 20 Windows 2000 Professional computers. The computer accounts for all client computers are contained in an organizational unit (OU) named Certkiller .

Four Group Policy objects (GPOs) are linked to the Certkiller OU. The Certkiller OU properties are configured as shown in the following exhibit.



The administrator of the Certkiller OU customizes each GPO by using several settings and a different security template, as shown in the following table.

Group Policy object	Policy	Policy setting
GPO A	Maximum security log size	8,000 KB
GPO B	Maximum security log size	20,032 KB
GPO C	Maximum security log size	6,016 KB
GPO D	Maximum security log size	8,000 KB

On average, the security logs increase by 1,000 KB per day. When you inspect the logs on one of the desktops, you find that approximately eight days of security logs are being retained. You want to retain approximately 20 days of security log settings.

What should you do?

- A. Make GPO B the highest in the GPO list.
- B. Make GPO B the lowest in the GPO list.
- C. Create a new domain security group and add the users of the desktops to the new group. Grant the security group Read and Apply Group Policy permissions on GPO B.
- D. Create a new domain security group and add the desktop computers to the new group. Grant the security group Read and Apply Group Policy permissions on GPO B.

Answer: A

Explanation:

GPO's are applied bottom to top, meaning that the GPO at the top would be applied last. GPO B must be applied last so that it is not overridden.

Note: If you have more than one GPO associated with an Active Directory folder, verify the GPO order; a GPO that is higher in the list has the highest precedence. Note that GPOs higher in the list are processed last (this is what gives them a higher precedence). GPOs in the list are objects; they have context menus that you use to view the properties

of each GPO. You can use the context menus to obtain and modify general information about a GPO. This information includes Discretionary Access Control Lists (DACLS, which are covered in the Security Group Filtering section of this document), and lists the other site, domain, or OUs to which this GPO is linked."

Reference:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/g>

Incorrect Answers

B: If we move GPO B lowest in the GPO list it would be applied first and would still be overridden.

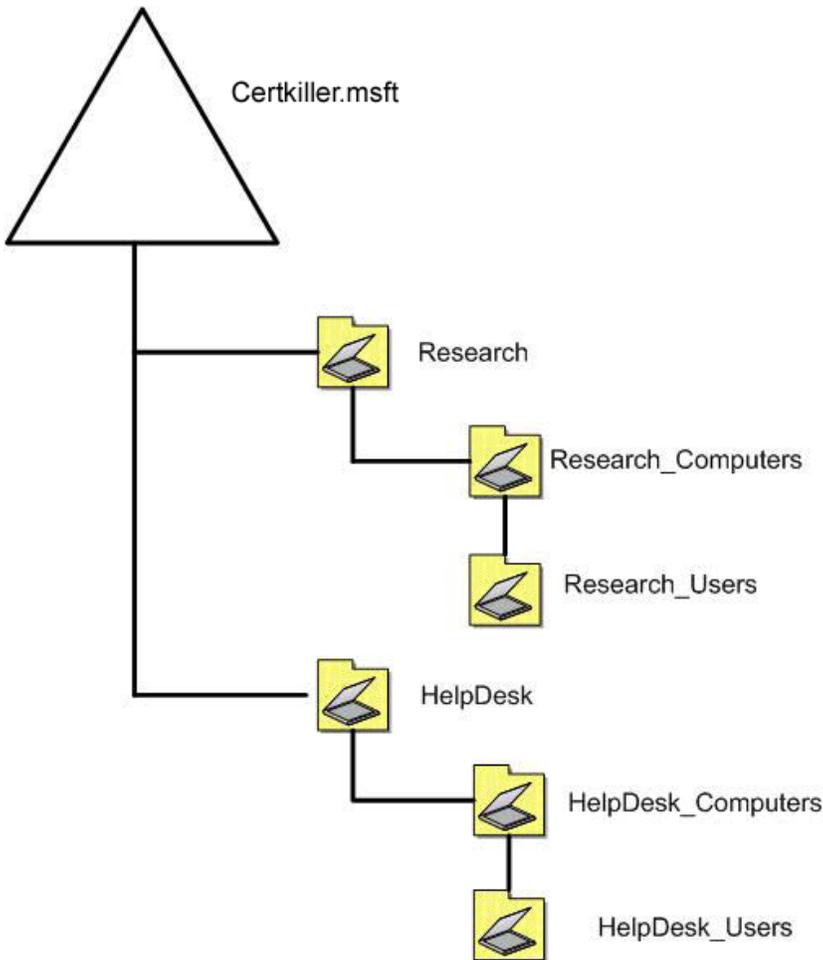
C: Read and Apply Group Policy permissions would enable the GPO to be applied to the Group. However, the GPO should be applied to the computer. Furthermore, the GPO is applied already, it just overridden.

D: Read and Apply Group Policy permissions would enable the GPO to be applied to the Group. However, the GPO is applied already, it just overridden.

QUESTION 60:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains two Windows 2000 domain controllers and 500 Windows Professional computers.

The relevant portion of the Active Directory hierarchy is shown in the exhibit.



The user accounts for all employees in the Technical Support department are located in the HelpDesk_Users organizational unit (OU). The client computer accounts for these employees' computers are located in the HelpDesk_Computers OU. All other user accounts are located in the Research_Users OU. All other client computer accounts are located in the Research_Computers OU.

You create a Group Policy object (GPO) named GPO1 and link it to the Research_Computers OU. You configure the GPO1 as shown in the following table.

Policy or Setting	Status
Do not display last user name on logon screen	Enabled
Disable Computer Configuration Settings	Selected
Disable User Configuration Settings	Cleared

Another administrator moves a user account named Jack to the Research_Computers OU. You notice that Jack's computer displays another user's name in the logon dialog box. You need to ensure that the name of the last user to

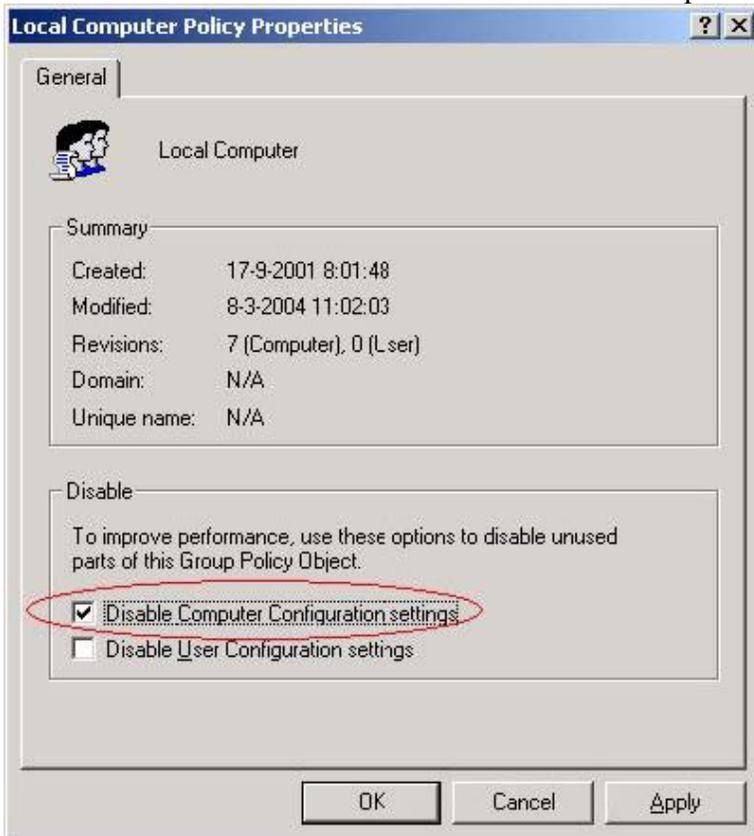
log on does not appear in the logon dialog box when Jack logs on to her computer. What should you do?

- A. Move Jack's user account to the Research_Users OU.
- B. Clear the Disable Computer Configuration Settings check box in GPO1.
- C. Disable the Do not display last user name in logon screen policy in GPO1.
- D. Run the `secedit /refreshpolicy user_policy /enforce` command on Maria's client computer.

Answer: B

Explanation:

After you disable the Computer Configuration settings in a Group Policy object, by selecting Disable Computer Configuration Settings, the computers configuration no longer affect. This is the reason the Do not display last user name on logon screen policy is not used. We must therefore clear the Disable Computer Configuration Settings setting.



Reference:

HOW TO: Administer GPO Properties in Windows 2000, Microsoft Knowledge Base Article - Q322176

Using Secedit.exe to Force Group Policy to Be Applied Again, Microsoft Knowledge Base Article - Q227448

Incorrect Answers

A: Moving Maria's user account is not necessary. We only need to adjust the GPO.

C: The Do not display last user name in logon screen is already correctly configured in

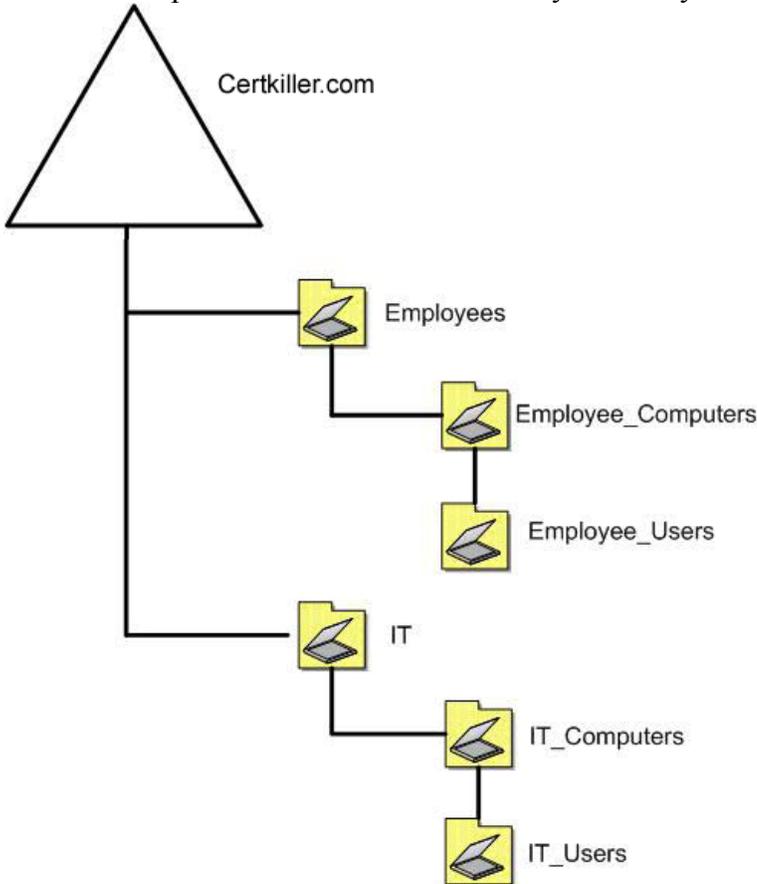
GPO1. We should not disable this policy.

D: The GPO is already applied, it must be reconfigured however.

QUESTION 61:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain Certkiller .com. The domain contains Windows 2000 Server computers and Windows 2000 Professional computers. All domain controllers run Windows 2000 Server.

The relevant portion of the Active Directory hierarchy is shown in the exhibit.



The written security policy for Certkiller requires that only network administrators have administrative capabilities on the domain controllers and member servers in the domain. An administrator's user account must not have administrative capabilities on any client computer in the domain, including the administrator's own client computer.

A Group Policy object (GPO) named Secure_lockdown is linked to the IT_Users OU and the Employee_Users OU. The Secure_lockdown GPO removes many Start menu options and does not give the users access to Control Panel utilities.

Administrators report that they cannot view all Start menu options when they log on to their client computers by using their domain user accounts.

You need to ensure that the administrators have access to all Start menu options and Control Panel utilities on their client computers but not on other client

computers in Certkiller .
What should you do?

A. Create a group named IT_staff.

Add each administrator's user account to the IT_staff group.

In the Default Domain Policy GPO, add the Administrators group under the Restricted Groups policy.

Add the IT_staff group to the member list in the Administrators group.

B. Create a group named IT_staff.

Add each administrator's user account to the IT_staff group.

Run the Delegation of Control wizard for the IT_Computers OU.

Grant the IT_staff group Full Control permission for the Computer objects.

C. Create a GPO and link it to the IT_Users OU.

In the computer configuration section of the GPO, set the loopback processing policy to Replace.

In the user configuration section of the GPO, configure Start menu options and Control Panel utilities to be accessible.

D. Create a GPO and link it to the IT_Computers OU.

In the computer configuration section of the GPO, set the loopback processing policy to Replace.

In the user configuration section, configure Start menu options and Control Panel utilities to be accessible.

Answer: D

Explanation:

Applies alternate user policies when a user logs on to a computer affected by this policy.

This policy directs the system to apply the set of Group Policy objects for the computer to any user who logs on to a computer affected by this policy. It is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user policy based on the computer that is being used.

By default, the user's Group Policy objects determine which user policies apply. If this policy is enabled, then, when a user logs on to this computer, the computer's Group Policy objects determine which set of Group Policy objects applies.

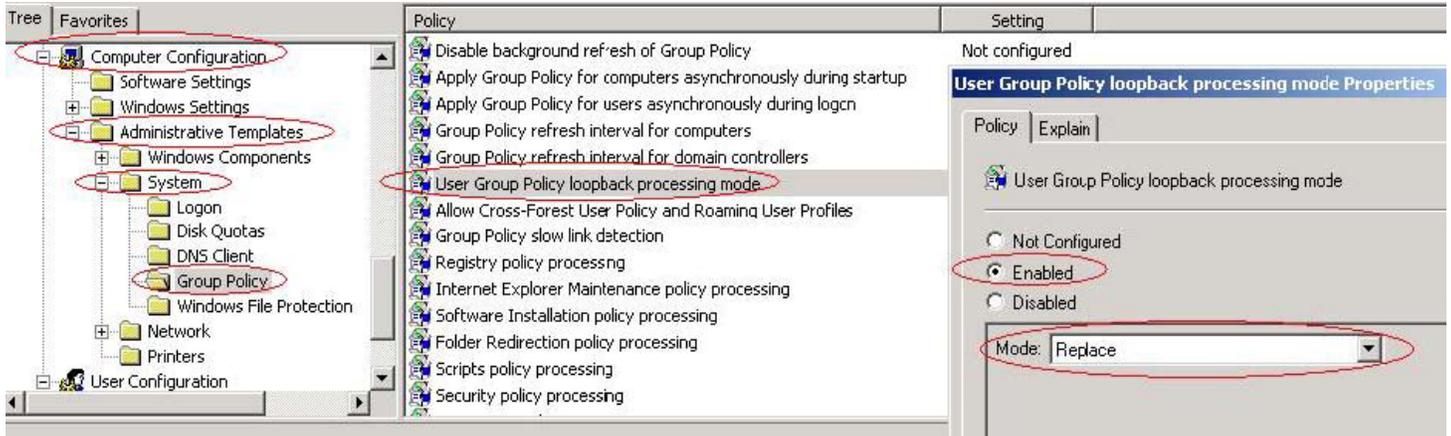
To use this policy, select one of the following policy modes from the Mode box:

-- "Replace" indicates that the user policies defined in the computer's Group Policy objects replace the user policies normally applied to the user.

-- "Merge" indicates that the user policies defined in the computer's Group Policy objects and the user policies normally applied to the user are combined. If the policy settings conflict, the user policies in the computer's Group Policy objects take precedence over the user's normal policies.

If you disable this policy or do not configure it, the user's Group Policy objects determines which user policies apply.

Note: This policy is effective only when both the computer account and the user account are in Windows 2000 domains.



In this scenario we want to apply special options, the availability of the Start menu options and Control Panel utilities, for the Administrators on the IT computers.

Reference:

Loopback Processing of Group Policy, Microsoft Knowledge Base Article - Q231287

Description of Group Policy Restricted Groups, Microsoft Knowledge Base Article - Q279301

Incorrect Answers

A: The Restricted Groups policy is used to control the members of the Administrators group. This does not address the problem of this scenario.

B: This would give the administrators full administrative to the computers in the IT_Computers OU. However, this is not related to the requirements of this scenario.

C: Loopback Processing is applied on computers, not on users.

QUESTION 62:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The network contains two Windows 2000 Server computers configured as domain controllers, 100 Windows 2000 Professional client computers, and 100 Windows 98 client computers, All Windows 98 Second Edition client computers have the Microsoft Directory Services Client installed and are configured with the appropriate LMCompatibilityLevel registry value.

Certkiller has three departments: research, sales, and operations. Each department has a separate organizational unit (OU) in the domain that contains all user and group accounts for that department.

The written security policy for Certkiller requires that domain controllers authenticate user logons only by using the most secure Microsoft authentication method available to all clients on the network. You review the Security Options portion of the security template for the domain. The following table shows the relevant Security Options settings in the template.

Policy	Computer settings
Lan Manager Authentication Level	Send NTLM response only

Message text for users attempting to log on	Not defined
Message title for users attempting to Log on	Not defined
Number of previous logons to cache (in case domain controllers is not available)	1 logons

You must ensure that no Windows 98 client computer can authenticate with the domain controller by using anything less than the most secure authentication method available.

What should you do?

A. Configure the Lan Manager Authentication Level on the security template to Not defined.

Import the template into the Domain Controllers Security Policy.

B. Configure the Lan Manager Authentication Level on the security template to Send NTLMv2 response only\refuse LM & NTLM.

Import the template into the Domain Security Policy.

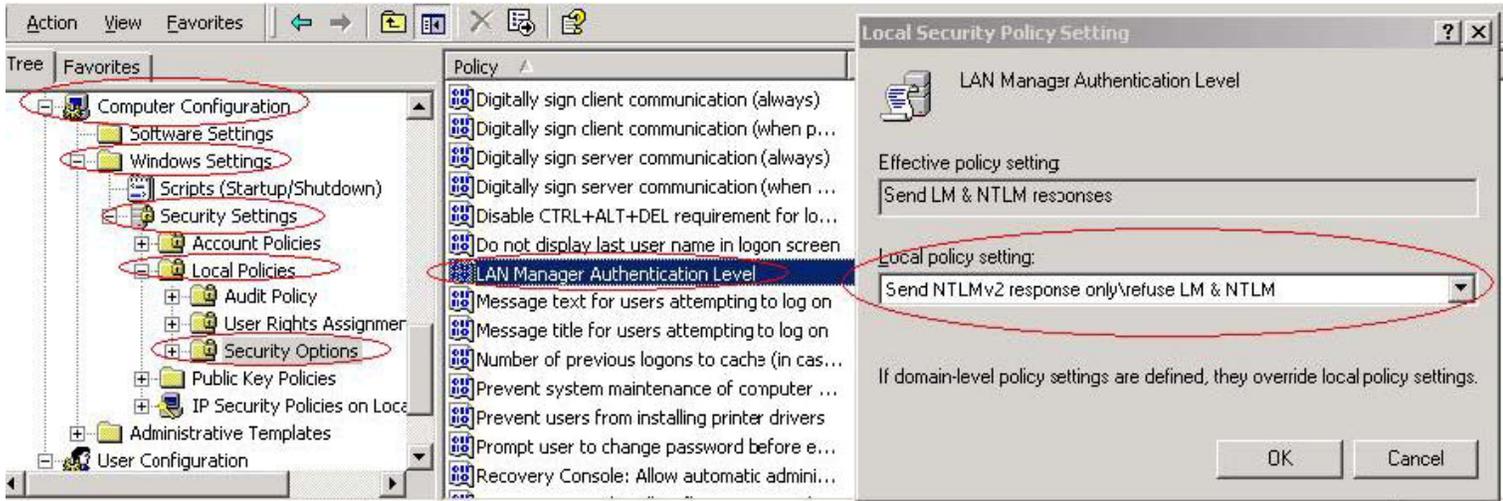
C. Configure the Default Domain Policy Group Policy object (GPO) to enable the Digitally encrypt secure channel data (when possible) setting in the Secure Options policy.

D. Configure the Default Domain Controllers Policy Group Policy object (GPO) to enable the Digitally encrypt or sign secure channel data (always) setting in the Secure Options policy.

Answer: B

Explanation:

NTLM 2 is the most secure LAN Manager authentication level. NTLM2 support to Windows 95 and Windows 98 can be added by installing the Directory Services Client from the Windows 2000 CD-ROM. This step has been taken in this scenario. By enforcing use of NTLMv2 we would ensure that the most secure authentication method is available.



Note: The LAN Manager authentication level determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers. The NTLM authentication package in Windows 2000 supports three methods of challenge/response authentication: LAN Manager (LM) which is least secure, NTLM version 1, NTLM version 2 which is the most secure.

By default, all three challenge/response mechanisms are enabled. You can disable authentication using weaker variants by setting the LAN Manager authentication level security option in local security policy for the computer.

Reference:

How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT, Microsoft Knowledge Base Article - Q239869

Incorrect Answers

A: A Lan Manager Authentication Level of Not defined would enable LAN Manager (LM) authentication which is least secure authentication method.

C: The Digitally encrypt secure channel data (when possible) setting is enabled, it ensures that all secure channel traffic is encrypted if the partner domain controller is also capable of encrypting all secure channel traffic. However, it allows unencrypted data. Furthermore it only applies to communication between domain controllers.

D: The Digitally encrypt or sign secure channel data (always) setting determines whether a secure channel can be established with a domain controller that is not capable of signing or encrypting all secure channel traffic. If this setting is enabled, a secure channel cannot be established with any domain controller that cannot sign or encrypt all secure channel data. It only applies to communication between domain controllers and is therefore useless in this scenario.

QUESTION 63:

You are the network administrator for Certkiller . The network consists of a Windows NT 4.0 domain. The domain has a Windows NT 4.0 PDC and 20 Windows NT 4.0 BDCs. All domain controllers use the latest service pack. Currently, all the 1,800 client

computers in the domain run Windows 2000 Professional.

You plan to upgrade the domain to Windows 2000. You plan to upgrade all the domain controllers to Windows 2000 domain controllers during a period of three weeks.

Before you upgrade the first domain controller to Windows 2000, you want to ensure that the Windows 2000 Professional client computers in the domain continue to use the Windows NT 4.0 domain controllers for authentication and not just the new Windows 2000 domain controllers.

What should you do?

- A. Manually add the DNS SRV (service) records of all the domain controllers to the DNS server on the network.
- B. Add the computer accounts of all the domain controllers to a group named Pre-Windows 2000 Compatible Access.
- C. Configure all the domain controllers to use NT4 emulation mode.
- D. Install the Microsoft Directory Services client on all remaining Windows NT 4.0 domain controllers.
- E. Disable the use of LAN Manager (LM) authentication on the remaining Windows NT 4.0 domain controllers.

Answer: C

Explanation:

After Windows 2000- and Windows XP-based computers join an Active Directory domain, they will not use a Windows NT 4.0-based domain controller (DC) for any operation that requires them to contact the DC. Therefore, all of the computers that run Windows 2000 or Windows XP contact only the lone Windows 2000- or Windows .Net Server-based DC.

The solution enables special configuration to make a DC emulate the behavior of a Windows NT 4.0-based DC. The domain member computers that run Windows 2000 or Windows .Net Server does not distinguish between a DC that is in Windows NT 4.0 (NT4) emulation mode and a DC that runs Windows NT 4.0. This configuration prevents overloading of the first DC that you upgrade to Windows 2000 SP2 or Windows .Net Server.

Reference:

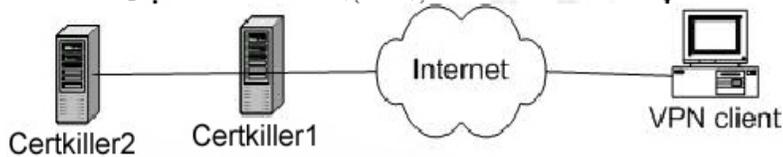
How to Prevent Overloading on the First Windows 2000- or Windows XP-Based DC During Domain Upgrade, Microsoft Knowledge Base Article - Q298713

QUESTION 64:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. A Windows 2000 Server computer named Certkiller 1 is located at the network perimeter. Certkiller 1 runs Microsoft Internet Security and Acceleration (ISA) Server and accepts PPTP connections from traveling users of the network.

Another Windows 2000 Server computer, named Certkiller 2, is located on the LAN and

runs the Internet Authentication Service (IAS). Certkiller 1 is configured as a Remote Authentication Dial-in User Service (RADIUS) client of Certkiller 2. The virtual private network (VPN) infrastructure components are shown in the exhibit.



The written security policy for Certkiller requires that the RADIUS authentication and accounting packets be encrypted. You create a custom IPsec policy and assign the policy in the Local Security Policy of both Certkiller 1 and Certkiller 2.

You must ensure that only the RADIUS traffic is encrypted. What should you do?

- A. Configure the custom IPsec policy to encrypt data sent from the VPN client to Certkiller 2 with default RADIUS ports as the destination ports. Implement IPsec transport mode in the custom IPsec policy.
- B. Configure the custom IPsec policy to encrypt data sent from the VPN client to Certkiller 2 with default RADIUS ports as the destination ports. Implement IPsec tunnel mode in the custom IPsec policy, with Certkiller 1 configured as the tunnel endpoint.
- C. Configure the custom IPsec policy to encrypt data sent from Certkiller 1 to Certkiller 2 with default RADIUS ports as the destination ports. Implement IPsec transport mode in the custom IPsec policy.
- D. Configure the custom IPsec policy to encrypt data sent from Certkiller 1 to Certkiller 2 with default RADIUS ports as the destination ports. Implement IPsec tunnel mode in the custom IPsec policy, with Certkiller 2 configured as the tunnel endpoint.

Answer: C

Explanation:

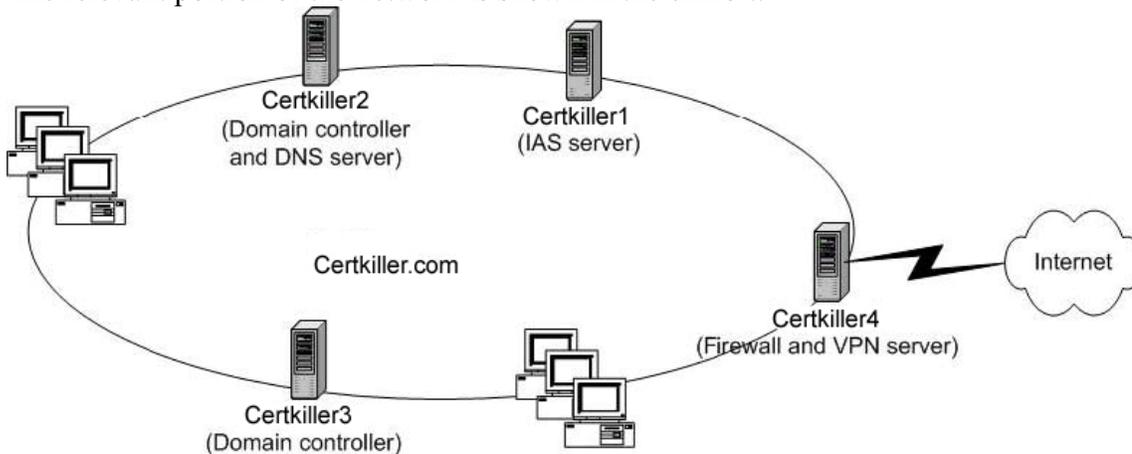
IPsec can be configured for either transport or tunnel mode. The transport mode authenticates and encrypts data moving between computers. This is the default mode for IPsec in Windows 2000. Unlike transport mode, which secures the packet from the source to the destination, tunnel mode places a secure, existing packet inside a new IP packet that is sent to a tunnel endpoint. The tunnel endpoint is probably not the final destination of the inside packet, but it is the final destination of the outside packet. The outside packet is stripped off at the tunnel endpoint and the internal packet can be further routed to the final destination. Tunnel mode does not provide security within each network that the packet will traverse. It simply provides security to the packet itself and guarantees that security to the endpoint (IP address) that you specify.

RADIUS messages are sent with the User Datagram Protocol (UDP) User Datagram Protocol (UDP) A Transmission Control Protocol (TCP) complement that offers a connectionless datagram service that guarantees neither delivery nor correct sequencing of delivered packets (much like Internet Protocol (IP))... UDP port 1812 is used for RADIUS authentication messages and UDP port 1813 is used for RADIUS accounting

messages. When you create inbound and outbound filters with IPSec, UDP traffic must be allowed on these ports. However, some network access servers might use UDP port 1645 for RADIUS authentication messages and UDP port 1646 for RADIUS accounting messages. By default, IAS supports both sets of ports. If your network access servers use UDP ports 1645 and 1646, you can create IPSec filters that allow traffic on these ports.

QUESTION 65:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains an Internet Authentication Service (IAS) server named Certkiller 1. All client computers run Windows XP Professional. The relevant portion of the network is shown in the exhibit.



You are deploying a new 802.11a high-speed wireless LAN. The wireless LAN will use Wired Equivalent Privacy (WEP) for all connections. You have enabled MAC Filtering on all wireless access points.

Another administrator configures Certkiller 1 to include a remote access policy that allows EAP-TLS wireless connections to the network. That administrator also distributes user certificates to all wireless users.

You want to ensure that only domain users can connect to the wireless LAN. You also want to ensure that client computers do not connect to the wireless LAN when a user is not logged on to the computer.

What should you do?

- A. Ensure that 802.1x network access control is enabled on client computers. Clear the Authenticate as computer when computer information is available option and configure the EAP type as Smart Card or other Certificate. Configure all wireless access points as Remote Authentication Dial-in User Service (RADIUS) clients that use Certkiller 1 as the RADIUS server.
- B. Select Network authentication (Shared Mode) and specify a 104-bit key length. Select the Authenticate as computer when computer information is available option and deploy smart cards to all wireless users.
- C. Ensure that 802.1x network access control is enabled on client computers. Select the Authenticate as computer when computer information is available option and configure the EAP type as Smart Card or other Certificate.

Configure all wireless access points as Remote Authentication Dial-in User Service (RADIUS) clients that use Certkiller 1 as the RADIUS server.

D. Select Network authentication (Shared Mode) and specify a 104-bit key length. Clear the Authenticate as computer when computer information is available option and deploy smart cards to all wireless users.

Configure the wireless access points as Remote Authentication Dial-in User Service (RADIUS) clients that use Certkiller 1 as the RADIUS server.

Answer: A

Explanation:

The IEEE (Institute of Electrical and Electronics Engineers) 802.1x standard is the next big step in wireless security. This standard manages and controls access to the wireless network using Extensible Authentication Protocol Over LANs (EAPOL) in combination with Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol with Transport Layer Security (EAP-TLS), Kerberos, or Message Digest 5. The 802.1x standard is not just for wireless implementations; it can also be used for LAN-based devices. Windows XP Professional is the only client that fully supports 802.1x. Windows 2000 Professional cannot use the features at this time.

The 802.1x standard is a great step forward for security; however, setting it up requires some extensive resources and a Private Key Infrastructure (PKI) to provide the certificates. The necessary resources include the following:

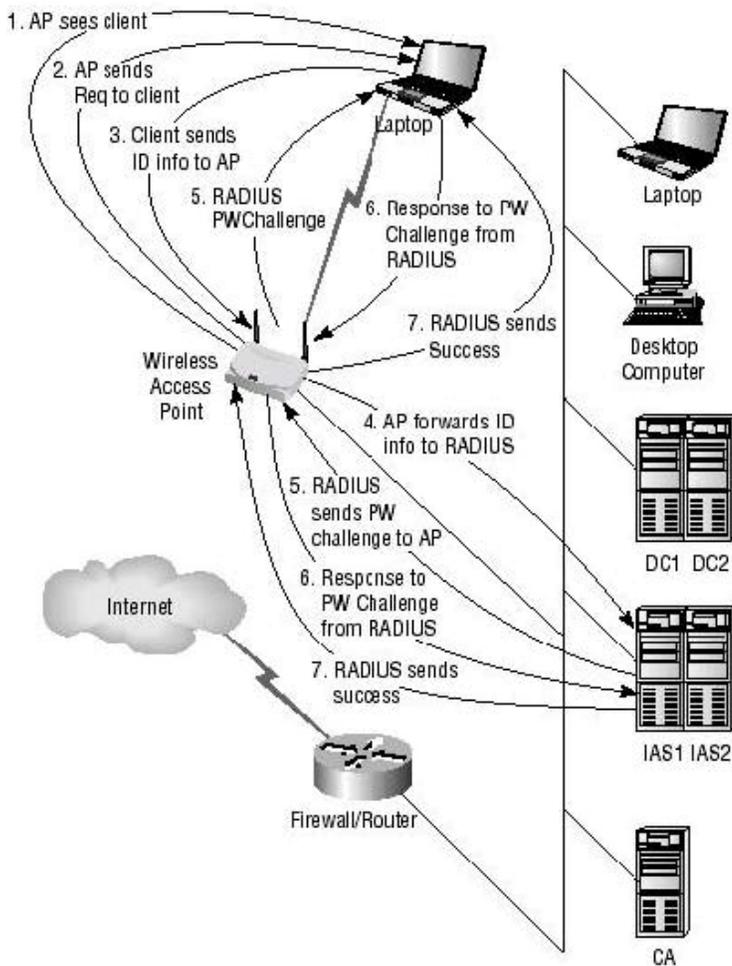
- * Wireless clients such as Windows XP Professional that support 802.1x
- * Active Directory running on Windows 2000 Server, SP3
- * A Certificate Authority
- * A remote access policy for wireless clients
- * RADIUS servers

In the next figure you can see the additional infrastructure needed to make this all work. DC1 and DC2 are the Active Directory domain controllers (you want at least two for redundancy),

IAS1 and IAS2 are the Internet Authentication Servers (again, two for redundancy) that will be used for RADIUS, and CA is the Certificate Authority.

The main goal of 802.1x is to securely authenticate clients associating with APs and to exchange encryption keys. The process is somewhat confusing, but it can be clarified a bit, see the figure for the visual of the process; the steps are outlined here

- * (1) The AP sees that a client exists on the network and initiates contact. Access is blocked by the AP until authentication is completed by the client. If authentication fails, no data is ever forwarded onto the wired network.
- * (2) The AP sends an EAPOL-encapsulated EAP Request-ID to the client.
- * (3) The client sends an EAPOL-encapsulated EAP Response-ID message that contains the user's identification information to the AP.
- * (4) The AP then forwards this EAP Response-ID by encapsulating it in a RADIUS access request packet and sending it to a RADIUS server. This could be either IAS1 or IAS2.



* (5) The RADIUS server responds with an EAP-Request, encapsulated in a RADIUS packet, that contains a password challenge for the client, and it is forwarded by the AP to the client after the AP encapsulates it using EAPOL.

* (6) The client responds to the challenge with EAPOL-encapsulated response information that is sent to the AP and then forwarded to the RADIUS server in an encapsulated RADIUS packet.

* (7) The RADIUS server responds with a RADIUS-encapsulated EAP success message to the AP. The AP then forwards this EAP success message to the client encapsulated with EAPOL.

Once all these steps have taken place, the client is considered properly authenticated and can

start transmitting data on the wireless network to the wired network. In this exchange, all traffic between the client and the AP is encapsulated using EAPOL. All traffic between the AP and the IAS (RADIUS) servers is encapsulated using RADIUS.

EAP-TLS is the default EAP type. TLS is intended for wired networks, but can also be used

in wireless environments. Using TLS requires that that RADIUS server and the client both

have certificates and that both devices have the certificates residing within a trusted CA.

In

order for the client to get a certificate for use with wireless access, though, it must first have

wired access to the CA to make the request and then apply the certificate.

Incorrect Answers:

B,D: We must use EAP-TLS so we must use RADIUS Clients

C: If the Enable IEEE 802.1x Authentication For This Network check box is checked and the AP is not set to use 802.1x or does not support it, the client will not be prevented from properly accessing the AP and participating in the wireless network. If the Enable IEEE 802.1x Authentication For This Network Enable =802.1x check box is cleared and the AP is enforcing 802.1x authentication, the client will not connect.

QUESTION 66:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active directory domain Certkiller .local. The Web developers at Certkiller use portable computers, which are members of the domain. These computers run Windows XP Professional and Internet Information Services (IIS). The developers use IIS to create Web applications for Certkiller .

A developer reports that his computer becomes infected with a virus every time he uses the computer at home. Certkiller 's anti-virus software successfully removes the virus each time the problem occurs.

You discover that the developer uses a USB network adapter to connect his computer to a cable modem when he works at home. You also discover that the same virus infects the computer each time by attacking IIS.

You need to prevent the virus from infecting the developer's computer and allow the developer to use the computer normally while working at home.

How should you configure the developer's computer?

- A. Modify the Remote Desktop permissions list so that only the local Administrator account is listed.
 - B. Disable Internet Connection Sharing for all network connections.
 - C. Enable the Internet Connection Firewall for the network connection used to connect to the developer's cable modem.
 - D. Create a Group Policy object (GPO) and link it to the organizational unit (OU) that contains the developer's computer.
- Configure the GPO to disable the World Wide Web Publishing service.
In the GPO, select the No Override check box.

Answer: C

Explanation:

The local computer can be protected by enabling the Internet Connection Firewall for the cable modem connection.

Incorrect Answers

A: Remote Desktop does not apply to this scenario.

B: Internet Connection Sharing does not apply to this scenario.

D: The developer must be able to work as normal at home. He must use the IIS Web Publishing Service in order to test his applications.

QUESTION 67:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain.

Certkiller has several sales employees who travel with Windows XP portable computers. To check their e-mail and upload data, the sales employees must dial in to Certkiller 's network using a toll-free number.

The network includes a stand-alone Windows 2000 Server computer named Certkiller 1, which runs Routing and Remote Access. Certkiller 1 is configured to allow PPTP connections to the network. Certkiller 1 is installed at the network perimeter. Employees who work from home connect to Certkiller 1 to gain access to Certkiller network.

You company wants to reduce long-distance charges by finding a cheaper solution. A national Internet service provider (ISP) has a calling plan that will provide local phone number Internet access for all cities the sales employees work in. The same phone numbers are used by all companies who subscribe to the service. Certkiller purchases the plan, and you configure the portable computers to use a local phone number and PPTP to connect to the corporate network.

You must develop a solution that allows users to use a single password when connecting to the ISP and the corporate network. First you install the Internet Authentication Service (IAS) on a server on the network of Certkiller to act as a Remote Access Dial-in User Service (RADIUS) server.

What else should you do?

A. Ask the ISP to configure a RADIUS client to forward authentication requests to the IAS server on your network.

Configure Certkiller 1 to use Windows Authentication, with Certkiller 1 providing authentication.

B. Ask the ISP to configure a RADIUS proxy to forward authentication requests to the IAS server on your network.

Configure Certkiller 1 to use Windows Authentication, with Certkiller 1 providing authentication.

C. Ask the ISP to configure a RADIUS client to forward authentication requests to the IAS server on your network.

Configure Certkiller 1 to use RADIUS Authentication, with the IAS server on your network providing authentication.

D. Ask the ISP to configure a RADIUS proxy to forward authentication requests to the IAS server on your network.

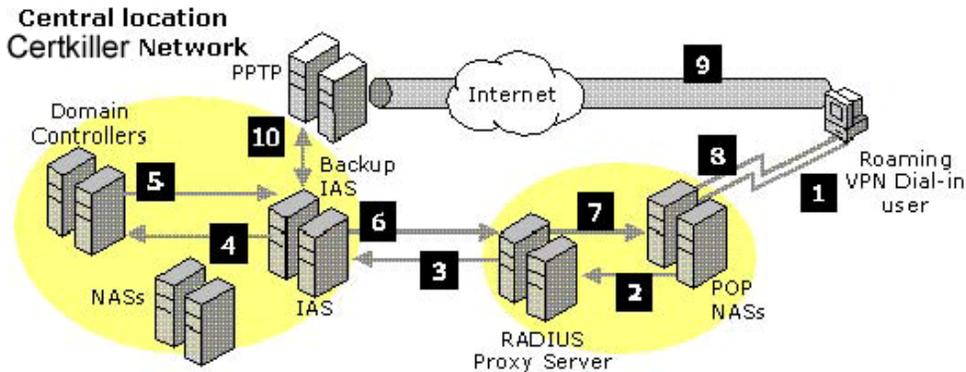
Configure Certkiller 1 to use RADIUS Authentication, with the IAS server on your network providing authentication.

Answer: D

Explanation:

Requests reach IAS through the RADIUS proxy server at the ISP and are routed to the corporate server. We should configure Certkiller 1 to use RADIUS authentication. The IAS server provides the authentication.

Illustrative diagram:



Reference:

Microsoft White Paper, Internet Authentication Service for Windows 2000, Outsourced Corporate Access Through Service Providers

Incorrect Answers

A, C: At the ISP a RADIUS proxy server that acts as a RADIUS client to other servers is needed.

B; Windows authentication could be used if there were only one single RRAS server. However, in this scenario there is an RRAS and an IAS server.

QUESTION 68:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. When the first domain controller in the domain was installed, permissions were defined to be compatible only with Windows 2000 Server operating systems.

Three servers accept dial-up remote access connections for the network. Certkiller 1 is a Windows NT Server 4.0 computer with the latest security updates and Routing and Remote Access for Windows 2000 add-in installed. Certkiller 1 also runs an accounting software package that does not run under Windows 2000.

Certkiller 2 and Certkiller 3 are Windows 2000 Server computers with Routing and Remote Access configured to allow dial-up connections.

At Certkiller 2 and Certkiller 3, the configured Remote Access Policy allows dial-up connections by all users. To allow dial-up connections to Certkiller 1, users who are allowed to dial in to the network are enabled for remote access in their user account properties.

All three servers allow CHAP, MS-CHAP, and MS-CHAP v2 authentication. Users report that they are sometimes unable to connect to the network. When they attempt to reconnect, the attempt often succeeds. Upon inspection of the event logs, you find that only dial-up connections to Certkiller 2 and Certkiller 3 are succeeding.

You must allow connections to Certkiller 1 without upgrading to Windows 2000 Server. What should you do?

- A. Install the Microsoft Directory Services Client on Certkiller 1.
- B. Install the Windows NT 4.0 High Encryption Pack on Certkiller 1.
- C. Add the Certkiller 1 Windows NT 4.0 computer account to the RAS and IAS Servers group.
- D. Add the Everyone group to the Pre-Windows 2000 Compatible Access group.

Answer: C

Explanation:

Users only get authenticated by the Windows 2000 RRAS servers, not by the Windows NT 4.0 RAS server. We need to add the Windows NT 4.0 RAS server to the RAS and IAS Servers group.

Procedure:

1. Log on to a Windows 2000 computer with an account that is a member of the Domain Administrators group.
2. Start the Active Directory Users and Computers MMC snap-in.
3. Navigate to <Your Domain Name> / Users / RAS and IAS Servers.
4. Right-click RAS and IAS Servers and press Properties.
5. Select the Members tab.
6. Add the RRAS server to the RAS and IAS Servers group.

Reference:

HOW TO: Add Users to the Pre-Windows 2000 Compatible Access Group, Microsoft Knowledge Base Article - Q303973

Incorrect Answers

A, B: Microsoft Directory Services Client or Windows NT 4.0 High Encryption Pack are not useful here.

D: By putting the Everyone group into the pre-Windows 2000 Compatible Access group enables any RAS caller to be authenticated by the Windows NT 4.0 RAS server.

However, this is not a solution to the problem in this scenario.

QUESTION 69:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

A Windows 2000 member server named Certkiller 1 hosts the corporate intranet Web site. Certkiller 1 runs Internet Information Services (IIS) 5.0.

All users are using Microsoft Internet Explorer as their default browser to connect to the intranet Web site. Currently, users in the domain connect to the intranet Web site by using Basic authentication.

You want to start using Digest authentication for the intranet Web site. You configure IIS on Certkiller 1 to allow only Digest authentication. In the Default Domain Group Policy object (GPO), you assign the Store passwords using reversible encryption for all users in the domain policy.

Users now report that when they connect to the intranet Web site, they are presented with a dialog box asking for a user name and passwords. However, no matter which user name and password combination they enter, they cannot access the site. After three connection

attempts, the Web browser displays the error message "HTTP 401.4 - Unauthorized: Authorization denied by filter."

You want to ensure that users in the domain can successfully authenticate to the intranet Web site by using Digest authentication.

What should you do?

- A. Add the intranet Web site to the Trusted Sites zone on each user's computer.
- B. Grant the Domain Users group the Log on locally user right on Certkiller 1.
- C. Configure all domain user accounts to enable the User must change password at next logon option.
- D. Configure IIS on Certkiller 1 to enable the Enable client certificate mapping option.

Answer: C

Explanation:

When you use Digest Authentication in Internet Information Services version 5.0, and a user navigates to your Web site, the following error message may be received by the user when they attempt to log in:

401.4 Unauthorized: Authorization denied by filter.

This error typically occurs because the user's password is either not stored in reversible encryption, or the password has not been reset (in order for the hashing to take place).

Reference: Error message: 401.4 Unauthorized: Authorization denied by filter, Microsoft Knowledge Base Article - Q241832

(<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B241832>)

Incorrect answers:

A: This doesn't have anything to do with if the site is trusted or not

B: Certkiller 1 is a domain member, so all domain users already have the Log on Locally user right by default.

D: This isn't a certificate issue, Digest Authentication does not use certificates. When you use Digest Authentication in Internet Information Services version 5.0, and a user navigates to your Web site, the following error message may be received by the user when they attempt to log in:

401.4 Unauthorized: Authorization denied by filter.

This error typically occurs because the user's password is either not stored in reversible encryption, or the password has not been reset (in order for the hashing to take place).

Reference: Error message: 401.4 Unauthorized: Authorization denied by filter, Microsoft Knowledge Base Article - Q241832

(<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B241832>)

Incorrect answers:

A: This doesn't have anything to do with if the site is trusted or not

B: Certkiller 1 is a domain member, so all domain users already have the Log on Locally user right by default.

D: This isn't a certificate issue, Digest Authentication does not use certificates.

QUESTION 70:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain with five Windows 2000 domain controllers. The other computers in the domain are 30 Windows 2000 member servers, 650 Windows 2000 Professional client computers, and 250 Windows XP Professional client computers. All domain controllers are members of the organizational unit (OU) named Domain Controllers. All servers are in an OU named Servers, and all client computers are in an OU named Clients.

The corporate security policy describes the following three encryption recommendations:

- * FTP traffic--Request Data Encryption Standard (DES) encryption
- * Terminal Services traffic--Request 3DES encryption
- * All other IP traffic--Permit

You want to ensure that all three encryption recommendations are implemented on all computers in the domain.

What should you do?

- A. Create a Group Policy object (GPO) and link it to the domain.
Configure the GPO with an IPsec policy that contains the three encryption recommendations.
- B. Create three Group Policy objects (GPOs) and link them to the domain.
Configure each GPO to have one of the encryption recommendations configured in an IPsec policy.
- C. Create a Group Policy object (GPO) and link it to the Domain Controllers, Servers, and Clients OUs.
Configure the GPO with an IPsec policy that contains the FTP and Terminal Services recommendations.
Create another GPO and link it to the domain.
Configure another GPO and link it to the domain.
Configure that GPO to have an IPsec policy that implements the recommendation to permit all other IP traffic.
- D. Create a Group Policy object (GPO) and link it to the Domain Controllers, Servers, and Clients OUs.
Configure the GPO with an IPsec policy that contains the FTP and Terminal Services recommendations.
Configure the local GPO on all computers to implement the recommendation to permit all other IP traffic.

Answer: A

Explanation:

We should configure only one GPO that implements the three encryption recommendations.

QUESTION 71:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional computers. All domain controllers run Windows 2000 Server.

You create an organizational unit (OU) named Clients and move all the client computer accounts to the Clients OU. Then, you create a Group Policy object (GPO) named Sec_clients and link it to the Clients OU. You enable multiple security policies in the computer configuration section of the Sec_clients GPO.

The written security policy for Certkiller requires that all security settings through GPOs be applied continuously.

What should you do to enforce the written policy?

- A. Configure the Sec_clients GPO to reduce the Group Policy refresh interval for computers to 0.
- B. Configure the Sec_clients GPO to enable the Apply Group Policy for computers asynchronously during startup policy.
- C. Configure the Sec_clients GPO to enable the Process even if the Group Policy objects have not changed policy in the Security Policy processing policy.
- D. Create a domain named Client_computers.
Add the client computer accounts to the Client_computers group.
Add the Client_computers group to the Sec_clients DACL and grant the group the Read and Apply Group Policy permissions.

Answer: C

Explanation:

To achieve the highest level of policy settings security, activate the Process Even If The Group Policy Objects Have Not Changed policy for each of the Group Policy client-side extensions that require it.

Note: These policy settings are located in the Computer Configuration node, under Administrative Templates, System, Group Policy. Each client-side extension has a policy setting for controlling the policy processing. By default, each Group Policy client-side extension updates its policy settings only when they have changed. Choosing this option ensures that the selected settings are applied at every logon session to Active Directory, but forgoes the performance optimization achieved by skipping the application of policy settings when they have not changed.

Incorrect Answers

A: If you select 0minutes, the computer tries to update Group Policy every 7seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations.

Note: The Group Policy refresh interval for computers policy specifies how often Group Policy for computers is updated while the computer is in use (in the background). This policy specifies a background update rate only for Group Policies in the Computer Configuration folder. You can specify an update rate from 0to 64,800minutes (45days). By default, computer Group Policy is updated in the background every 90 minutes, with a random offset of 0to 30minutes. In addition to background updates, Group Policy for

the computer is always updated when the system starts.

B: This would be counterproductive. Some policies might not be applied until after the user has access to the Desktop. The Apply Group Policy for computers asynchronously during startup policy is used to optimize Group Policy for Logon Performance in Windows 2000.

D: A new domain is not required.

QUESTION 72:

You are the administrator of a Windows 2000 network. The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers. The corporate security policy specifies that users cannot use the Offline Files feature of Windows 2000. You want to ensure that Offline Files is disabled on the client computers and that users cannot enable this functionality. What should you do?

- A. On the Windows 2000 Professional client computers, clear the Enable Offline Files option on the Folder Options dialog box in Windows Explorer.
- B. Create a Group Policy object (GPO) and link it to the domain. Configure the GPO to disable the Enabled policy in the computer configuration of Offline Files.
- C. Create a Group Policy object (GPO) and link it to the domain. Configure the GPO to enable the Disable user configuration of Offline Files policy in the user configuration of Offline Files.
- D. Configure the Default Domain Policy Group Policy object (GPO) to enable the Disable "Make Available Offline" policy in the user configuration of Offline Files.

Answer: C

Explanation:

We create an appropriate GPO and link it to the domain. It will be applied to all client computers in the domain.

Note: The Disable user configuration of Offline Files policy prevents users from enabling, disabling, or changing the configuration of Offline Files.

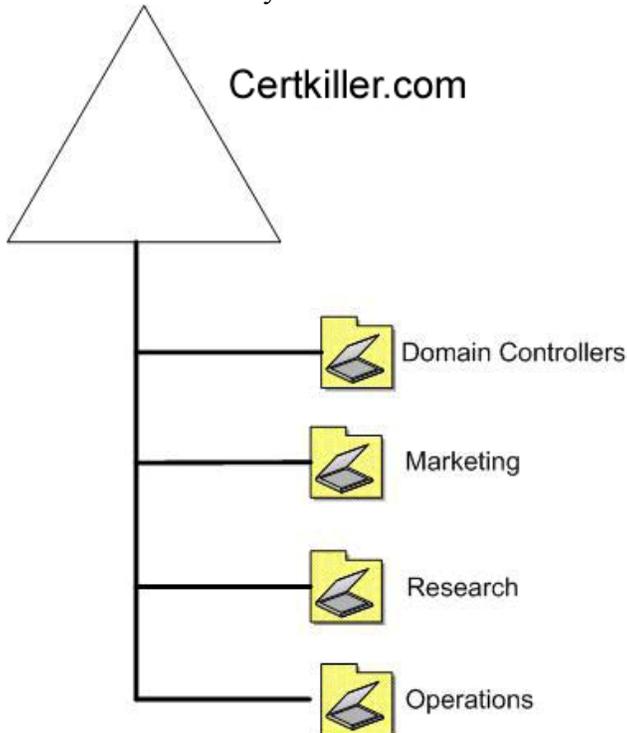
Incorrect Answers

- A: Manual reconfiguration of every single client computer would be a daunting task. Furthermore, the users could simply check the Enable Offline Files option themselves.
- B: We must use the Disable user configuration of Offline Files policy.
- D: This will not work.

QUESTION 73:

You are one of the network administrators for Certkiller . The network consists of a Windows 2000 Active Directory domain. Certkiller has three departments: research, sales, and operations. Each department has a separate organizational unit (OU) in the

domain that contains all user and computer accounts for that department. Each OU has the Block Policy inheritance option selected. The Active Directory structure is shown in the exhibit.



The network includes two Windows 2000 Server computers configured as domain controllers. The domain controllers are named Certkiller 1 and Certkiller 2. The network also contains 500 Windows 2000 Professional client computers. One of the client computers is named CK1 .

You administer the Research OU. A Group Policy object (GPO) named SPDeploy contains a software deployment package for the latest Windows 2000 Server pack. You connect to Certkiller 2 and link SPDeploy to the Research OU. You restart CK1 . You discover the service pack did not apply to CK1 . You run the gpresult command on CK1 and obtain the results shown in the following exhibit.

Group Policy was applied from: Certkiller 1. Certkiller .com

#####

The computer received "Registry" settings from these GPOs:

Local Group Policy
Default Domain Policy

The computer received "Security" settings from these GPOs:

Default Domain Policy

=====

The computer received "EFS recover" settings from these GPOs:

Local Group Policy
Default Domain Policy

You must ensure that CK1 receives the service pack.

What should you do?

- A. Disable Block Policy inheritance on the Research OU.
- B. Force and verify replication between domain controllers.
Restart CK1 .
- C. Configure the Everyone group for Read and Apply Group Policy permissions on the DACL of SPDeploy.
- D. Edit SPDeploy and configure the software installation package under the user configuration section of the GPO.
Remove the installation package from the computer configuration section.
Restart CK1 .

Answer: C

Explanation:

Read and Apply Group Policy permissions on a GPO ensures that the GPO can be applied.

Incorrect Answers

A: The GPO is directly linked to the OU. The Block Policy inheritance would have no effect.

B: Other GPOs have been applied. This is not a replication problem.

D: Service Packs should be assigned to computers, not deployed to users.

QUESTION 74:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. All client computers are in an organizational unit (OU) named Clients.

The network included two Windows 2000 Server computers, named Certkiller 1 and Certkiller 2, configured as domain controllers. One Windows 2000 Server computer, named Certkiller 3, is configured as a file server.

The network also contains 1,500 Windows 2000 Professional client computers.

You are distributing a new hotfix to the Windows 2000 Professional clients on your network. You place the hotfix in a shared folder on Certkiller 3. You create a batch file to install the hotfix from the share on Certkiller 3. You create a Group Policy object (GPO) named HF1 and link it to the Clients OU. HF1 runs the batch file as a startup script. All computers receive the hotfix.

A network user named Jack reports that her computer named CK1 had an application problem. You discover that Jack is using an application that you did not test. Jack tells you that the application worked correctly before the hotfix was applied. All other client computers are working correctly.

Management determines the application is necessary for Jack's computer. All new computers must continue to receive the hotfix.

You must ensure that Jack can continue to use the application and that all other computers retain the hotfix.

What should you do?

- A. Configure the Block Policy inheritance policy on the Domain Controllers OU.
Uninstall the hotfix from CK1 .
- B. Delete the HF1 GPO.
Uninstall the hotfix from CK1 .
- C. Configure the DACL on the HF1 GPO to deny CK1 's computer account Read and Apply Group Policy permissions.
Uninstall the hotfix from CK1 .
- D. Configure the DACL on the HF1 GPO to deny Jack's user account Read and Apply Group Policy permissions.
Uninstall the hotfix from CK1 .

Answer: C

Explanation:

The GPO is linked to an OU which contain the client computer account. We deny CK1 's computer account Read and Apply Group Policy permissions to the GPO. This ensures that the GPO will not be applied to CK1 . It still applies to all other computers.

Incorrect Answers

- A: The Domain Controllers OU is unrelated to the problem in this scenario.
B: We need to GPO to apply to all computers except CK1 .
D: The OU contain computer accounts, not user accounts.

QUESTION 75:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 100 Windows 2000 Server computers, 5,000 Windows 2000 Professional computers, and 1,000 Windows XP Professional computers.

The computer accounts for all servers are located in an organizational unit (OU) named Servers. The computer accounts for all client computers are located in an OU named Desktops. All user accounts are located in an OU named CorpUsers.

You download a new Windows 2000 service pack from the Microsoft Web site. The service pack is distributed as a Microsoft Windows Installer package.

You need to ensure that all Windows 2000 Professional computers receive the service pack. The service pack must not be deployed to any Windows XP Professional computers.

Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

- A. Create a child OU named WinXP under the Desktops OU.
Move all Windows XP Professional computer accounts to the WinXP OU.
- B. Create a child OU named Win2000 under the Desktops OU.
Move all Windows 2000 Professional computer accounts to the Win2000 OU.
- C. Create a Group Policy object (GPO) named W2KSP.
In the user configuration section of W2KSP, publish the service pack installer file.

- D. Create a Group Policy object (GPO) named W2KSP.
In the computer configuration section of W2KSP, assign the service pack installer file.
- E. Link W2KSP to the Desktops OU.
- F. Link W2KSP to the CorpUsers OU.
- G. Link W2KSP to the Win2000 OU.

Answer: B, D, G

Explanation:

B: We create a separate OU for the Windows 2000 Professional computers.

D: We create a GPO that assigns the service pack installer file. This ensures that the installation of the installer file starts the next time the Windows 2000 Professional computers are restarted.

G: Finally we link the GPO to the OU with the Windows 2000 Professional computers.

Incorrect Answers

A: We must apply the GPO to the Windows 2000 computers, so we cannot make a child OU with Windows XP computers.

C: If we publish the service pack we rely that the users install the it. This is not acceptable.

E: If we link the GPO to the Desktops it would be applied to the Windows XP computers as well. They are either in this OU or in a child OU (see A).

F: We should not apply the service pack to all users, just to the Windows 2000 Professional computers.

QUESTION 76:

You are the network administrator for Certkiller . Certkiller has a main office and 25 branch offices. The network consists of a Windows 2000 Active Directory domain. The domain included 10 Windows 2000 Server computers configured as domain controllers and 100 Windows 2000 Professional computers. The computer accounts for all portable computers are in an organizational unit (OU) named PortableComputers.

Employees in the sales department use the portable computers and have user accounts that are located in an OU named Sales.

You create a new Group Policy object (GPO) named App1 and link it to the PortableComputers OU. You configure App1 to deploy a security update by using an .msi file that is configured in the computer configuration section of the GPO.

After a week, you discover that none of the portable computers has installed the security update. You need to ensure that the portable computers install the security update.

What should you do?

- A. Enable the Group Policy slow link detection policy.
- B. Link App1 to the Sales OU and ask the users to log off and log back on their computers.
- C. Restart the portable computers while the computers are connected directly to the main office network.
- D. Force synchronization of the Active Directory database and the Sysvol share of all

domain controllers.

Answer: A

Explanation: Some Group Policies will automatically not run when they detect a slow network link-specifically:

1. Internet Explorer Maintenance
2. Software Installation (this applies in current scenario)
3. Folder Redirection
4. Scripts (logon/logoff, shutdown/startup)
5. Disk Quota

The Group Policy Slow Link Detection policy, which sets the transfer rate at which a workstation or server communicating with a DC should consider the link slow and alter Group Policy processing behavior. By enabling this policy the GPO would be applied to the portable computers.

Incorrect Answers

B: There is no need to link the GPO to the user OU. We should keep the GPO linked to OU which contains the computer accounts.

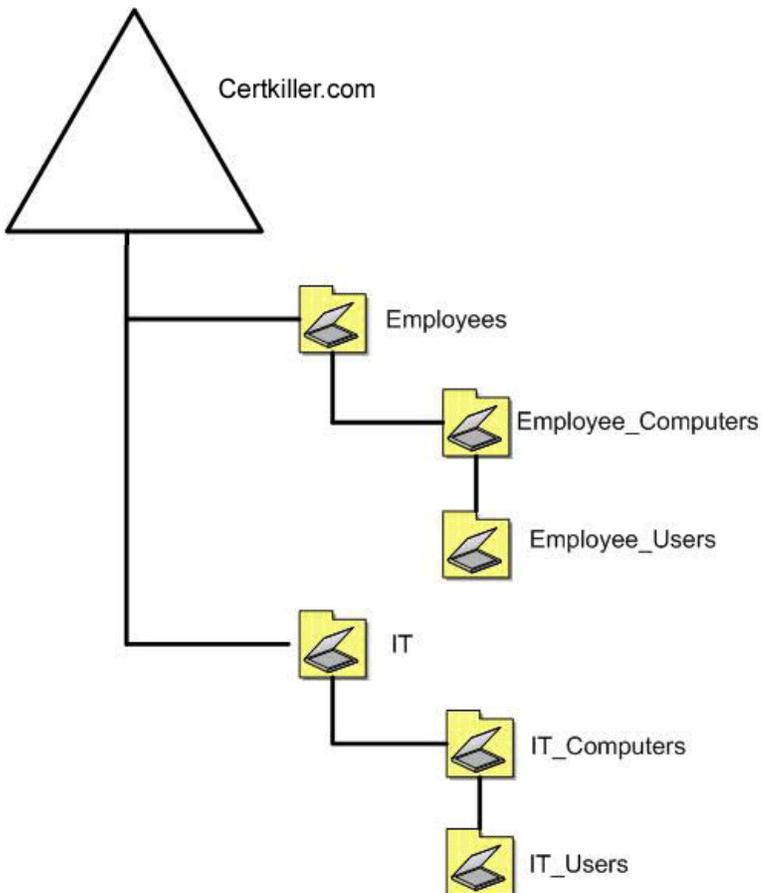
C: This seems possible as well, but is more awkward and might require more effort.

D: This is not an Active Directory synchronization problem.

QUESTION 77:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains two Windows 2000 domain controllers and 500 Windows 2000 Professional computers.

The relevant portion of the Active Directory hierarchy is shown in the exhibit.



The user accounts for all administrators are located in the IT_Users organizational unit (OU). All other user accounts are located in the Employee_Users OU. The client computer accounts for the administrator's computers are located in the IT_Computers OU. All other client computers accounts are located in the Employee_Computers OU. You create a Group Policy object (GPO) named GPO1 and link it to the Employee_Users OU. You select the Block Policy inheritance check box in the Employee_Users OU. You configure GPO1 as shown the in the following table.

Policy or setting	Status
Do not display last user name on logon screen	Enabled
Disable Computer Configuration Settings	Cleared
Disable User Configuration Settings	Selected

An employee named Jack reports that another user's name was in the logon dialog box when he attempted to log on to the network. You need to ensure that the name of the last user to log on does not appear in the logon dialog box.

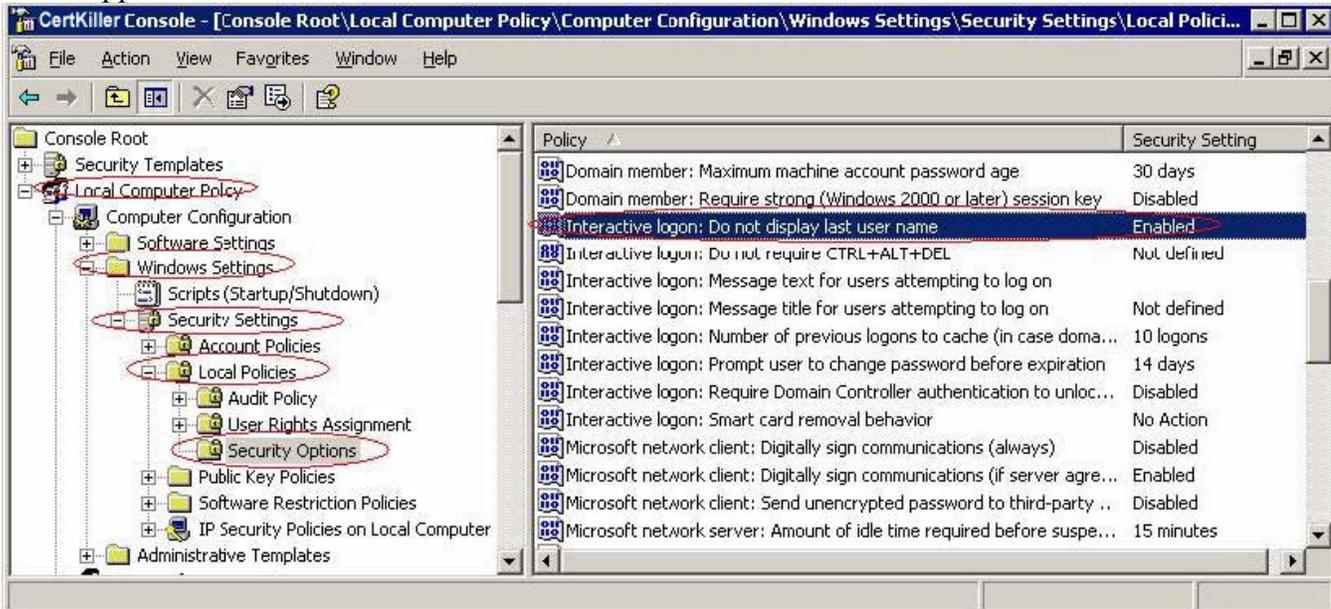
What should you do?

- A. Link GPO1 to the Employee_Computers OU.
 - B. Clear the Disable User Configuration Settings check box in GPO1.
 - C. Clear the Block Policy Inheritance check box in the Employee_Users OUD.
- Disable the Do not display last user name in logon screen policy in GPO1.

Answer: A

Explanation:

The Do not display last user name on logon screen policy applies to computers not to users (see below). We should therefore link the GPO to the OU with computers, it should not be applied to an OU with users.



Reference:

HOW TO: Prevent the Last Logged-On User Name from Being Displayed in Windows 2000, Microsoft Knowledge Base Article - Q310125

Incorrect Answers

B: The Do not display last user name on logon screen policy applies to computers, so it is not affected by the Disable User Configuration Settings policy.

C: Block Policy Inheritance does not affect a GPO directly linked to the OU.

D: We must keep this policy enabled.

QUESTION 78:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional computers. All domain controllers run Windows 2000 Server.

The domain includes two organizational units (OU) named Sales and IT. The sales department contains 50 users who have user accounts in the Sales OU. Bill is an administrator who resets passwords for all user accounts in the Sales OU when necessary. Bill's user account is located in the IT OU. You create a new group named Sales_pw

and place the group in the Users container. You add Bill's user account to the new Sales_pw group.

You create a custom MMC console that includes a Taskpad view of the Sales OU. The Taskpad view allows one task, which is the ability to reset passwords. You restrict the console so that only the Sales OU can be seen and set the console mode to User mode. You discover that Bill is able to create an MMC console and include all of the Active Directory tools. You want to ensure Bill can access the snap-in only to reset passwords. What should you do?

- A. Add Bill's user account to the Account Operators group.
- B. Modify the DACL on the Sales OU so that the Sales_pw group has the Reset Password permission on the user object.
- C. Create a Group Policy object (GPO) and link it to the IT OU. Configure an MMC restriction policy that allows Bill to open the Active Directory Users and Computers snap-in.
- D. Create a Group Policy object (GPO) and link it to the Sales OU. Configure an MMC restriction policy that allows Bill only to open the Active Directory Users and Computers snap-in.

Answer: D

Explanation:

We create a new GPO, link it to Sales OU, and configure an appropriate MMC restriction policy for the GPO.



Incorrect Answers

- A, B: We need to restrict Bill.
- C: The MMC console includes a Taskpad view of the Sales OU, not the IT OU.

QUESTION 79:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain that contains 5,000 Windows 2000 Professional client computers. All client computer accounts are located in an organizational unit (OU) named ClientComputers. All Certkiller employees log on to their computers by using

domain user accounts.

All client computers are installed by using a standard Windows 2000 Professional image, which includes Internet Information Services (IIS). However, only three software developers use IIS on their client computers.

These developers report that their client computers are infected with a virus. You discover that the virus infects computers by attacking IIS. You estimate that one-third of the client computers are infected with the virus, and the virus is slowly spreading to other computers.

Your anti-virus software does not currently detect this virus, although an update will be available in three business days. The developers can work normally without IIS for several days, if necessary.

Until the anti-virus update is available, you need to prevent the virus from spreading to additional client computers.

What should you do?

A. On each developer's client computer, configure the World Wide Web Publishing service to have a startup type of Disabled.

B. On each computer infected by the virus, configure the properties of the LAN connection so that IP filters prevent inbound network traffic on TCP port 80.

C. On each computer not infected by the virus, configure the properties of the default Web site so that only Integrated Windows authentication is enabled.

Then, stop the default Web site.

D. On a domain controller, create a Group Policy object (GPO) and link it to the ClientComputers OU.

Configure the GPO to disable the World Wide Web Publishing service.

In the GPO, select the No Override check box.

Restart the computers.

Answer: D

Explanation:

We need to disable the WWW Publishing service on all client computers. We create a new GPO, configure it to disable the service, and link it to the ClientComputers OU. We also use the No Override option and finally restart all client computer.

Incorrect Answers

A: It is better to deploy this option through a GPO: It requires less administrative effort.

B: Inadequate measure. It would most likely not stop the virus from spreading.

C: We should disable the WWW service.

QUESTION 80:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains a Windows 2000 Server computer named Certkiller 1. Certkiller 1 is configured as a domain controller.

During a security audit on Certkiller 1, you discover that every five minutes, the application event log repeats the following two events:

Event Source: SceCli
Event Category: None
Event ID: 1001
Date: 4/7/2002
Time: 4:30:46 AM
User: N/A
Computer: Certkiller1
Description: Security policy cannot be propagated. Cannot access the template.
Error code = 3.
\\ Certkiller.com\sysvol\ Certkiller.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf.

Event Type: Error
Event Source: Userenv
Event Category: None
Event ID: 1000
Date: 4/7/2002
Time: 4:40:46 AM
User: NT AUTHORITY\SYSTEM
Computer: Certkiller1
Description: The Group Policy client-side extension Security was passed flags (17) and returned a failure status code of (3).

Date: 4/7/2002
Time: 4:30:46 AM
User: N/A
Computer: Certkiller1
Description: Security policy cannot be propagated. Cannot access the template.
Error code = 3.
\\Certkiller.com \sysvol\ Certkiller.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTempl.inf.

Event Type: Error
Event Source: Userenv
Event Category: None
EventID: 1000
Date: 4/7/2002
Time: 4:30:46 AM
User: NT AUTHORITY\SYSTEM
Computer: Certkiller1

You need to correct the condition that is causing these errors.
What should you do?

- A. Delete and then re-create the computer account.
- B. Restore the Systemroot\Sysvol\Domain\Policies folder.
- C. Ensure that the Key Distribution Center service is started.
- D. Use a Windows 2000 Server CD-ROM to perform a Repair of the installation.

Answer: B

Explanation:

This issue can occur if the %SystemRoot%\SYSVOL\Domain\Policies Group Policy directory structure is missing or is incorrect. The Replication service is trying to replicate the directory but cannot locate it.

To resolve this issue, the directory must be restored to allow replication between domain controllers. This directory can either be restored from a backup or it can be recreated.

Reference:

Event ID 1000 and 1001 Repeat Every 5 Minutes in the Event Log, Microsoft Knowledge Base Article - Q271213

QUESTION 81:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain named Certkiller .com. The domain contains 10 Windows 2000 Server computers that run Internet Information Services (IIS) 5.0. These servers host Certkiller 's public Web site. Only the computer accounts for these Web servers are in an organizational unit (OU) named Web.

According to the written security policy for Certkiller , the World Wide Web publishing service on each Web server must always have a startup type of Automatic, and the FTP service on each Web server must always have a startup type of Disabled. Only the members of the Domain Admins group are allowed to stop and start these services.

You need to configure the Web servers to comply with the written policy.

What should you do?

A. On each Web server, configure the startup types for the World Wide Web Publishing service and the FTP service to comply with the written policy.

For both services, configure the Log on as account as Certkiller \Domain Admins.

B. On each Web server, configure the startup types for the World Wide Web Publishing service and the FTP service to comply with the written policy.

Add the Domain Admins group to the Power Users group on each Web server.

C. Create a Group Policy object (GPO) and link it to the Web OU.

Create a security template that configures the startup types for the World Wide Web Publishing service and the FTP service to comply with the written policy.

Configure the Domain Admins group as the only group that can stop and start these services.

Import the security template into the new GPO.

D. Install a new Windows 2000 Server computer that is running IIS 5.0, then place the new server in the Web OU.

Create a Microsoft Windows Installer package that includes the correct configuration for the World Wide Web Publishing service and FTP service startup types.

For both services, configure the Log on as account as Certkiller \Domain Admins.

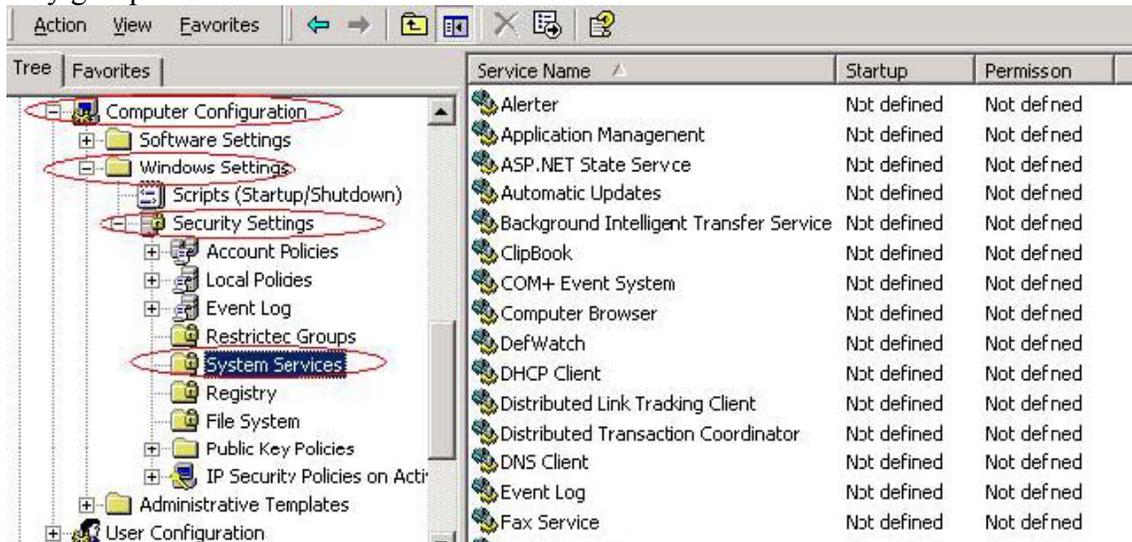
Create a Group Policy object (GPO) and link it to the Web OU.

Assign the installer package to the computer configuration section in the new GPO.

Answer: C

Explanation:

We configure a GPO with the appropriate settings and link it to the Web OU. The GPO will be applied to all Web servers. We also configure the Domain Admins groups as the only group that can start these services.



Incorrect Answers

A: If the services runs as Domain Admins they are a security risk. Furthermore, we have not ensured that only Domain Admins are allowed to stop and start these services.

B: We have not ensured that only Domain Admins are allowed to stop and start these services.

D: If the services runs as Domain Admins they are a security risk. Furthermore, it is not necessary to use a new server, and configuration of the services through an Installer package is an awkward approach.

QUESTION 82:

You are the administrator of a Windows 2000 network. Users on the network use Windows 2000 Professional client computers. All client computers are part of the same domain.

Each quarter, users install updates for an accounting application. The updates are provided in the form of a Microsoft Windows Installer package.

To increase the security of the network and the Windows 2000 Professional client computers, you change several permissions on folder on the file system and in the registry of the client computers. Users then report that they can no longer install the quarterly Windows Installer packages. When they double-click a Windows Installer package, they receive an "Access denied" error message halfway through the installation.

You want to ensure that the quarterly Windows Installer packages are installed successfully on the client computers without lowering the level of system security.

What should you do?

A. Configure the Default Domain Policy to direct Windows Installer to always install Windows Installer packages with elevated privileges.

B. Create a Group Policy object (GPO) and link it to the domain.

Configure the GPO to assign the Windows Installer packages to the users.

C. Configure the Active Directory user accounts with a logon script.

Use the `msiexec.exe` command in the logon script to install the Windows Installer packages.

D. Create a Group Policy object (GPO) and link it to the domain.

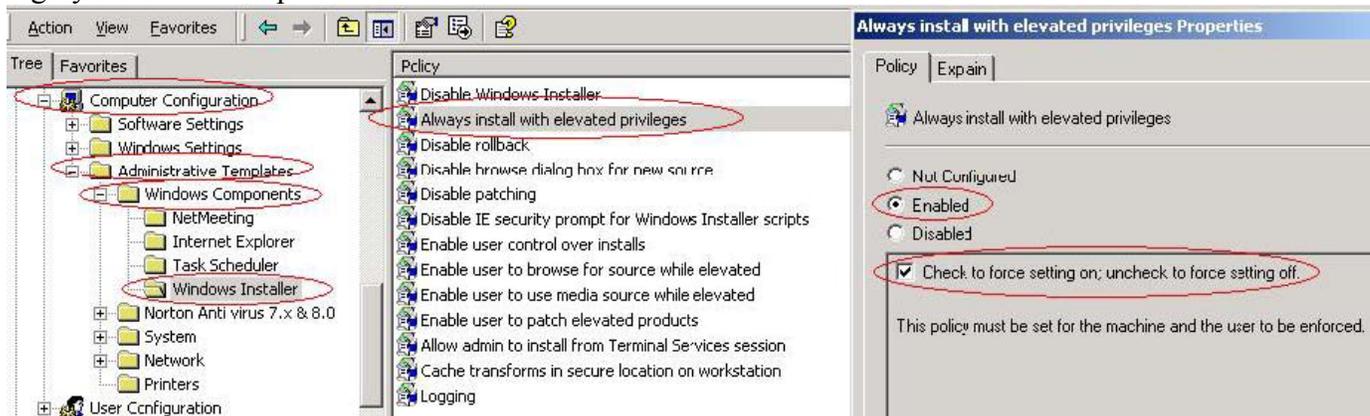
Configure the GPO to specify a logon script.

Use the `msiexec.exe` command in the logon script to install the Windows Installer packages.

Answer: A

Explanation:

Windows 2000 has an Always install with elevated privileges Group Policy, that directs Windows Installer to always use System permissions when installing a program. This policy extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add/Remove Programs in Control Panel. This policy lets users install programs which require access to directories that the user might not have permission to view or change, including directories on highly restricted computers.



Reference:

How to Manage Windows Installer Local Policies, Microsoft Knowledge Base Article - Q227181

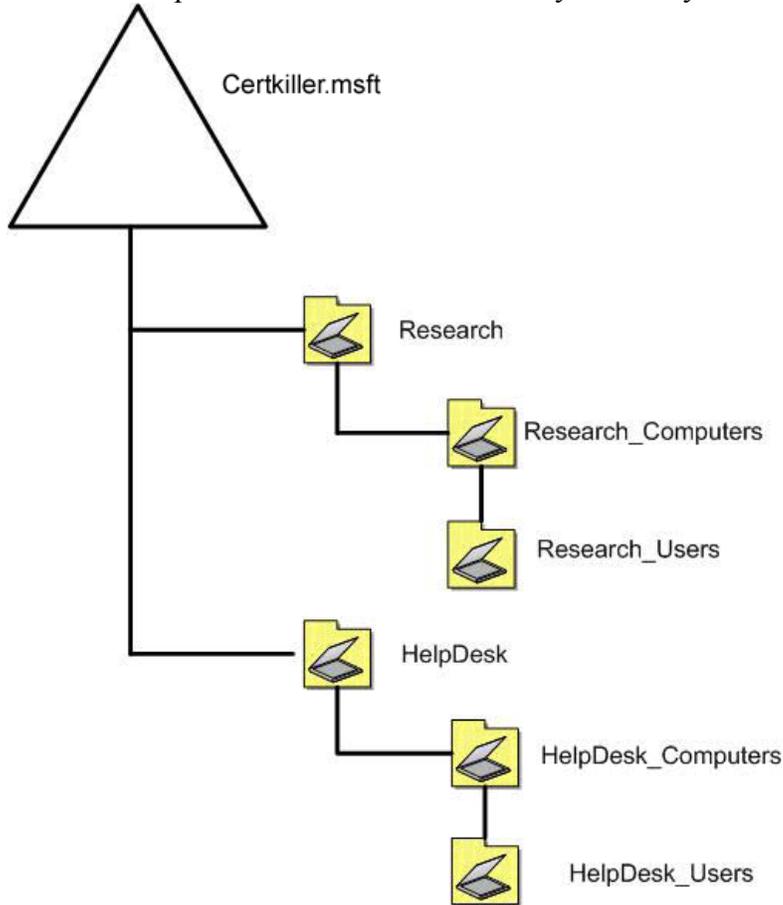
Incorrect Answers

B: Assigned applications would still be installed in the security context of the user account and the "Access denied" problem would still be present.

C, D: The installation would run in the context of the user account and the "Access denied" problem would occur.

QUESTION 83:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains two Windows 2000 domain controllers and 500 Windows 2000 Professional computers. The relevant portion of the Active Directory hierarchy is shown in the exhibit.



You detect an intrusion against the administrator account on the servers located in the Research_Computers OU. You create a new Group Policy object named RenameAdmin and link it to the Research_Computers OU. You configure RenameAdmin to rename the administrator account to CertKiller.

You need to apply RenameAdmin to the servers in the Research_Computers OU immediately.

What should you do?

- A. Restart the Net Logon service on each domain controller.
- B. Restart the Net Logon service on each server computer.
- C. Run the `secedit /refreshpolicy machine_policy /enforce` command on each domain controller.
- D. Run the `secedit /refreshpolicy machine_policy /enforce` command on each server computer.

Answer: D

Explanation:

We want to apply the changes on the servers in the Research_computers OU. These are not necessarily Domain Controller. We use the `secedit /refreshpolicy` command to enforce the changes immediately.

Incorrect Answers

A, B: Restarting the Net Logon Service would not apply GPOs.

C: We want to apply the changes on the servers in the Research_computers OU. These are not necessarily Domain Controller.

QUESTION 84:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The forest is divided into two sites: East and West. The domain contains 500 Windows 2000 Professional computers and two Windows 2000 domain controllers: Certkiller 1 and Certkiller 2.

You configure Certkiller 1 in the East site and Certkiller 2 in the West site. Certkiller 1 holds the PDC emulator and RID master Flexible Single Master Operation (FSMO) roles. Certkiller 2 holds the other FSMO roles.

You create a Group Policy object (GPO) named GPO1 and link it to the domain. You configure a security template and import it to GPO1. The security template configures the message title and text for the message that appears when users log on to the network.

Mr Bill is a user in the East site, and Jack is a user in the West site. You ask Mr Bill and Jack to restart their computers so that you can verify that GPO1 is applied. Mr Bill reports that he can see the logon message, but Jack reports that she does not see the message.

You need to ensure that Jack receives the logon message as soon as possible.

What should you do?

A. Stop and start the File Replication service on both domain controllers.

Instruct Jack to restart her client computer.

B. Restart the Net Logon service on each employee's client computer.

C. Ensure that both domain controllers are configured as global catalog servers.

Run the `secedit /refreshpolicy machine_policy` command on Jack's client computer.

D. Force synchronization of the Active Directory database across site boundaries.

Run the `secedit /refreshpolicy machine_policy` command on Jack's client computer.

Answer: D

Explanation:

We must force an Active Directory replication between the sites, and then apply the updates GPOs through the `secedit /refreshpolicy machine_policy` command.

Incorrect Answers

A, B: The File replication or Net logon services do not affect the Active Directory and GPOs.

C: A global catalog server in each site is not a bad long-term idea, but it is not necessary for the current problem.

QUESTION 85:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 domain controllers and Windows 2000 Professional computers. The network also includes Windows 98 computers.

You create an organizational unit (OU) named Client_Comps. You move all Windows 2000 client computers accounts to this OU. You create a Group Policy object (GPO) named CK1 and link it to the Client_Comps OU. You import the Securews.inf security template to CK1 .

The Windows 98 computers contain security settings by means of a system policy. You upgrade the Windows 98 computers to Windows 2000 Professional.

You discover that the upgraded client computers do not have the same security settings as the other Windows 2000 Professional computers. You need to ensure that all client computers have the same security settings.

What should you do?

- A. Move the computer account for each upgraded computer to the Client_Comps OU.
- B. Set No Override on the Default Domain Group Policy object (GPO).
- C. Clear the Block Policy inheritance check box in the Client_Comps OU.
- D. Perform a clean install of Windows 2000 Professional on each upgraded computer.

Answer: A

Explanation:

The computer accounts of the upgraded computers must move to the OU to which GPO CK1 is linked. This ensures that they will get the appropriate security settings.

Incorrect Answers

B: The default Domain Group Policy does not contain the security settings that are required.

C: CK1 is directly linked to the Client_Comps OU and is not directly affected by the Block Policy inheritance setting of the OU.

D: It is not necessary to re-install Windows 2000.

QUESTION 86:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 3,500 Windows XP Professional computers. All computers use Microsoft Internet Explorer as their only Web browser. All users have roaming profiles.

The written security policy for Certkiller prohibits users from modifying the sites listed in the Trusted Sites zone of Internet Explorer. The contents of the zone are specified in a Group Policy object (GPO) named IEZones. The IEZones GPO also enables the Security

Zones: Use only machine settings policy.

You link IEZones to the domain.

The next morning, users report that their roaming profiles are not working.

You need to ensure that users' roaming profiles work and that the written policy is enforced.

What should you do? (Each correct answer presents part of the solution. Choose two)

A. Run the gpupdate.exe /force /sync command on each Windows XP Professional computer.

B. Remove the link between the IEZones GPO and the domain.

Link the IEZones GPO to each organizational unit (OU) that contains computer accounts.

C. In the user configuration section of the IEZones GPO, enable the Disable the Security page policy.

D. In the computer configuration section of the IEZones GPO, disable the Security

Zones: Use only machine settings policy.

E. In the user configuration section of the IEZones GPO, enable the Do not allow users to change policies for any security zone policy.

Answer: D, E

Explanation:

D: The Security Zones: Use only machine settings policy. It applies security zone information to all users of the same computer. If you enable this policy, changes that the user makes to a security zone will apply to all users of that computer. We must disable this policy.

E: The Security Zones: Do not allow users to change policies policy prevents users from changing security zone settings. This policy prevents users from changing security zone settings established by the administrator. This is required and we should not disable this policy.

Incorrect Answers

A: The gpupdate.exe /force /sync command reapplies all policy settings. However, the policy settings are incorrect so this command would not do much good.

B: The GPO could very well be applied to the domain.

C: We do not want to disable all security settings. We only want to prevent the users from change policies for any security zone.

Note: The Disable the Security page policy which removes the Security tab from Internet Explorer in Control Panel, takes precedence over the Security Zones: Do not allow users to change policies policy. If Disable the Security page is enabled, this policy is ignored.

QUESTION 87:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 100 Windows 2000 Server computers and 5,000 Windows 2000 Professional computers.

The computer accounts for all servers are located in an organizational unit (OU)

named Servers. The computer accounts for 4,000 client computers are located in an OU named Desktops. The computer accounts for the remaining client computers are located in a OU named Research, which is a child of the Desktops OU. Certkiller uses Group Policy objects (GPOs) to configure client computers. However, the written security policy for Certkiller permits alternate configurations for client computers in the research department. The Research OU is configured to block Group Policy inheritance.

You download a new Windows 2000 service pack from the Microsoft Web site. The service pack is distributed as a Microsoft Windows Installer package.

You need to ensure that all Windows 2000 servers and client computers receive the service pack. You want to accomplish this task with the least amount of administrative time.

Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

- A. Configure a GPO named SvcPack that assigns the service pack to users.
- B. Configure a GPO named SvcPack that assigns the service pack to computers.
- C. Configure the SvcPack GPO to use the No Override option.
- D. Configure the SvcPack GPO to use loopback processing.
- E. Link the SvcPack GPO to the domain.
- F. Link the SvcPack GPO to the Desktops OU.

Answer: B, C, E

Explanation:

B: The service pack should be assigned to computers NOT to users.

C: The No Override option ensures that the GPO will be applied and not overridden by another GPO.

E: By linking the GPO to the domain it will be applied to all computers in the domain.

Reference: Microsoft® Windows® 2000 Service Pack Installation and Deployment Guide
Incorrect Answers

A: The service pack should be assigned to computers, NOT to users.

D: Loopback processing mode is used to establish machine-specific settings, so that the computer's client settings take precedence. It does not fit in this scenario.

F: The GPO must be applied to the servers as well. Linking the GPO to the Desktops OU would only apply the GPO to the Windows 2000 Professional computers.

QUESTION 88:

You and Bruno are the network administrators for Certkiller . The network consists of a Windows 2000 Active Directory domain. All client computers are in an organizational unit (OU) named Clients

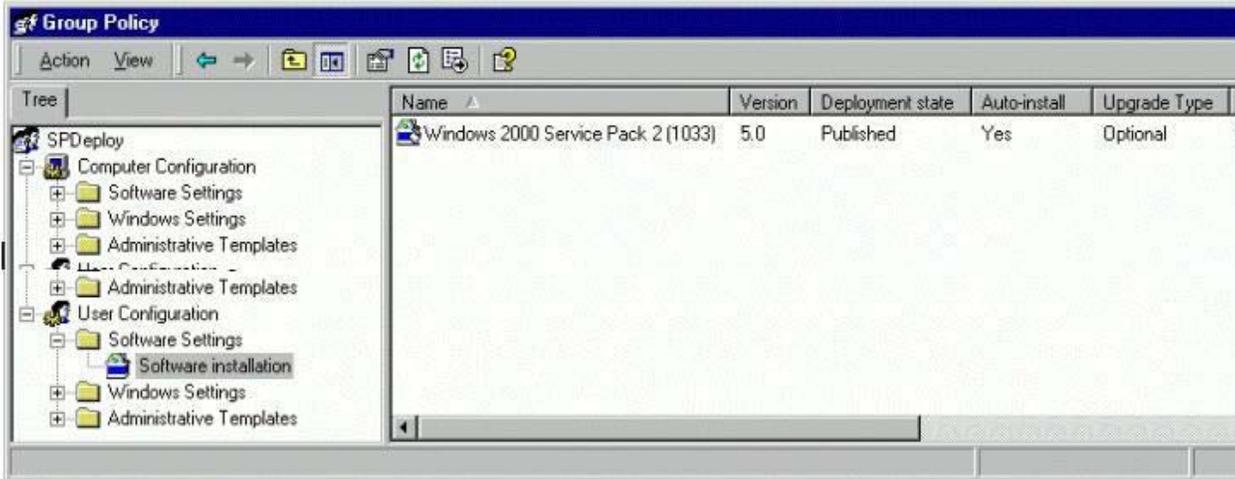
The network contains two Windows 2000 Server computers configured as domain controllers and three Windows 2000 Server computers configured as file servers.

The network also contains 1,500 Windows 2000 Professional client computers.

You and Mr Bill are responsible for deploying a service pack to all Windows 2000 Professional client computers. Mr Bill creates a Group Policy object (GPO) named

SPDeploy and links it to the Clients OU. He configures SPDeploy with a software package that installs the service pack.

You initiate an automatic restart of all client computers. After the client computers restart, none of the client computers you check has the service pack. Mr Bill asks you to review the software deployment package configuration, which the following exhibit shows.



You confirm that these client computers receive other GPOs that are linked to the Clients OU. You must ensure that SPDeploy is correctly deployed. What should you do?

- A. Change the Deployment state to Assign.
Select the Redeploy Application menu option on the software deployment package.
Restart the client computers.
- B. Remove all service packs from the client computers.
Select the Redeploy Application menu option on the software deployment package.
Restart the client computers.
- C. Remove the existing installation package.
Add update.msi as a new software installation package under the user configuration section of SPDeploy.
Restart the client computers.
- D. Remove the existing installation package.
Add update.msi as a new software installation package under the computer configuration section of SPDeploy.
Restart the client computers.

Answer: D

Explanation:

Because service packs are applied across organizations to computers rather than to specific users, you should deliver the Update.msi package by using a computer-level Group Policy deployment.

Reference:

Best Practices for Using Update.msi to deploy Service Packs, Microsoft Knowledge Base

Article - Q278503

Incorrect Answers

A, B; C: We should apply the service pack to computers, not to users.

QUESTION 89:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

On the Windows 2000 Server computers on the network, you want to install the latest service pack. However, you have already installed several post-service pack hotfixes. You install the latest service pack. You run the hfnetchk tool to verify the status of hotfixes on the server computers. The post-service pack hotfixes are now reported as "Not Found," even though they are installed.

You want hfnetchk to report correctly that the post-service pack hotfixes are installed. However, you do not want to reinstall the post-service pack hotfixes on the server computers.

What should you do?

- A. Run the sfc.exe command and specify that you want the tool to purge the file cache and scan all system files.
Then, run the hfnetchk tool.
- B. Run the qchain.exe command.
Then, run the hfnetchk tool.
- C. Run the hfnetchk.exe command and specify that you do not want the tool to perform registry checks.
- D. Run the hfnetchk.exe command and specify that you want the tool to display all hotfixes that are baseline critical.
- E. Run the hfnetchk.exe command and use the -history switch to display all hotfixes that have been explicitly installed.

Answer: E

Explanation:

The history switch with the hfnetchk.exe tool should provide the proper information. hfnetchk - history --> This switch displays updates that have been explicitly installed, explicitly not installed, or both. You do not require this switch for ordinary operation. However, you may require it under very specific circumstances. You can use any one of three values for n with this switch:

- * 1 - Displays those updates that have been explicitly installed.
- * 2 - Displays those updates that have been explicitly not installed.
- * 3 - Displays those updates that have explicitly been installed and not installed.

Reference:

Knowledge base Q303215

QUESTION 90:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

The written security policy for Certkiller specifies that users are not allowed to install or use the full version of the Network Monitor tool on the network. You want to verify whether the users on all Windows 2000 computers comply with this policy.

You find that when you install the full version of the Network Monitor tool, it installs a new service named the Monitor Control Service (mcsvc) on the computer. You want to ensure that when you check the security-related settings from your Windows 2000 Professional computer, you can find out whether the mcsvc service is installed on the computer in the domain.

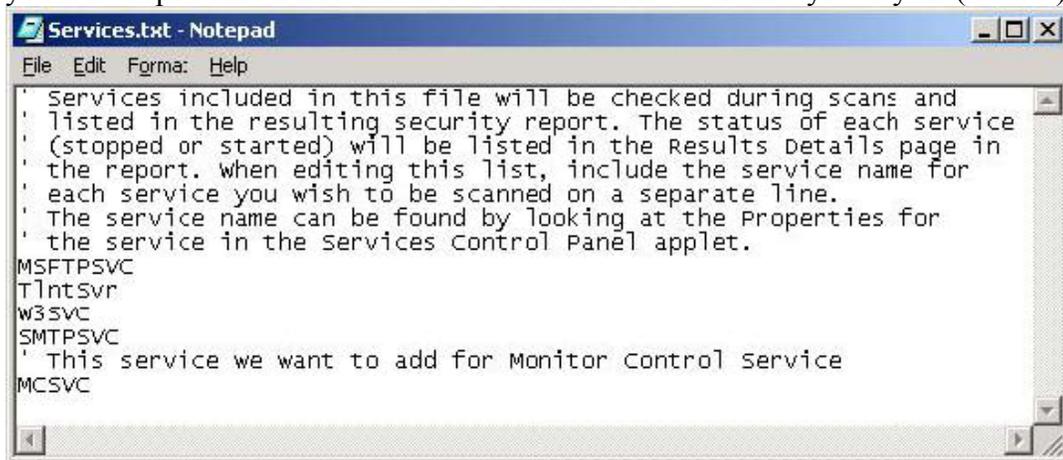
What should you do?

- A. Run the sigverif.exe command and check the resulting Sigverif.txt file.
- B. Run the mbsacli.exe command and specify that you want to display a detailed report.
- C. Edit a file named Services.txt to include the mcsvc service, and then run the Microsoft Baseline Security Analyzer (MBSA).
- D. Edit a file named Mssecure.xml to include the mcsvc service, and then run the hfnetchk.exe command.

Answer: C

Explanation:

If a service is installed, we don't know at what point someone might enable it so we take the safe route and report it. You can edit the services.txt file to add or remove services you want reported. We then run the Microsoft Baseline Security Analyzer (MBSA)



Incorrect Answers

- A: Signature Verification tool (Sigverif.exe) can be used to identify unsigned drivers on a Windows-based computer.
- B: Mbsacli.exe is the command line version of the Microsoft Baseline Security Analyzer (MBSA) tool. However, we must specify which services we want to be included in the

detailed report by editing the Services.txt file.

D: The Hfnetchk tool is used to assess hotfix patch status.

QUESTION 91:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

The written security policy for Certkiller specifies that the hotfix status and security-related settings of the servers in the domain must be examined regularly. You want to automate that process so that reports for all the servers are generated every night. What should you do?

- A. Schedule a task on each server to run the qfecheck.exe command every night.
- B. Schedule a task on each server to run the hfnetchk.exe command every night.
- C. Schedule a task on a central Windows 2000 Professional computer to run the mbsacli.exe command for each server every night.
- D. Schedule a task on a central Windows 2000 Professional computer to run Microsoft Baseline Security Analyzer (MBSA) for each server every night.

Answer: C

Explanation:

Mbsacli.exe is the command line version of the Microsoft Baseline Security Analyzer (MBSA) tool. It can be used to centrally scan Windows-based computers for common security misconfigurations. Mbsacli.exe can be used to scan for Windows Operating System checks, IIS checks, SQL checks, Hotfix checks, and Password checks.

Reference:

Microsoft Baseline Security Analyzer (MBSA) Version 1.0 Is Available. Microsoft Knowledge Base Q320454

Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available, Microsoft Knowledge Base Article - Q303215

Qfecheck.exe Verifies the Installation of Windows 2000 and Windows XP Hotfixes, Microsoft Knowledge Base Article - Q282784

Incorrect Answers

A: The qfecheck.exe tool is used to verify the installation of Hotfixes, not to scan for hotfix status or security settings, however.

B: The Hfnetchk tool is used to assess hotfix patch status. However, it cannot be used to analyze further security settings.

D: The Microsoft Baseline Security Analyzer tool (MBSA, or Mbsa.exe) tool centrally scans Windows-based computers for common security misconfigurations. MBSA can be used to scan for Windows Operating System checks, IIS checks, SQL checks, Hotfix checks, and Password checks. However, we cannot schedule the graphical MBSA tool. We must use the command line version instead.

QUESTION 92:

You are a network administrator for your branch office of Certkiller. You are responsible for 200 Windows 2000 Professional computers and one Windows 2000 Server computer that functions as a file server. The systems you administer are configured for a single internal IP subnet.

None of these computers has access to the Internet. Management has mandated that remote networks, including your branch office, should not be exposed to the Internet. You must verify that the latest hotfixes and service packs are applied to the computers in your branch office. What should you do?

- A. Run the netdiag /v command on the first domain controller installed on your domain.
- B. Install a modem on the Windows 2000 Server.
Implement Internet Connection Sharing.
Use Windows Update to perform the updates.
- C. Download the latest XML security update database from Microsoft on a computer that has Internet access.
Copy the database to a share on the local network.
Use hfnetchk with the XML security database to check service packs and hotfixes on your local segment.
- D. Install a second Ethernet adapter on the Windows 2000 Server computer.
Use the second adapter to connect to a network segment that has an Internet connection.
Configure Network Address Translation (NAT) on the Windows 2000 Server computer.
Use Windows Update to keep all the computers updated.

Answer: C

Explanation:

We should download the latest security update database from the Microsoft Internet site. We should use a computer that already has Internet access. We make the security updates available through a share on the LAN. We then use the Hfnetchk tool to verify that latest hotfixes and service packs are applied to the computers in the LAN.

Note: The Hfnetchk tool (Hfnetchk.exe) is a command-line tool that administrators can use to centrally assess a computer or group of computers for the absence of security patches.

Reference:

Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available, Microsoft Knowledge Base Article - Q303215

DCDiag and NetDiag in Windows 2000 Facilitate Domain Join and DC Creation, Microsoft Knowledge Base Article - Q265706

Incorrect Answers

A: The Network Diagnostics tool, Netdiag.exe, provides general Windows 2000 diagnostic capabilities. It cannot be used to verify hotfixes.

B: The network must not be exposed to Internet.

D: The network must not be exposed to Internet.

QUESTION 93:

You are the administrator of a regional office LAN on the Certkiller network. The network consists of a Windows 2000 Active Directory domain. All computers on Certkiller's network are using either Windows 2000 Professional or Windows 2000 Server.

Certkiller has one main office and several regional offices. Each regional office is represented by an organizational unit (OU). The main office has two domain controllers. Each regional office has a domain controller. All the computers at your regional office have an IP address in the same subnet. Your user account has full administrative control over every computer at your office.

You must find out whether the computers in your regional office have the latest hotfixes and service packs applied.

What should you do? (Each correct answer presents a complete solution. Choose two)

- A. Run the `netdom verify` command for your domain from any domain computer attached to your regional office network.
- B. Run the `netdiag /v` command for your domain from any domain computer attached to your regional office network.
- C. Run the `hfnetchk` command for the local subnet of your regional office from any domain computer attached to your regional office network.
- D. Run Microsoft Baseline Security Analyzer (MBSA) for the local subnet of your regional office from any domain computer attached to your regional office network.
- E. Run the `msicuu.exe` command on all domain computers on the local subnet of your regional office network.

Answer: C, D

Explanation: .

C: The `Hfnetchk` tool is a command-line tool that administrators can use to centrally assess a computer or group of computers for the absence of security patches.

D: The Microsoft Baseline Security Analyzer tool (MBSA, or `Mbsa.exe`) tool centrally scans Windows-based computers for common security misconfigurations. MBSA can be used to scan for Windows Operating System checks, IIS checks, SQL checks, Hotfix checks, and Password checks. Password checks can detect weak or blank passwords. However, the graphical user interface version of the tool is run by starting `Mbsa.exe` from the folder in which the tool was installed.

Computers in a range of IP addresses can be scanned.

Reference:

Microsoft Network Security Hotfix Checker (`Hfnetchk.exe`) Tool Is Available, Microsoft Knowledge Base Article - Q303215

Microsoft Baseline Security Analyzer (MBSA) Version 1.0 Is Available. Microsoft Knowledge Base Q320454

Incorrect Answers

A, B, E: The netdom verify, the netdiag /v, or the msicuu.exe commands do not assess hotfixes and service packs status.

QUESTION 94:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

From a Windows 2000 Professional client computer in the domain, you want to use the Microsoft Baseline Security Analyzer (MBSA) to verify the status of hotfixes and security-related settings of computers in the domain. You have installed a copy of MBSA on the Windows 2000 Professional computer.

The Windows 2000 Professional computer does not have access to the Internet. However, you want to ensure that you can verify the latest hotfixes.

What should you do?

A. Copy the latest available version of Mssecure.cab to the %ProgramFiles%\Microsoft Baseline Security Analyzer folder, then run MBSA.

B. Copy the latest available version of Hfnetchk.exe to the %ProgramFiles%\Microsoft Baseline Security Analyzer folder, then run MBSA.

C. From another computer, download the latest available version of the MBSA tool. Install the tool on the Windows 2000 Professional computer, then run MBSA.

D. From another computer, download the latest available version of the Microsoft XML parser (MSXML).

Install the parser on the Windows 2000 Professional computer, then run MBSA.

Answer: A

Explanation:

You can manually download the signed mssecure.XML file used for the hotfix check from the following Microsoft Web site:

<http://download.microsoft.com/download/xml/security/1.0/nt5/en-us/mssecure.cab>.

MBSA will automatically try and download the latest mssecure.cab file (signed by MS)

Reference:

Microsoft Baseline Security Analyzer (MBSA) Version 1.0 Is Available. Microsoft Knowledge Base Article - Q320454

QUESTION 95:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

From a Windows 2000 Professional client computer in the domain, you want to find out whether the local user accounts on the Windows 2000 member servers and Windows 2000 Professional client computers in the domain use a blank password or a common simple password, such as "password" or "admin."

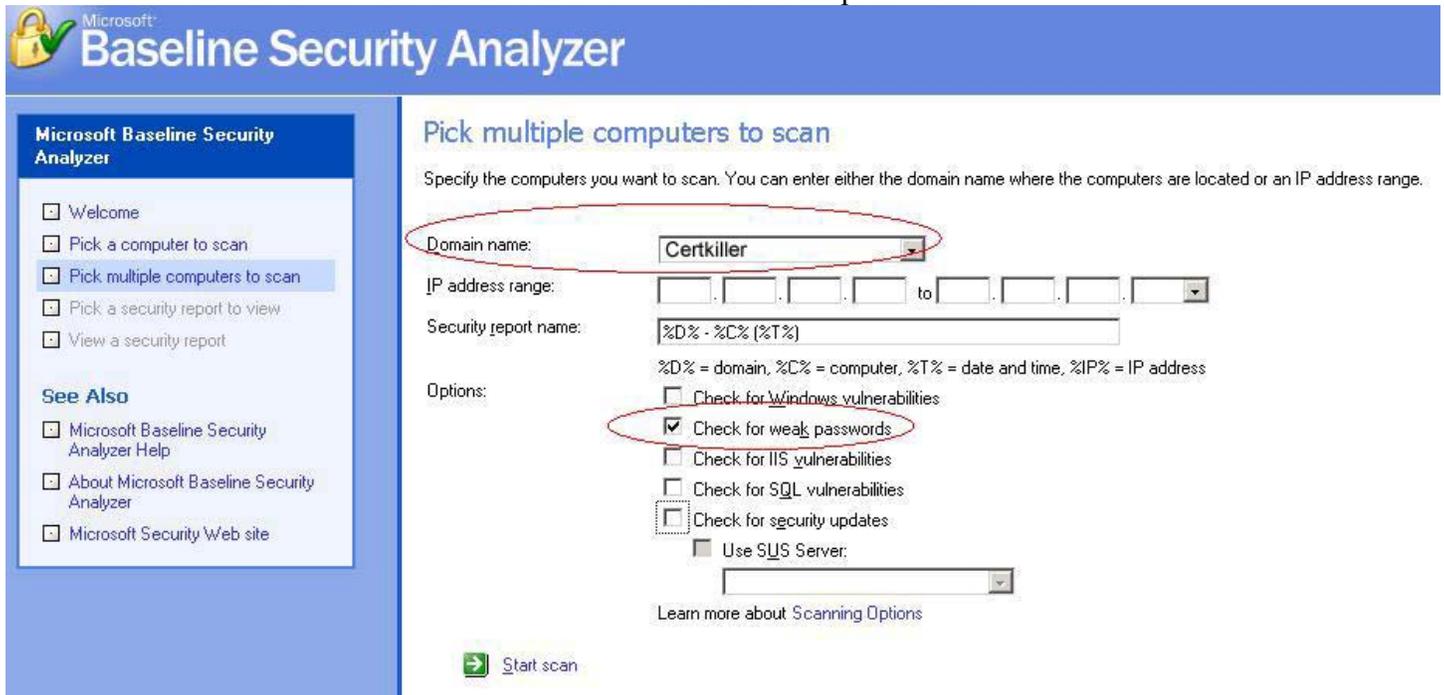
What should you do?

- A. Run Microsoft Baseline Security Analyzer (MBSA) for the computers in the domain.
Ensure that you are a local administrator on the scanned computers.
- B. Run the hfnetchk.exe command for the computers in the domain.
Ensure that no account lockout policy is defined on the scanned computers.
- C. Run the sigverif.exe command on the computers in the domain.
Ensure that Account Management auditing is turned off on the scanned computers.
- D. Run the qfecheck.exe command on the computers in the domain.
Ensure that you have the Log on as a batch job user right on the scanned computers.

Answer: A

Explanation:

The Microsoft Baseline Security Analyzer tool (MBSA, or Mbsa.exe) tool centrally scans Windows-based computers for common security misconfigurations. MBSA can be used to scan for Windows Operating System checks, IIS checks, SQL checks, Hotfix checks, and Password checks. Password checks can detect weak or blank passwords.



Reference:

Microsoft Baseline Security Analyzer (MBSA) Version 1.0 Is Available. Microsoft Knowledge Base Q320454

Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available, Microsoft Knowledge Base Article - Q303215

How to Use the File Signature Verification Tool to Find Third-Party Drivers, Microsoft Knowledge Base Article - Q259283

Qfecheck.exe Verifies the Installation of Windows 2000 and Windows XP Hotfixes,

Microsoft Knowledge Base Article - Q282784

Incorrect Answers

B: The Hfnetchk tool is used to assess hotfix patch status.

C: Signature Verification tool (Sigverif.exe) can be used to identify unsigned drivers on a Windows-based computer. It is not helpful for analyzing passwords.

D: The qfecheck.exe tool is used to verify the installation of Hotfixes, not to analyze password weaknesses.

QUESTION 96:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

Every night at 2:00 A.M., you automatically run the mbsacli.exe command on a Windows 2000 Server named Certkiller 1 to verify the status of hotfixes and security-related settings of the computers in the domain. In the morning, you want to view the results that mbsacli.exe has generated.

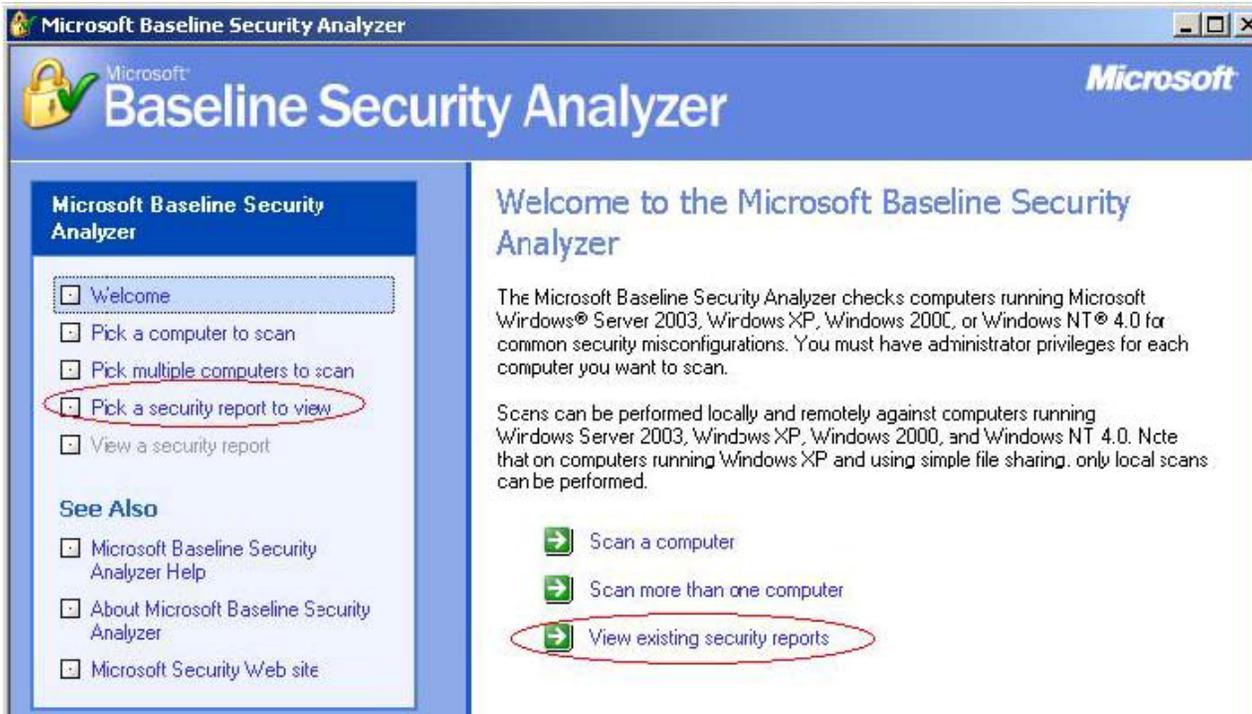
What should you do?

- A. Run the qfecheck.exe command and specify that you want to display verbose output.
- B. Run the hfnetchk.exe command and include the -history switch.
- C. Run the Microsoft Baseline Security Analyzer (MBSA) and specify that you want to view existing reports.
- D. Run the Eventcomb tool to collect reports from the computers in the domain.

Answer: C

Explanation:

Mbsacli.exe is the command line version of the Microsoft Baseline Security Analyzer (MBSA) tool. Scan reports are stored on the computer on which the tool is installed in the %userprofile%\SecurityScans folder. We can use the graphical MBSA tool to analyze the scan reports that has been produced by the MBSA command line tool.



Reference:

Microsoft Baseline Security Analyzer (MBSA) Version 1.0 Is Available. Microsoft Knowledge Base Q320454

Incorrect Answers

A: The qfecheck.exe tool is used to verify the installation of Hotfixes only.

B: The hfnetchk.exe command line tool is used to check for missing patches.

D: Eventcomb is a tool that allows event logs across servers to be parsed for events.

However, it is not used to view scan results of the MBSA tool..

QUESTION 97:

You are one of two administrators for Certkiller . The network structure contains a Windows 2000 Active Directory domain named Certkiller .com. The network infrastructure is divided into two sites: TestA and TestB.

The other administrator, Mr Bill, is responsible for ensuring that security updates are deployed in Test

A. You are responsible for ensuring that security updates are deployed in TestB.

While you are on vacation, Mr Bill writes a script that applies several security updates to all the computers in TestA and TestB. When you return, you discover that one of the security updates applied to TestB computers is incompatible with some of the software on those computers. Mr Bill confirms that his script applied the security update, and he also reports that he had to run his script a couple of times because it failed once about halfway through.

You must determine which systems currently have incompatible security update.

You must also verify which security updates are currently on your system. You would like to accomplish these tasks with the least amount of administrative effort.

What should you do?

- A. Configure a script to retrieve the OS build number and return the results to a centralized database.
- B. Rewrite Mr Bill's script to place the files on the Netlogon share of the domain controllers.
Configure auditing on the domain controllers to record success and failure of Account Logon.
- C. Run Microsoft Baseline Security Analyzer (MBSA) on the subnets that make up SiteB.
- D. Write a script that runs both the qfecheck and winver commands on each computer in SiteB.
- E. Modify Mr Bill's script to apply all updates except the conflicting update.
Create a Group Policy object (GPO) and link it to the domain that runs the script as a logon script.

Answer: C

Explanation:

The Microsoft Baseline Security Analyzer tool (MBSA, or Mbsa.exe) tool centrally scans Windows-based computers for common security misconfigurations. MBSA can be used to scan for Windows Operating System checks, IIS checks, SQL checks, Hotfix checks, and Password checks.

In this scenario we can configure MBSA to run on all computers at SiteB. This is a practical solution with a low amount of administrative effort.

Microsoft Baseline Security Analyzer

Pick multiple computers to scan

Specify the computers you want to scan. You can enter either the domain name where the computers are located or an IP address range.

Domain name:

IP address range: to

Security report name:

Options:

Check for Windows vulnerabilities

Check for weak passwords

Check for IIS vulnerabilities

Check for SQL vulnerabilities

Check for security updates

Use SUS Server:

[Learn more about Scanning Options](#)

Start scan

Incorrect Answers

- A: This would not give enough information.
- B: Auditing Domain logon would not be of much help in this scenario.
- D: The qfecheck.exe tool is used to verify the installation of Hotfixes while winver only provides the current Windows version. The information would not be so useful here.
- E: We don't want to apply any changes. We just want to check the current situation.

QUESTION 98:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

From a Windows 2000 Professional client computer in the domain, you want to find out the hotfix status of other computers in the domain. When you use Microsoft Baseline Security Analyzer (MBSA) to scan a Windows 2000 Server computer named Certkiller 1, you receive the error message that you are not an administrator on the scanned computer.

You want to ensure that you can find the hotfix status of Certkiller 1 from the Windows 2000 Professional computer.

What should you do?

- A. Run the runas command to start MBSA and specify local administrator credentials for Certkiller 1.
- B. Run the net use command to specify local administrator credentials for a connection to

Certkiller 1, then run MBSA.

C. Run the hfnetchk command and specify local administrator credentials for Certkiller 1 to connect to and scan Certkiller 1.

D. Run the mbsacli command to connect to and scan Certkiller 1.

Answer: C

Explanation:

The Hfnetchk command line tool is used to assess hotfix patch status. It can be used to access hotfix patch status for remote computers. The [-u username] and [-p password] switches are used to specify the appropriate login information.

```
Select C:\WINNT\system32\cmd.exe
Microsoft Baseline Security Analyzer
Version 1.2 (1.2.3316.1)
(C) Copyright 2002-2004 Microsoft Corporation. All rights reserved.
HFNetChk developed for Microsoft Corporation by Shavlik Technologies, LLC.
(C) Copyright 2002-2004 Shavlik Technologies, LLC. www.shavlik.com

mbsacli /hf [-h hostname] [-i ipaddress] [-d domainname] [-n]
[-r range] [-history level] [-t threads] [-b] [-sus]
[-o output] [-x datasources] [-z] [-v] [-s suppression]
[-nosum] [-sum] [-u username] [-p password] [-f outfile]
[-fh Hostfile] [-fip ipfile] [-about] [-fq Ignorefile]
[-unicode]
```

Reference:

Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available, Microsoft Knowledge Base Article - Q303215

Microsoft Baseline Security Analyzer (MBSA) Version 1.0 Is Available. Microsoft Knowledge Base Q320454

Incorrect Answers

A: The runas command is not useful. We must use the command line version of MBSA, mbsacli, to assess the hot fix patch status of remote computers.

B: It is not useful to map a connection to ServerA. We must use the command line version of MBSA, mbsacli, to assess the hot fix patch status of remote computers.

D: The mbsacli tool is the command line tool version of MBSA.

QUESTION 99:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain Certkiller .com. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers. The network also contains Windows XP Professional client computers that are not joined to the domain. The Windows XP computers are not using Internet Connection Firewall.

From a Windows 2000 Professional client computer in the domain, you regularly run Microsoft Baseline Security Analyzer (MBSA) to verify the hotfix status of computers in the domain. You want to look at the hotfix status of the Windows XP Professional computers as well.

You log on to the Windows 2000 Professional computer with a local administrator account. The same user name and password combination as you used on the Windows 2000 Professional computer is also defined as a local administrator

account on the Windows XP Professional computers. However, when you run MBSA and connect to the Windows XP computers, you receive an error message stating that you are not an administrator on the scanned computers.

You want to ensure that you can find out the hotfix status of the Windows XP computers from the Windows 2000 Professional computer.

What should you do?

- A. On the Windows 2000 Professional computer, run the net use command to specify the local administrator credentials for connections to the Windows XP computers. Then, run MBSA.
- B. On the Windows 2000 Professional computer, run the hfnetchk command and specify the local administrator credentials.
- C. On the Windows XP Professional computers, disable the use of simple file sharing.
- D. On the Windows XP Professional computers, copy the Mssecure.cab file to the System32 folder.

Answer: C

Explanation:

The question basically asks why you can't do a network scan with MBSA from a Win2K machine of WinXP machines. The actual answer is C. Simple File sharing must be disabled on Windows XP (Pro and Home) in order to do a network scan. You can only do a local scan if it's enabled.

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod112.asp>

What You Must Know

Before using this How To, you should be aware of the following:

* You can use MBSA by using the graphical user interface (GUI) or from the command line. The GUI executable is Mbsa.exe and the command line executable is Mbsacli.exe.

* MBSA uses ports 138 and 139 to perform its scans.

* MBSA requires administrator privileges on the computer that you scan. The options /u (username) and /p (password) can be used to specify the username to run the scan. Do not store user names and passwords in text files such as command files or scripts.

* MBSA requires the following software:

* Windows NT 4.0 SP4 and above, Windows 2000, or Windows XP (local scans only on Windows XP computers that use simple file sharing)

If you simply shut off simple file sharing on the Windows XP machines, MBSA would be able to scan the XP computers.

QUESTION 100:

You are the network administrator for Certkiller . The network contains 500 Windows XP Professional computers and four Windows 2000 Server computers. All computers use Internet Explorer as their default browser.

For security reasons, the four servers are located on an isolated network subnet. The four servers are accessible to other local network subnets, but a firewall runs on the network.

The firewall prevents the servers from accessing the Internet. All other local subnets have access to the Internet through Certkiller Internet connection.

You receive a notice that a critical security update is available for Windows 2000 Server. The update is available on <http://windowsupdate.microsoft.com>.

You need to download the update so that you can install it on the four Windows 2000 Server computers as quickly as possible. You also need to maintain the security of the isolated subnet that contains the servers.

What should you do?

- A. On each Windows 2000 Server computer, use the route command to add a route to Certkiller Internet router.
Then, use Microsoft Internet Explorer to connect to <http://windowsupdate.microsoft.com>.
- B. On each Windows 2000 Server computer, add an entry for windowsupdate.microsoft.com to the local host file.
Then, use Internet Explorer to connect to <http://windowsupdate.microsoft.com>.
- C. On a Windows XP Professional computer, use Internet Explorer to enable the Windows Update Catalog on <http://windowsupdate.microsoft.com> and download the critical security update.
- D. Install Windows 2000 Server on a new computer.
Connect the new computer to a local subnet that has Internet access.
Use Internet Explorer to connect to <http://windowsupdate.microsoft.com>.

Answer: C

Explanation:

We download the update from a client computer. We then make the update available to the four servers within the LAN.

Incorrect Answers

A, B: The firewall would still stop Internet traffic to the four Windows 2000 servers.

D: It is not necessary to install Windows 2000 Server on a computer. We can download the update from a client computer.

QUESTION 101:

You are the network administrator for Certkiller . The network contains 300 Windows XP Professional computers. You receive two new hotfixes for these computers: HotfixA and HotfixB. Each hotfix modifies some of the same operating system files and requires the computer to be restarted for the hotfix to take affect. HotfixA must be installed before HotfixB.

You need to install each hotfix on all client computers. You decide to write a startup script that will install the hotfixes. You want the hotfixes to be installed with the minimum number of restarts.

How should the startup script install the hotfixes?

- A. Check whether HotfixA is already installed.
If it is installed, install HotfixB.
If it is not installed, install HotfixA.
- B. Install HotfixA by using the command-line switch that prevents an automatic restart.

Then, install HotfixB.

C. Run the qchain.exe command.

Install both HotfixA and HotfixB by using the command-line switch that prevents an automatic restart.

Run the shutdowncommand to restart the computer.

D. Install both HotfixA and HotfixB.

Run the qchain.exe command.

Run the shutdown command to restart the computer.

Answer: D

Explanation:

To Install Multiple Hotfixes with Only One Reboot

1. Run the hotfix installer with the -z switch to instruct the installer not to reboot after the installation.

2. After all of the hotfixes have been installed, run QChain.exe.

3. Reboot the computer.

Reference:

Use QChain.exe to Install Multiple Hotfixes with Only One Reboot, Microsoft Knowledge Base Article - Q296861

Incorrect Answers

A, B: We must use Qchain.exe.

C: Qchain should be run after installing the hotfixes..

QUESTION 102:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain Certkiller .com. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

You regularly check the hotfix status of computers on the network. For a Windows 2000 Server computer named Certkiller 1, several error messages appear that report checksum differences in third-party device driver files. However, the versions of the device driver files on Certkiller 1 are the same. You suspect that a malicious administrator has replaced some of the device driver files on Certkiller 1.

You want to find out whether the files described in the error messages are the original Microsoft files.

What should you do?

A. Run the sfc.exe command to check the files.

B. Run the sigverif.exe command to check the files.

C. Use Device Manager to scan for hardware changes.

D. Configure the driver-signing options to prevent installation of unsigned files.

Answer: B

Explanation:

You can use sigverif.exe to identify unsigned drivers on a Windows-based computer.
Reference: How to Use the File Signature Verification Tool to Find Third-Party Drivers,
Knowledge Base Article - Q259283

Description of the Windows 2000 Windows File Protection Feature, Microsoft
Knowledge Base Article - Q222193

Incorrect Answers

A: System File Checker (sfc.exe) checks for damaged or replaced system files, and then prompts you to replace any files that do not match the original Windows files. Sfc.exe does not check device drivers.

C: We want to check software, the device drivers, not the hardware.

D: Unsigned drivers have already been installed.

QUESTION 103:

You are the network administrator for Certkiller . Your network consists of a Windows 2000 Active Directory domain. The domain contains three domain controllers, one Windows 2000 Server computer configured as an intranet Web server, and 500 Windows 2000 Professional client computers.

You must install five hotfixes on your intranet Web server. Two of the hotfixes modify some of the same files. Your manager wants you to minimize the time that the intranet Web server is offline.

What should you do?

A. Apply the hotfixes to your intranet Web server with the switch that prevents a restart. Run the netdiag /v /fix command on the intranet Web server. Restart the intranet Web server.

B. Apply the hotfixes to your intranet Web server with the switch that prevents a restart. Run the qchain.exe command on the intranet Web server. Restart the intranet Web server.

C. Run the qchain.exe command on the intranet Web server. Apply the hotfixes to your intranet Web server with the switch that prevents a restart. Run the netdiag /v /fix command on the intranet Web server. Restart the intranet Web server.

D. Run the qfecheck.exe command on the intranet Web server. Apply the hotfixes to your intranet Web server with the switch that prevents a restart. Run the qfecheck.exe command on the intranet Web server. Restart the intranet Web server.

Answer: B

Explanation:

To Install Multiple Hotfixes with Only One Reboot

1. Run the hotfix installer with the -z switch to instruct the installer not to reboot after the installation. Add the -m switch (for Quiet mode) in addition to the -z switch if you do not want to see prompts or messages during the installation.

The hotfix installer is either:

o The self-extracting package program file (for example, Qnnnnnn_w2k_spx_x86_en.exe)

or

o Hotfix.exe (if you have extracted all of the files from the package)

2. After all of the hotfixes have been installed, run QChain.exe.

3. Reboot the computer.

Note: Microsoft has released a command-line tool named QChain.exe that gives system administrators the ability to safely chain hotfixes together. Hotfix chaining involves installing multiple hotfixes without rebooting between each installation. Without this tool, the only supported method is to reboot after each hotfix installation.

Reference:

Use QChain.exe to Install Multiple Hotfixes with Only One Reboot, Microsoft Knowledge Base Article - Q296861

Qfecheck.exe Verifies the Installation of Windows 2000 and Windows XP Hotfixes, soft Knowledge Base Article - Q282784

Incorrect Answers

A: We must use the Qchain.exe tool.

C: Qchain.exe should be run after all hotfixes have been installed.

D: Qfecheck.exe network administrators increased ability to track and verify installed Windows 2000 and Windows XP hotfixes. However, we must use the Qchain.exe tool to apply several hotfixes without rebooting.

QUESTION 104:

You are the network administrator for Certkiller . Your network consists of a Windows 2000 Active Directory domain. Certkiller has three departments: research, sales, and operations. Each department has an organizational unit (OU) in the domain that contains all user and group accounts for that department. All computer accounts are in the Computer container.

The network contains two Windows 2000 Server computers, named Certkiller 1 and Certkiller 2, configured as domain controllers. One Windows 2000 Server computer, named Certkiller 3, is configured as a file server. Certkiller 3 contains a distribution share containing the Windows 2000 Professional installation files, the latest service pack files applies to the installation files, and unattended answer file, and uniqueness database file.

The network contains 1,500 Windows 2000 Professional client computers, which were installed from the distribution share on Certkiller 3.

Certkiller receives 25 new computers for the research department. These new computers require the latest service pack and a security update for a service that only these new client computers run. You must place the computer accounts for these client computers in the Research OU. You must ensure that these new client computers have the latest service pack and the security update.

You want to install these computers and software by using a network boot disk. What should you do?

A. Copy the update executable to the distribution share on Certkiller 3.

Use the existing answer file and uniqueness database file to install each client from the distribution share by using a network boot disk.

Move each new client computer account to the Research OU after its installation.

B. Use the existing answer file and uniqueness database file to install each client from a network boot disk.

Create a new Group Policy object (GPO) and link it to the Research OU.

Configure the GPO with a software installation package for the latest service pack.

C. Create an \$OEM\$ folder in the existing distribution share on Certkiller 1 and copy the update into the folder.

Use Setup Manager to create an answer file and a uniqueness database file.

Specify the appropriate hotfix executable as a program to run after installation in Setup Manager.

Set the OemPreinstall = Yes value in the answer file.

Copy the answer file to the distribution share.

Run the winnt.exe command on each new client computer with the appropriate unattended installation switches.

Move the client computers into the Research OU.

D. Create an \$OEM\$ folder in the existing distribution share on Certkiller 1 and copy the update into the folder.

Use Setup Manager to create an answer file and a uniqueness database file.

Specify the appropriate update executable as a program to run after installation in Setup Manager.

Set the OemPreinstall = No value in the answer file.

Copy the answer file to the distribution share.

Run the winnt32.exe command on each new client computer with the appropriate unattended installation switches.

Move the client computer accounts into the Research OU.

Answer: C

Explanation: We must use winnt.exe to install Windows from the distribution folder. Furthermore, we must use the OemPreinstall = Yes to perform an unattended installation.

Incorrect Answers

A, B: The new computers are not present in the uniqueness database.

D: Winnt32.exe can only be used from within Windows, not when starting a fresh installation of Windows. Also we must use the OemPreinstall = Yes to perform an unattended installation.

QUESTION 105:

You are the network administrator for Certkiller . The network contains a Windows 2000 Server computer named Certkiller 1. Certkiller 1 runs Remote Installation Services (RIS). You use Certkiller 1 and a RIS image to install Windows 2000 Professional on new computers that Certkiller purchases.

You download a new Windows 2000 security update from the Microsoft Web site. You

want to ensure that the update is installed automatically on all new computers. What should you do?

- A. Install the security update on Certkiller 1.
Restart Certkiller 1.
- B. Copy the security update files to a new shared folder named \\ Certkiller 1\SvcPack\i386.
Restart RIS on Certkiller 1.
- C. Install the security update on a model Windows 2000 Professional computer.
Create a new RIS image of the computer.
Delete the original RIS image.
- D. Install the security update on a model Windows 2000 Professional computer.
Run the sysprep command on the computer and select the Reseal option.

Answer: C

Explanation:

We need to create a new RIS image. We create it from a model Windows 2000 Professional computer, on which we have installed the Windows 2000 Security updates.

Reference:

Description of New Features in Sysprep for Windows XP - Microsoft Knowledge Base Article - 282190

Incorrect Answers

A: We want the security applied on the client computer, not on the RIS server.

B: We need to create a new image.

D: Sysprep has four basic modes: Audit Mode, Clean Mode, Factory Mode, and Reseal Mode.

Reseal is run after an original equipment manufacturer (OEM) has run Sysprep in factory mode and is ready to prepare the computer for delivery to a customer.

QUESTION 106:

You are the network administrator for Certkiller . The network includes a file server named Certkiller 1. Certkiller 1 contains a shared folder named Win2000. The shared folder contains a subfolder named Server, which contains the i386 folder from the Windows 2000 Server CD-ROM. The Win2000 shared folder also contains a subfolder named Pro, which contains the i386 folder from the Windows 2000 Professional CD-ROM. You use these two i386 folders as the source for operating system installations.

You download a new Windows 2000 service pack from the Microsoft Web site. You expand the service pack into \\ Certkiller 1\Win2000\SP.

You want to ensure that all future operating system installations and upgrades incorporate the new service pack.

What should you do?

- A. From the \\ Certkiller 1\Win2000\SP\i386 folder, run the update.exe

/s:\\ Certkiller 1\win2000 command.

B. From the \\ Certkiller 1\Win2000\SP\i386 folder, run the update.exe

/s:\\ Certkiller 1\win2000\server command.

Then, run the update.exe /s:\\ Certkiller 1\win2000\pro command.

C. Copy the files from the \\ Certkiller 1\Win2000\SP\i386 to the \\ Certkiller 1\Win200\Server\i386 folder.

Then, copy the same files to the \\ Certkiller 1\Win200\Pro\i386 folder.

D. On a Windows 2000 Server computer, run the \\ Certkiller 1\Win2000\SP\i386\update.exe command.

Then, on a Windows 2000 Professional computer, run the \\ Certkiller 1\Win2000\SP\i386\update.exe command.

E. Copy the service pack to the \\ Certkiller 1\Win2000\Server\i386 folder and the \\ Certkiller 1\Win2000\Pro\i386 folder.

From the \\ Certkiller 1\Win2000\Server\i386 folder, run the update.exe command.

Then, from the \\ Certkiller 1\Win2000\Pro\i386 folder, run the update.exe command.

Answer: B

Explanation:

We must slipstream the service packs to both installation folders. The update.exe command with the slipstream switch /s performs the service pack slipstreaming. The update.exe command must be run from the folder with the service packs.

Note: To perform a slipstream installation:

1. Create a distribution folder (C:\Win2000), and share, on your Windows 2000 'server' and

XCOPY <Windows 2000 CD_ROM Drive:>\ c:\Win2000 /e.

2. Slipstream the service pack by running

<Windows 2000 Service Pack CD_ROM Drive:>\Update.exe /s:C:\Win2000.

3. Install Windows 2000 from the distribution share.

Incorrect Answers

A: We must slipstream both installation folders

C: Just copying the service pack files will not apply the service pack

D, E: We must use the slipstream switch /s with the update.exe command.

QUESTION 107:

You are the network administrator for Certkiller . Your network consists of a Windows 2000 Active Directory domain. Certkiller has three departments: research, sales, and operations. Each department has a separate organizational unit (OU) in the domain that contains all user and group accounts for that department.

The network includes two Windows 2000 Server computers configured as domain controllers. One Windows 2000 Server computer, named Certkiller 3, is running Remote Installation Services (RIS) and the DHCP service. The network also contains 1,500 Windows 2000 Professional client computers, which were installed from CD-based RIS images stored on Certkiller 3.

Certkiller receives 25 new computers of the same type that you are using for your

network client computers. You prepare to install 25 new Windows 2000 Professional client computers. You must place the computer accounts for these client computers in the Research OU. All these client computers require a custom set of applications and the latest service pack.

You install Windows 2000 Professional on a client computer and name the computer CK1 . You install and configure all the custom applications and the latest service pack on CK1 .

You want to install the required applications and the service pack on the rest of the new client computers with the least amount of administrative effort.

What should you do?

- A. Create new Group Policy objects (GPOs) and link them to the Research OU. Configure a GPO with an installation package for each required application and the service pack.
- B. Create an unattended answer file based on the configuration of CK1 . Save that answer file as Risetup.sif and associate it with the CD-based RIS image on Certkiller 3. Use the CD-based RIS image to install the software on each new client computer.
- C. Copy the contents of the Windows 2000 Professional CD-ROM to a folder on Certkiller 3. Slipstream the latest service pack to that folder. Create a new RIS image from that folder. Run the riprep command on CK1 to create a new image on Certkiller 3. Use the riprep image to install the new client computers.
- D. Install the new client computers by using the existing CD-based RIS image on the RIS server. Install each required application on each client manually. Create a new Group Policy object (GPO) and link it to the domain. Configure the GPO with a software installation package for the latest service pack.

Answer: C

Explanation:

First we create a CD-ROM-based RIS image that has a slipstreamed service pack. We then create a riprep CD image based on the CK1 client computer. We use this image to install the other computers identically as CK1 .

Reference:

Slipstream Switch for Windows 2000 Service Pack Update.exe Does Not Work with RIS Server Images, Microsoft Knowledge Base Article - Q258868

Incorrect Answers

A: We must install Windows on these computers before installing the applications and the service pack.

B: The unattend.txt file cannot be used to the Application and the service pack.

D: Manually installing each application on each client would not minimize administration

QUESTION 108:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains five domain controllers, 1,500 Windows 2000 Professional client computers, and one Windows 2000 Server computer configured as an Internet Web server.

You update the Web server by using the Windows Update service to download all critical updates, software, and service packs. You want to apply the latest hotfixes to your Web server each night at midnight.

What should you do?

- A. Create a Microsoft Visual Basic script to connect the Web server to windowsupdate.microsoft.com, then run the hfnetchk command on the Web server every night at midnight.
- B. Configure the Automatic Updates feature to run on the Web server every night at midnight.
- C. Use the Scheduled Tasks utility to run the mbsaclcommand on the Web server every night at midnight.
- D. Schedule a batch file to run the netdiag command on the Web server every night at midnight.

Answer: B

Explanation:

We should use the Automatic Update and schedule it to run every night.

QUESTION 109:

You are the network administrator for Certkiller . The network contains 500 Windows XP Professional computers. All client computers are configured to use the Automatic Update service and to notify users before downloading updates. All client computers are also configured so that users cannot directly access http://windowsupdate.microsoft.com.

An employee named Bruno is notified of a new security update and, when prompted, accidentally declines to install it. Bruno reports that the Automatic Update service is able to install additional updates, but the security update he declined is no longer listed.

You want to ensure that the security update is listed.

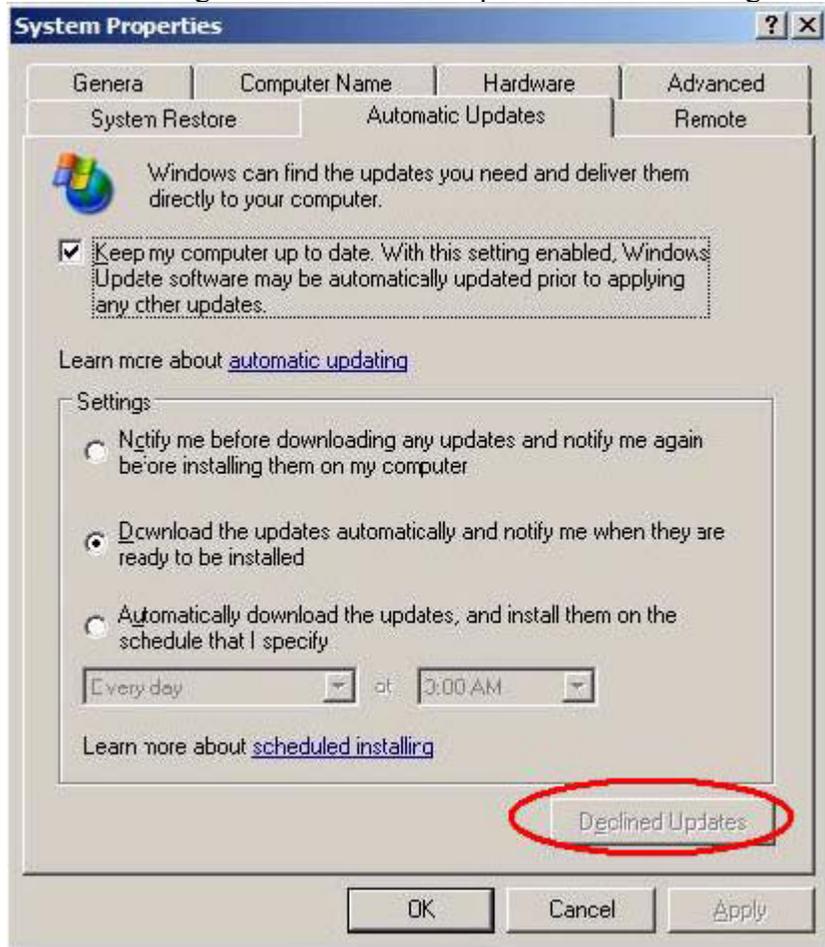
What should you do?

- A. Use Registry Editor to delete the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates registry key. Restart the computer.
- B. On the Automatic Updates tab of System Properties, restore the update.
- C. Open the Systemroot\Temp folder. Locate and delete any Setup.exe files.
- D. Run the qfecheck.exe /l /q /c command. Restart the computer.

Answer: B

Explanation:

If Bruno got the possibility to decline the installation of the update then it means that Bruno is an user with administrative permissions. Otherwise that button would be greyed out. So he can go to the Automatic Updates Tab and configure it.



Reference:

Knowledge base article 282784 Qfecheck.exe Verifies the Installation of Windows 2000 and Windows XP Hotfixes.

Incorrect Answers:

- A. Deleting this key will cause all updates to be re-installed.
- C. Not applicable here
- D. There is no /c option for the qfecheck command line.

QUESTION 110:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 10 Windows 2000 Server computers that act as file servers. All of the computer accounts for these file servers are located in an organizational unit (OU) named File_Servers.

You create a new security template named Sec_file.inf to all Windows 2000 file servers.

However, before the security template is applied, you need to create a report of each change the template will make to the servers.

What should you do?

- A. On each file server, run the `secedit /validate sec_file.inf` command.
- B. On each file server, use the Security Configuration and Analysis console in conjunction with the `Sec_file.inf` template to analyze that server.
- C. Import the `Sec_file.inf` file to the Default Domain Policy Group Policy object (GPO) and select the No Override check box.
- On each file server, run the `gpresult.exe /v /c` command.
- D. Create a Group Policy object (GPO) and link it to the `File_Servers` OU. Import the `Sec_file.inf` file to the new GPO. In the properties for the `File_Servers` OU, select the Block Policy inheritance check box. On each file server, run the `gpresult.exe /v /c` command.

Answer: B

Explanation:

The question states : "before the security template is applied". So before we put the template into a GPO we must analyze what changes it will make. We can do this with the Security Configuration and Analysis console.

Incorrect Answers

A: The `secedit /validate` command only validates the syntax of a security template you want to import into a database for analysis or application to a system

C: We do not want to apply the GPO to the whole domain, only the file servers in the `File_Server` OU.

D: The question states : "before the security template is applied". So before we put the template into a GPO we must analyze what changes it will make. The `gpresult.exe` command-line tool displays information about the result Group Policy has had on the current computer and logged-on user. (so AFTER the GPO has been applied)

QUESTION 111:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains two domain controllers and two Windows 2000 Server computers. One server is configured as a file server named Certkiller 1, and the other server is configured as an intranet Web server. In addition, the network contains 50 Windows XP Professional client computers.

All but five client computers receive scheduled automatic updates. The five client computers that are not updated automatically are on an isolated LAN segment that is not connected to the Internet. The client computers on the isolated LAN have access to Certkiller 1 and the intranet Web server.

You want to apply three security updates on these client computers.

What should you do?

- A. From a computer connected to the Internet, download and copy the security updates to

a network share on Certkiller 1.

Run Windows Update on the client computers located on the isolated LAN.

B. From a computer connected to the Internet, download and copy the security updates to a network share on Certkiller 1.

Connect each client computer on the isolated LAN to the network share and apply each update individually.

C. From a computer connected to the Internet, download the XML security database from the Microsoft Web site.

Share this database on the intranet Web server.

Connect each client computer on the isolated LAN to the intranet Web server.

Run the qchain.exe command on each client computer on the isolated LAN.

D. From a computer connected to the Internet, download the XML security database from the Microsoft Web site.

Place the XML security database in the C:\inetpub folder on the intranet Web server.

Connect each client computer on the isolated LAN to the Default Web site in the intranet Web server.

Run the Windows Update service on the client computers on the isolated LAN.

Answer: D

Explanation: .

Software Update Services (SUS) allows information technology professionals to configure a server that contains content from the live Windows Update site in their own Windows-based intranets to service corporate servers and clients. SUS manages and distributes critical Windows patches.

We need to install the updated

Automatic Updates client that can pull updates from the internal SUS server.

We should configure the client computers, preferably through a GPO, to receive automatic updates from the Web server which acts as a SUS server.

Reference:

Software Update Services Deployment White Paper

Software Update Services Overview White Paper

Incorrect Answers

A: Windows update can only be run on computers that can access the Microsoft Internet site.

B: This proposed solution requires a lot of administrative work.

C: This is not the way we should configure the clients. Qchain.exe does not apply here.

QUESTION 112:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain.

Certkiller purchases 50 new client computers each month. These computers come installed with Windows 2000 Professional. You add the computers to the domain as soon as they arrive and place their computer accounts in an organizational unit (OU) named Desktops.

You want to ensure that all new computers receive the latest service pack as soon as possible. You want to accomplish this task by using the least amount of administrative effort required to install service packs on new computers each month.

What should you do?

- A. Install Critical Update Notification on each computer.
- B. Create a Group Policy object (GPO) and link it to the Desktops OU. Configure the GPO to assign the latest service pack to computers.
- C. For each new service pack, run its update.exe command on each domain controller.
- D. For each new service pack, copy its files to a shared folder. On each new computer, connect to the shared folder and run the update.exe command.

Answer: B

Explanation:

We should use a GPO to assign the latest service pack to the clients throughout the domain.

QUESTION 113:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains three domain controllers, four Windows 2000 member servers, and 350 Windows 2000 Professional client computers. A firewall at the perimeter of the network controls inbound and outbound access to the Internet.

All the computer accounts and user accounts for the research department are in an organizational unit (OU) named Research. You give users who have user accounts in the Research OU local administrative access to their client computer so they can install software. However, you do not want any of these users to use the Windows Update service.

You want only the default administrator account from the domain to be able to use Windows Update.

What should you do?

- A. Block the outbound NetBIOS ports on the firewall. Disable outbound access to the windowsupdate.microsoft.com domain.
- B. Block the inbound NetBIOS ports on the firewall. Disable outbound access to the windowsupate.microsoft.com domain.
- C. Create a Group Policy object (GPO) and link it to the domain. Configure the GPO to enable the Disable and remove links to Windows Update policy.

Answer: C

Explanation:

The Disable and remove links to Windows Update policy disables access to the Windows Update tool.

Reference: Group Policy Does Not Disable All Windows Update Components,
Microsoft Knowledge Base Article - Q279006

Incorrect Answers

A, B: Blocking NetBIOS ports would not make any distinction between different user accounts. It is not a plausible solution.

QUESTION 114:

You are the network administrator for Certkiller . Certkiller network contains 1,000 Windows XP Professional computers and 2,500 Windows 2000 Professional computers. The network is connected to the Internet by means of a 512-Kbps connection. All computers use Internet Explorer as their default browser.

Ten new security updates are releases for Windows XP Professional and Windows 2000 Professional. The updates are available on <http://windowsupdate.microsoft.com> for both operating systems. However, you decide to deploy the updates internally so that each user does not have to connect to the Web site.

You use Internet Explorer on a Windows XP Professional computer to connect to windowsupdate.microsoft.com. However, the Web site offers only the option to apply the updates to the local computer.

You want to download the updates so that you can apply them to each client computer.

What should you do?

- A. On each Windows XP Professional computer, enable Automatic Updates. On each Windows 2000 Professional computer, enable Critical Update Notification.
- B. Use the Web site to download and install the updates on the local computer. After the update completes, locate the downloaded files on the computer's hard disk and copy them to a shared folder.
- C. Use the Web site to download and install the updates on the local computer. Before the computer restarts, locate the downloaded files on the computer's hard disk and copy them to a shared folder.
- D. On the Web site, select the option to personalize the site. Then, select the option to display Windows Update Catalog and download the updates to a shared folder.

Answer: D

Explanation:

You can search the Windows Update Catalog to find updates that you can download and install later on Windows-based computers across your home or corporate network.

To Add the Windows Update Catalog to Windows Update:

1. Visit the following Microsoft Windows Update Web site:
<http://v4.windowsupdate.microsoft.com>
2. Click Personalize Windows Update.
3. Click to select the Display the link to the Windows Update Catalog under See Also

check box.

4. Click Save Settings. A Windows Update Catalog link appears under See Also.

Reference:

HOW TO: Download Windows Updates and Drivers from the Windows Update Catalog on Windows 2000, Microsoft Knowledge Base Article - Q326426

Incorrect Answers

A: We only want to download the updates once, not one time for each computer.

B, C: There is no need to set up manually like this. We should use the Windows Update Catalog feature.

QUESTION 115:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active directory domain. All client computers are in an organizational unit (OU) named Clients.

The network contains two Windows 2000 Server computers configured as domain controllers. One Windows 2000 Server computer is configured as a file server. The network also contains 1,500 Windows 2000 Professional client computers.

You use a Group Policy object (GPO) named SPDeploy to deploy a new service pack. SPDeploy is linked to the Clients OU. All client computers receive the new service pack.

One network user reports problems after the installation of the new service pack.

You discover that this user's computer has hardware that is incompatible with the new service pack. No other users on the network are experiencing difficulty.

You must remove the service pack from this user's computer but ensure that it remains on the other computers.

What should you do?

A. Remove the service pack from the user's computer by using Add/Remove Programs. Configure the DACL on SPDeploy to grant the user account Read and Apply Group Policy permissions.

B. Remove the service pack from the user's computer by using Add/Remove Programs. Configure the DACL on SPDeploy to deny the user account Read and Apply Policy permissions.

C. Create an OU named NoSP subordinate to the domain. Move the problem user's computer account into the NoSP OU.

Remove the service pack from the user's computer by using Add/Remove Programs.

D. Create an OU named NoSP subordinate to the Clients OU.

Move the problem user's computer account into the NoSP OU.

Remove the service pack from that user's computer by using Add/Remove Programs.

Answer: C

Explanation:

We move this particular computer account to a separate OU on which the SPDeploy GPO is not applied. This ensures that the service not will be reinstalled later. We must also

manually remove the service pack from the computer.

Incorrect Answers

A: Read and apply group policy to the GPO would ensure that GPO would be applied.

This is not our desired goal.

B: This prevents this particular user, not the computer, from using the GPO.

D: As the new OU is a child OU of the Clients OU, the SPDeploy GPO would be applied to the new OU as well.

QUESTION 116:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain includes two domain controllers and 50 Windows XP Professional client computers.

All computers on the network have the latest service packs and security updates installed. All computers on the network have access to the Internet. All computers remain on 24 hours a day, but Certkiller is closed from 10:00 P.M to 6:00 A.M. All users are members of the Domain Users group only.

You are responsible for ensuring that the latest updates are applied to all client computers on your network. Your manager wants these updates to be applied in a decentralized manner, either by the user or automatically.

What should you do?

A. Use the Scheduled Tasks utility to run a batch file in the security context of the user account that connects to windowsupdate.microsoft.com.

B. Configure Automatic Updates feature to download and automatically update the client computers during the night when users are not at their computers.

C. Configure the Domain Security Policy to enable the Disable and remove links to Windows Update policy.

Ask the users to run the Windows Update service daily.

D. Configure the Domain Security Policy to disable the Disable and remove links to Windows Update policy.

Ask the users to run the Windows Update service daily.

Answer: B

Explanation:

Normally Automatic Updates are performed in the background at unscheduled occasions.

In this scenario we schedule this update to the night.

The users would still be able to apply manual update if they wish.

Incorrect Answers

A: This is a primitive solution. The functionality is already included in Windows XP so there is no need to use batch files.

C: Enabling the Disable and remove links to Windows Update policy would disable Windows update.

D: We should not rely only on the users. We must enable Windows to automatically update the client computers.

QUESTION 117:

You are the new network administrator for Certkiller . The network consists of a single subnet and a Windows 2000 Active Directory domain. The network contains 400 Windows XP Professional computers. The domain includes an organizational unit (OU) named ClientComputers. The ClientComputers OU contains all client computer accounts. All client computers receive IP configuration from a DHCP server.

The domain also includes an OU for each company department. Each department OU contains that department's user accounts. All departments OUs are linked to Group Policy objects (GPOs) that provide configuration settings to the objects in the OU.

Users in the accounting department report that they cannot download a new update from <http://windowsupdate.microsoft.com>. The update repairs a problem that prevents a company application from printing correctly. Users in other departments are able to download and apply the update.

You need to ensure that all users can download and apply updates from <http://windowsupdate.microsoft.com>.

What should you do?

- A. Configure the firewall to permit outbound access to windowsupdate.microsoft.com.
- B. On the desktop of each client computer in the accounting department, create a shortcut to <http://windowsupdate.microsoft.com>.
- C. On each client computer, use the route command to configure a route to the Windows Update Web site that uses the network's Internet router as the gateway.
- D. Create a GPO and link it to the ClientComputers OU. Configure the GPO to place the Domain Users group in the local Administrators group on each client computer.

Answer: D

Explanation:

Making the Domain Users member of the local Administrator group would enable the installation of update package.

Incorrect Answers

A: Other users can access windowsupdate.microsoft.com so there is no need of any firewall reconfiguration.

B: Making a shortcut would not enable downloading.

C: It is not necessary to add route to specific web sites. Client computers need a configured default gateway.

QUESTION 118:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains two domain controllers CK1 and CK2 , one Windows 2000 Server computer configured as an intranet Web server, and 500

Windows XP Professional client computers.

All client computers remain on 24 hours a day, but business hours are from 8:00

A.M to 5:00 P.M. Your supervisor wants you to automate the installation of security updates to all client computers on the network.

What should you do? (Each correct answer presents part of the solution. Choose three)

A. Install and configure Microsoft Software Update Services (SUS) on the intranet Web server to synchronize each night at midnight.

Configure the service to automatically approve new updates.

B. Configure a Group Policy object (GPO) and link it to the domain.

Configure the GPO with a software distribution package containing the Microsoft Automatic Updates installer.

Assign this software to the computers.

C. Write a batch file to download all new security updates each night at midnight.

Configure the batch file to place the new security updates in the Sysvol share of both domain controllers.

D. Configure client computers to receive automatic updates from the intranet Web server each night at midnight.

Restart all client computers.

E. Configure client computers to receive automatic updates from either domain controller each night at midnight.

Restart the client computers.

F. Run the Microsoft Baseline Security Analyzer (MBSA) for all segments on the domain from any domain computer each night at midnight.

G. Write a batch file that runs the qchain.exe command each night at midnight.

Create a new Group Policy object (GPO) and link it to the domain.

Configure the GPO to run the script as a logon script.

Answer: A, B, D

Explanation:

A: Software Update Services (SUS) allows information technology professionals to configure a server that contains content from the live Windows Update site in their own Windows-based intranets to service corporate servers and clients. SUS manages and distributes critical Windows patches.

B: We need to install the updated Automatic Updates client that can pull updates from the internal SUS server. Windows XP SP1 already has the updates client.

D: We should configure the client computers, preferably through a GPO, to receive automatic updates from the Web server which acts as a SUS server.

Reference:

Software Update Services Deployment White Paper

Software Update Services Overview White Paper

Incorrect Answers

C: It is not necessary to write a batch file. SUS contains these features already.

E: The updates are managed by the Web servers which acts as a SUS server. We are not using the domain controllers to receive the updates.

F: Microsoft Baseline Security Analyzer (MBSA) scans for missing hotfixes and vulnerabilities. However, it is not useful for automating security updates for an entire network.

G: There is no need to create a batch file. The functionality corresponding to the proposed batch file is already included in SUS.

QUESTION 119:

You are the network administrator for your Certkiller . The network consists of a Windows 2000 Active Directory domain. Certkiller has three departments: research, sales, and operations. Each department has a separate organizational unit (OU) in the domain that contains all user and group accounts for that department. Users do not have administrative access to their computers. Each OU has the Block Policy inheritance option selected.

The network includes two Windows 2000 Server computers, named Certkiller A and Certkiller B, configured as domain controllers. One Windows 2000 Server computer is configured as a file server named Certkiller C. Certkiller C has a distribution share folder that holds the contents of the Windows XP Professional installation CD-ROM. The network also contains 1,500 Windows XP Professional client computers, which were installed from the distribution share on Certkiller C.

You are installing 25 additional Windows XP Professional client computers in the Research OU. After 10 clients have been installed, a new service pack becomes available.

You want to install the service pack on all the new research department client computers as quickly as possible with the least amount of administrative effort. What should you do?

- A. Create a new Group Policy object (GPO) and link it to the domain.
Configure the GPO with a software installation package for the new service pack.
Move the computer accounts to the Research OU.
- B. Run the service pack's update /s command to update the distribution share on Certkiller 1.
Install all 25 new client computers from the distribution share on Certkiller C.
Move the computer accounts to the Research OU.
- C. Complete the installation of the remaining client computers.
Move the computer accounts to the Research OU.
Configure the Automatic Updates feature to run on each new computer every night at midnight.
- D. Complete the installation of the remaining client computers.
Move the computer accounts to the Research OU.
Instruct users to run the Windows Update service.

Answer: B

Explanation:

We should slipstream the service pack into the distribution share. We can then install the new client computers from this share. This will ensure that all clients will be installed

with the latest service pack.

Incorrect Answers

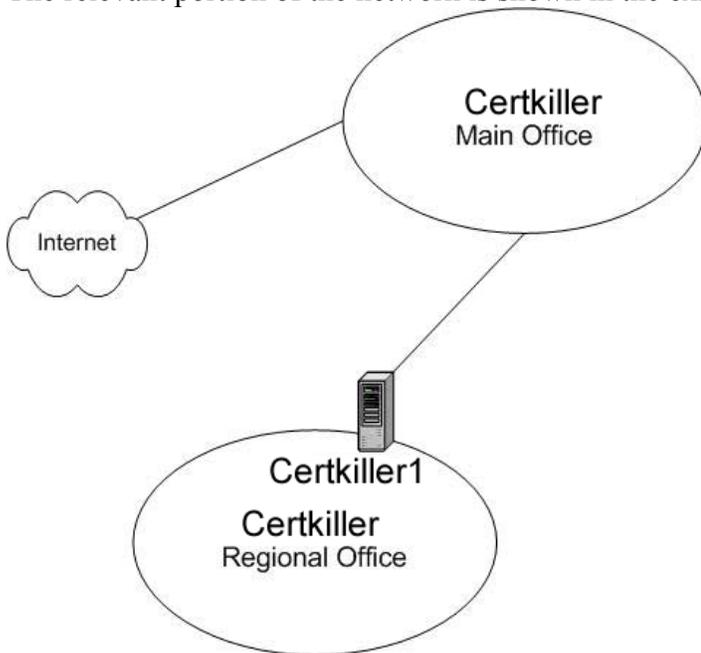
A: We are not required to deploy the service pack to all computers in the domain, just the new research client computers.

C: We should not put the clients into production without applying the latest Service pack.

D: We should not rely and require the Users to perform the necessary updates.

QUESTION 120:

You are the network administrator for a branch office of Certkiller . Certkiller has a main office and a regional office network. All computers at your regional office are configured with static IP addresses from the 10.168.1.0/24 subnet range. The relevant portion of the network is shown in the exhibit.



The regional office has a Windows 2000 Server computer named Certkiller 1 running Routing and Remote Access for Windows 2000. Certkiller 1 contains two network adapters that are used to connect the branch office to the main office.

You have portable computer with a dial-up connection and a network adapter. You use a dial-up connection to connect the portable computer to the Windows Update Web site. The portable computer also connects to your branch office by using the network adapter.

You replace the network adapter in Certkiller 1 for the main office connection. Now, Certkiller 1 cannot connect to the main office or the Internet. You realize that Certkiller 1 requires a driver and a security update that is available from the Windows Update site.

What should you do?

A. Enable Internet Connection Sharing on the portable computer.

Use Windows Update on Certkiller 1.

B. Enable Internet Connection Sharing on Certkiller 1.

Run the Microsoft Baseline Security Analyzer (MBSA) on Certkiller 1.
C. Download the latest Microsoft security XML database to the portable computer.
On the portable computer, create a share that contains the XML database.
Run the Microsoft Baseline Security Analyzer (MBSA) on Certkiller 1.
D. Use the Windows Update Catalog to download the new driver and security update to the portable computer.
On the portable computer, create a share that contains the new driver and update.
Use the share on the portable computer to update Certkiller 1.

Answer: D

Explanation:

The Windows Update Catalog provides a comprehensive catalog of updates that can be distributed over a corporate network. We use the LapTop to download the updates into a share that is accessible from Certkiller 1. We then install the required drivers and security updates on Certkiller 1. Certkiller 1 would then be able to access Internet again.

Reference:

HOW TO: Download Windows Updates and Drivers from the Windows Update Catalog on Windows 2000, Microsoft Knowledge Base Article - Q326426

Incorrect Answers

A: Enabling Internet Connection Sharing on the portable computer would not give Certkiller 1 Internet connectivity as it use a static IP address.

B: Enabling Internet Connection Sharing on Certkiller 1 would not enable it to access Internet.

C: This is not the way the Microsoft's security XML database is used.

Note: The HFNetChkPro tool provides real-time patch fix information direct from Microsoft's security XML database.

QUESTION 121:

You are the network administrator for Certkiller . You are working at one of four company's branch offices. The branch office has a Windows 2000 Server computer configured as file server named Certkiller 1. Certkiller 1 contains a distribution share named Files1. Files1 contains the contents of the Windows 2000 Professional installation CD-ROM.

You start to install 25 new Windows 2000 Professional client computers by using the distribution share on Certkiller 1. You finish installing the first client computer and then learn that a new service pack is available. You install Windows 2000 Professional on a test computer from the distribution share. You install and test the service pack on the test client computer.

You want to install the service pack on the remaining client computers a quickly as possible with the least amount of administrative effort.

What should you do?

A. Run the service pack's update -s:\\ Certkiller 1\Files1command.
Install the client computers from the distribution share on Certkiller 1.

- B. Copy the service pack files to the distribution share on Certkiller 1.
Install the client computers from the distribution share on Certkiller 1.
- C. Configure a separate Windows 2000 Active Directory domain for the branch office.
Create a new Group Policy object (GPO) and link it to the new domain.
Configure the GPO with a software installation package for the new service pack.
- D. Use Setup Manager to create an answer file and a uniqueness database file.
Specify the appropriate service pack executable as a program to run after installation in Setup Manager.
Copy the answer file to the distribution share.
Run the winnt.exe command with the appropriate unattended installation switches.

Answer: A

Explanation:

Slipstreaming the service pack by the -s switch will allow installation of the software with the least effort.

QUESTION 122:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains computers that run Windows 2000 Server, Windows 2000 Professional, or Windows XP Professional. One of the computers running Windows 2000 Server is named Certkiller 1. Certkiller 1 runs Internet Information Services (IIS) 5.0 and hosts Certkiller 's public Web site. Mr Bill is Certkiller 's Web site developer. Mr Bill asks you to configure Certkiller 1 so that he can stop and start the World Wide Web Publishing service. What should you do?

- A. Configure IIS to use Mr Bill's domain user account for anonymous access.
- B. Configure the World Wide Web Publishing service to use Mr Bill's domain user account as the service account.
- C. Create a security template that configures Mr Bill's domain user account as a user account that can stop and start the World Wide Web Publishing service.
Apply the template to Certkiller 1.
- D. Create a custom administrative template that configures Mr Bill's domain user account as a user account that has security permissions to the folder containing Certkiller Web site.
Apply the template to Certkiller 1.

Answer: C

Explanation:

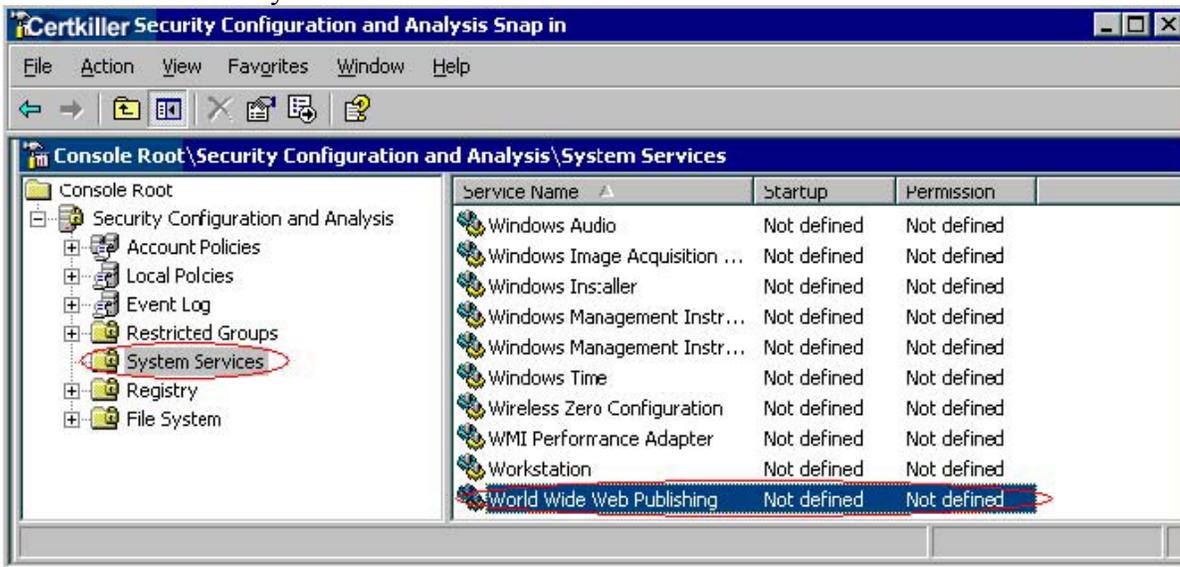
There are three methods to

1. Grant Rights Using Group Policy
2. Grant Rights Using Security Templates (this is C)
3. Grant Rights Using Subinacl.exe

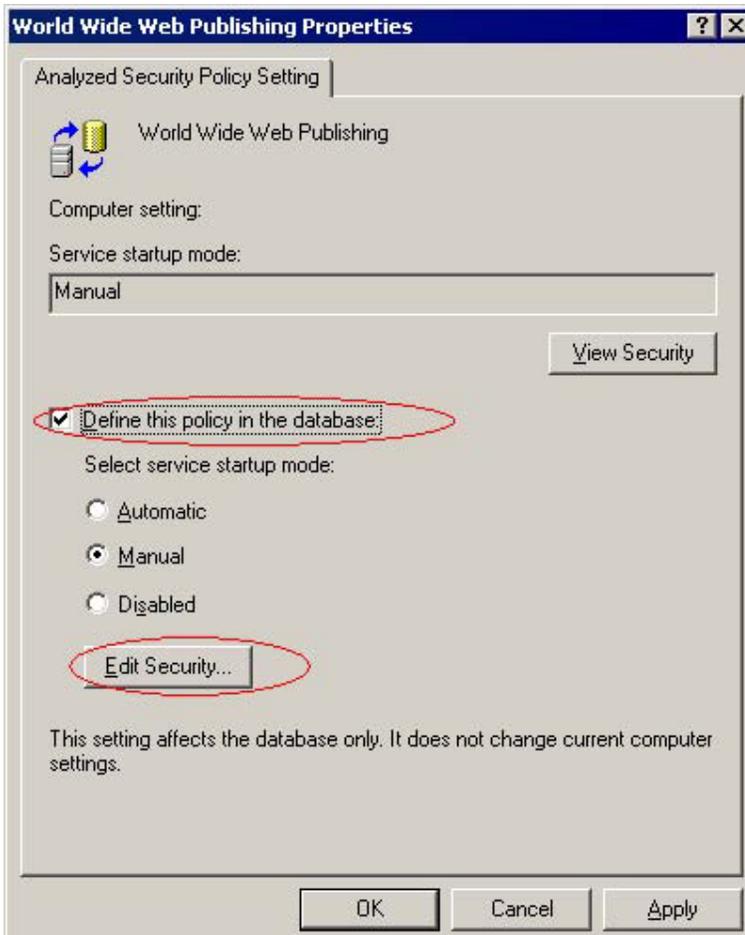
Procedure to Grant Rights Using Security Templates:

This method is very similar to Method 1, but it uses Security templates to change the permissions on system services. To do this, follow these steps:

1. Click Start, click Run, and then type MMC.
2. On the Console menu, click Add/Remove Snap-in.
3. Click Add.
4. Select the Security Configuration and Analysis snap-in, and then click Add.
5. Click Close, and then click OK.
6. In the MMC, right-click the Security Configuration and Analysis item, and then click Open Database.
7. Give a name for the database, and then browse to where you would like to store it.
8. When prompted, select a Security Template to import. For example, the "basicwk.inf" contains values for the standard settings found on a Windows 2000 Professional computer.
9. In the MMC, right-click the Security Configuration and Analysis item, and then click the Analyze Computer now option. Choose a location for the log file, when prompted.
10. After analysis is complete, configure the service permissions as follows:
 - a. Double-click the System Services branch in the MMC.



- b. Right-click the service that you want to change, and then click Security.
- c. Click Edit Security.



d. Add user accounts as required, and configure the permissions for each account. By default, the user will be granted "Start, stop and pause" permissions.

11. To apply the new settings to the local computer, simply right-click the Security Configuration and Analysis item, and then click the Configure Computer Now option.

Reference:

HOW TO: Grant Users Rights to Manage Services in Windows 2000, HOW TO: Grant Users Rights to Manage Services in Windows 2000

Incorrect Answers

A: If anonymous users run in the security of the Mr Bill's domain user account it would be a major security flaw.

B: We should configure the IIS to run in the security context of Mr Bill domain user account.

D: We cannot configure a custom administrative template to allow a domain user account to start the WWW publishing service. Furthermore, the proposed solution is inadequate, security permission to a specify folder will not give permission to start a particular service.

QUESTION 123:

You are the network administrator for Certkiller . The network includes a file server named Certkiller 1. Certkiller 1 contains a shared folder named Win2000Pro. The shared

folder contains the contents of a Windows 2000 Professional CD-ROM slipstreamed with the latest service pack.

You download five post-service pack Windows 2000 security updates from the Microsoft Web site. You want to include the updates in all future installations and upgraded of Windows 2000 Professional. You want to accomplish this task by using the fewest number of additional steps during Windows 2000 Professional Setup.

What should you do?

A. Expand each security update.

Copy the files for each security update to the \\ Certkiller 1\Win2000Pro\i386 folder.

B. Add a Commands.inf file to the \\ Certkiller 1\Win2000Pro\i386 folder, then add the executable name for each security update to the file.

C. Integrate the security updates into the \\ Certkiller 1\Win2000Pro source files by creating a Svcpack.inf file that references the catalog files provides with the security updates.

Modify Dosnet.inf to refer to the folder containing the catalog files.

D. Copy each security update to a subfolder named

\\ Certkiller 1\Win2000Pro\i386\SvcPack.

Open the default Dosnet.inf file, remove the uniproc entry, and add a svcpack entry.

Answer: C

Explanation:

Procedure installing Windows2000 integrated with SP3 and Windows2000 hotfixes

1. Connect to the network or computer on which you want to create the distribution folder.
2. Create an \i386 distribution, for example: E:\i386
3. Copy the files and subfolders from the Windows2000 integrated SP3 installation CD to the E:\i386 folder.
4. Edit E:\i386\dosnet.inf to add svcpack to the [OptionalSrcDirs] section.
5. Create an E:\i386\svcpack folder.
6. Copy the hotfix executable program to the E:\i386\svcpack folder.
7. Expand the hotfix to a unique temporary location.
8. Copy the catalog files (.cat) and hotfix binary files (such as .exe, .dll, .sys) as follows:
9. Delete the E:\i386\svcpack.in_ file.
10. Create a new svcpack.inf file at E:\i386\svcpack.inf which, among other things, must include a reference to the folder containing the security update files.
11. If you will be installing multiple hotfixes, copy Qchain.exe to the E:\i386\svcpack folder.

Incorrect Answers

A: Hotfixes cannot be slipstreamed into the distribution folder.

B: This would be awkward.

D: This is an incorrect procedure.

QUESTION 124:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. All client computers are in an organizational unit (OU) named Clients.

The network includes three Windows 2000 Server computers configured as domain controllers and one Windows 2000 Server computer, named Certkiller 1, configured as a file server. Certkiller 1 has a distribution share folder that holds the contents of the Windows 2000 Professional installation CD-ROM and the latest service pack slipstreamed into the installation files. The network contains 1,500 Windows 95 client computers.

Bruno, the desktop administrator, manages the client computers in your network. Bruno has full administrative rights to all client computers.

You upgrade the Windows 95 client computers from the distribution share on Certkiller 1. Three of the upgraded Windows 2000 Professional client computers (CK1 , CK2 , and CK3) must run software that is incompatible with the service pack. You need to ensure that the service pack is removed from CK1 , CK2 , and CK3 . What should you do?

- A. Instruct Bruno to use the Windows 2000 Professional CD-ROM distribution media to reinstall the operating system of CK1 , CK2 , and CK3 .
Reinstall the required applications and security updates.
- B. Instruct Bruno to reinstall the operating system of CK1 , CK2 , and CK3 by using the distribution share on Certkiller 1.
Reinstall the required applications and security updates.
- C. Instruct Bruno to boot CK1 , CK2 , and CK3 from the Windows 2000 Professional CD-ROM and use the Repair Installation option.
- D. Instruct Bruno to boot CK1 , CK2 , and CK3 from the Windows 2000 Professional CD-ROM and use the Recovery Console.

Answer: A

Explanation:

You cannot uninstall a Service Pack that you install in slipstream mode. We must therefore reinstall Windows 2000. We should reinstall Windows 2000 from a Windows 2000 CD that does not contain any Service Pack.

Incorrect Answers

B: The distribution share has already been slipstreamed with the latest service pack.
C, D : We cannot fix this problem by the Repair Installation option or the Recovery Console because the Service Pack is generating this error.

[QUESTION 125:](#)

You are the administrator of a Windows 2000 Server computer named Certkiller 1. Users on the network use Windows 2000 Professional client computers to connect to the server. The client computers and Certkiller 1 are members of the same Windows 2000 domain. All network traffic to and from Certkiller 1 is protected by IPsec. The client computers are configured with the Client (Respond Only) IPSec policy. Certkiller 1 is

configured with the Secure Server (Require Security) IPSec policy.
You want to increase security on all IPSec connections to Certkiller 1.
What should you do?

- A. Configure Certkiller 1 with an IPSec policy that uses Perfect Forward Secrecy.
- B. Configure Certkiller 1 with the Server (Request Security) IPSec policy.
- C. Configure the client computers with the Secure Server (Require Security) IPSec policy.
- D. Configure the client computers and Certkiller 1 with an IPSec policy that uses a certificate for authentication.

Answer: C

Explanation:

By changing the policy on the clients to the Secure Server (Require Security) IPSec policy the communication between Windows 2000 Professional computers would be secure as well.

Incorrect Answers

A: The Perfect Forward Secrecy policy ensures that a new key pair is generated for every message you send. However, it would not secure the communication between Windows 2000 Professional computers.

B: The Server (Request Security) IPSec policy is less secure than the current Secure Server (Require Security) IPSec policy.

D: It would be better to secure all communication with the Secure Server (Require Security) IPSec policy.

QUESTION 126:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain Certkiller .com. The domain contains 5,000 Windows XP Professional computers. All computers use Microsoft Internet Explorer as their only Web browser.

The written security policy for Certkiller prohibits users from executing Microsoft ActiveX controls that are contained in Web pages. Users are allowed to run only ActiveX controls that are listed as approved in the written policy. All company computers have been configured with security settings that comply with the written policy by means of a Group Policy object (GPO) named CKSecurity. The CKSecurity GPO is linked to the domain.

Users report that they cannot access a Web page that is hosted on a company Web server. You discover that the pag is attempting to load an ActiveX control. The control was recently created by Certkiller 's Web developers and added to the list of approved ActiveX controls in the written policy.

You need to ensure that all users can access the Web page containing the new ActiveX control.

What should you do?

A. On your computer, modify the Internet Explorer security settings for the Internet zone so that ActiveX controls are permitted to run.

Import the security zone settings to the CKSecurity GPO.

B. On your computer, set the Internet Explorer security settings for the Web server security zone to Trusted.

Import the security zone settings to the CKSecurity GPO.

C. In the computer configuration section of the IESecurity GPO, modify the Internet Explorer security settings for the Internet zone so that the Security Zones: Use only machine settings policy is enabled.

D. In the user configuration section of the CKSecurity GPO, add the new ActiveX control to the Administrator Approved Controls policy.

Enable the policy and select the control.

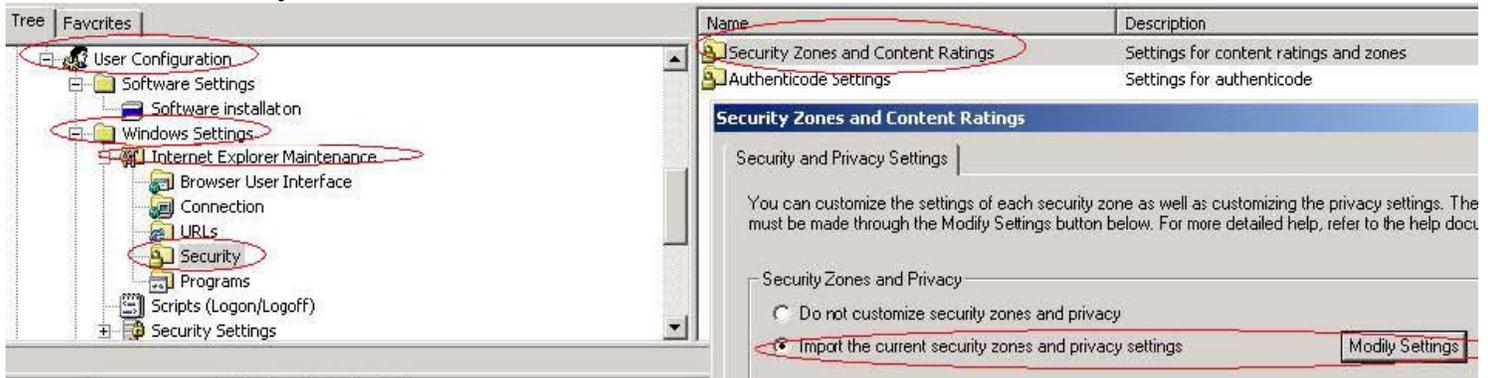
Answer: B

Explanation:

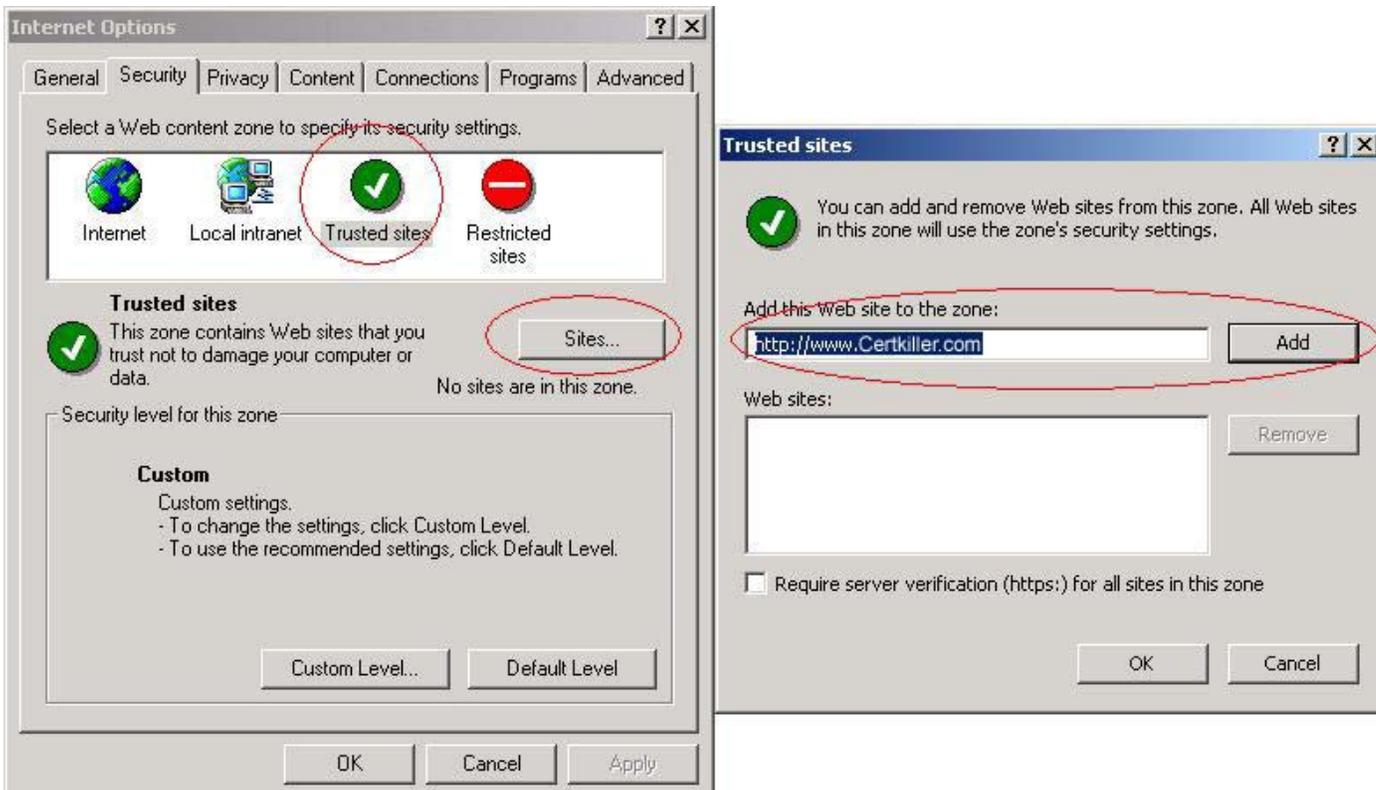
ActiveX controls extend the functionality of Internet Explorer, but they can also pose significant security risks. An ActiveX control could potentially access sensitive data, delete files, or cause other damage.

You can use Windows 2000 group policy to restrict ActiveX controls on a user's computer to a specific set of administrator-approved controls. By doing so, you let users continue using certain controls while restricting all others.

You can configure ActiveX group policy either at the local computer or at a higher level, such as an organizational unit or domain. To configure approved controls, open the MMC, and goto User Configuration\Windows Settings\Internet Explorer Maintenance\Security.



Select Security Zones and Content Ratings and click Import the current security zones and privacy settings and click modify.



Select the trusted web content zone and click sites.

Then add the webdevelopers website to the trusted web sites list.

Repeat the process for other controls as needed to allow or deny them based on your user and security requirements.

Incorrect Answers

A: We cannot allow all ActiveX controls from the Internet zone to run. Only ActiveX controls that are listed as approved in the written policy should be allowed to run.

C: The Security Zones: Use only machine settings policy applies security zone information to all users of the same computer. This policy is not useful in this scenario.

D: It is not possible to ADD custom activeX settings to the Administrator Approved Controls policy.

QUESTION 127:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain.

You must maintain a text-based accounting package migrated from a UNIX server.

Access to the accounting software is provided by using a telnet client at all accounting department Windows 2000 Professional client computers. A Windows 2000 Server computer named Certkiller 1 runs the accounting software. Certkiller 1 also has the Telnet service enabled to allow telnet connections.

The accounting manager is concerned that employees who are not members of the accounting department might intercept the data entered into the accounting software.

You create a custom IPsec policy and assign it in the Local Security Policy for Certkiller 1. You configure the custom IPsec policy to implement Encapsulating Security

Payload (ESP). You also create an organizational unit (OU) named Accounting in the domain. Then, you create a Group Policy object (GPO) and link it to the Accounting OU. You configure the GPO to assign the Client (Respond Only) default IPsec policy. You need to ensure that the telnet session traffic is encrypted. What should you do?

- A. Configure ESP in the custom IPsec policy for connections to Certkiller 1 on TCP port 23 from any IP address and any port.
Move all accounting department computer accounts into the Accounting OU.
- B. Configure ESP in the custom IPsec policy for connections from TCP port 23 from any IP address to any port on Certkiller 1.
Move all accounting department computer accounts into the Accounting OU.
- C. Configure ESP in the custom IPsec policy for connections to Certkiller 1 on TCP port 23 from any IP address and any port.
Move all accounting department user accounts into the Accounting OU.
- D. Configure ESP in the custom IPsec policy for connections from TCP port 23 from any IP address to any port on Certkiller 1.
Move all accounting department use accounts into the Accounting OU.

Answer: A

Explanation:

To protect the telnet application with ipsec, we must configure an IPsec policy TO Certkiller 1 on TCP port 23 from any ipaddress and any port. Further we must assure that the Client (Respond Only) default IPsec policy is applied to the Accounting OU computers.

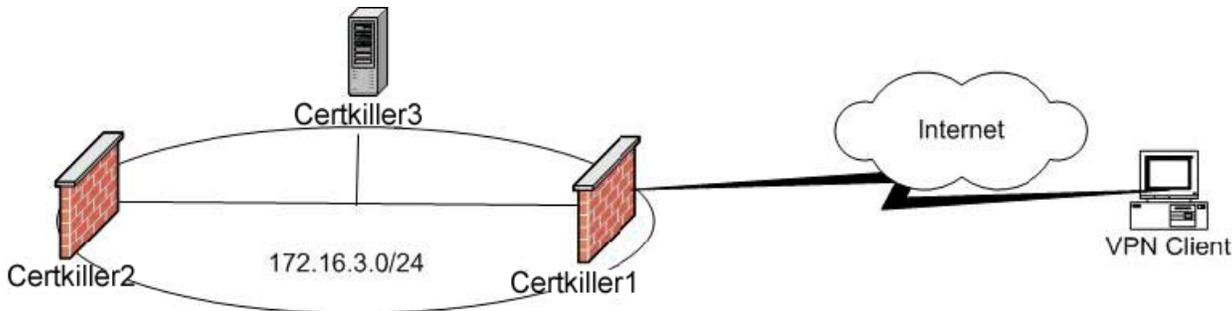
Reference :

Moc - Windows 2000 Network Security Design (70-220) (Course 2150a) Student Guide
Incorrect Answers

- B: Will must secure Telnet traffic port 23 on Certkiller 1. Not all ports.
- C: We must apply the the Client (Respond Only) policy to computers. Not users.
- D: We must apply the the Client (Respond Only) policy to computers. Not users.

QUESTION 128:

You are the network administrator for Certkiller . The network includes a perimeter network (also known as DMZ) that hosts all Internet-accessible services. The DMZ includes a Windows 2000 Server computer named Certkiller 3. Certkiller 3 runs Routing and Remote Access and is Certkiller 's virtual private network (VPN) server. The DMZ is protected by two third-party firewalls: Certkiller 1 and Certkiller 2. Certkiller 1 currently performs Network Address Translation (NAT) on all traffic entering and exiting the DMZ. The DMZ infrastructure components are shown in the exhibit.



Currently, VPN client computers can connect to Certkiller 3 by using PPTP connections. All VPN client computers are upgraded to Windows 2000 Professional from Windows 95, Windows 98, and Windows NT Workstation 4.0. Your manager revises the written security policy for Certkiller to restrict all VPN connections to use L2TP over IPsec (L2TP/IPsec) connections.

You configure Certkiller 3 to allow L2TP/IPsec VPN connections, but in test using the current DMZ infrastructure, all L2TP/IPsec connections fail. You must modify Certkiller 1 to allow L2TP/IPsec VPN connections.

What should you do?

- A. Implement packet filters that allow all connections that use L2TP to each Certkiller 3. Leave the network-addressing scheme in the DMZ unchanged.
- B. Implement packet filters that allow all connections that use Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) to reach Certkiller 3. Leave the network-addressing scheme in the DMZ unchanged.
- C. Implement packet filters that allow all connections that use L2TP to reach Certkiller 3. Change the network-addressing scheme in the DMZ to use a public Internet address.
- D. Implement packet filters that allow all connections that use Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) to reach Certkiller 3. Change the network-addressing scheme in the DMZ to use a public Internet address.

Answer: D

Explanation:

NAT destroys the IP header used by L2TP/IPsec. We must therefore use a public Internet address on Certkiller 3. Firewalls generally reject IPsec packets by default. You'll need to configure your router or proxyserver for some specialized filtering to ensure that packets secured with IPsec are not rejected. Here are some recommended filters for your router:

- * Allow protocol ID 51 for inbound and outbound IPsec AH traffic.
- * Allow protocol ID 50 for inbound and outbound ESP traffic.
- * Allow UDP port 500 for inbound and outbound IKE traffic.

Without these ports and protocol IDs allowed, your firewall will not pass IPsec traffic.

Note: L2TP with IPsec requires the following protocols: Encapsulating Security Payload (ESP), Internet Key Exchange (IKE), and L2TP.

Assuming there is a firewall protecting the intranet from the Internet, the placement of the L2TP server directly affects what IP filters are required on the firewall. If the L2TP server is outside of the firewall, the firewall will have to filter IKE and L2TP. If the

L2TP is within the intranet, the firewall will have to filter IKE and ESP. The filtering configuration is required because the L2TP packets are encapsulated with the ESP packets.

Incorrect Answers

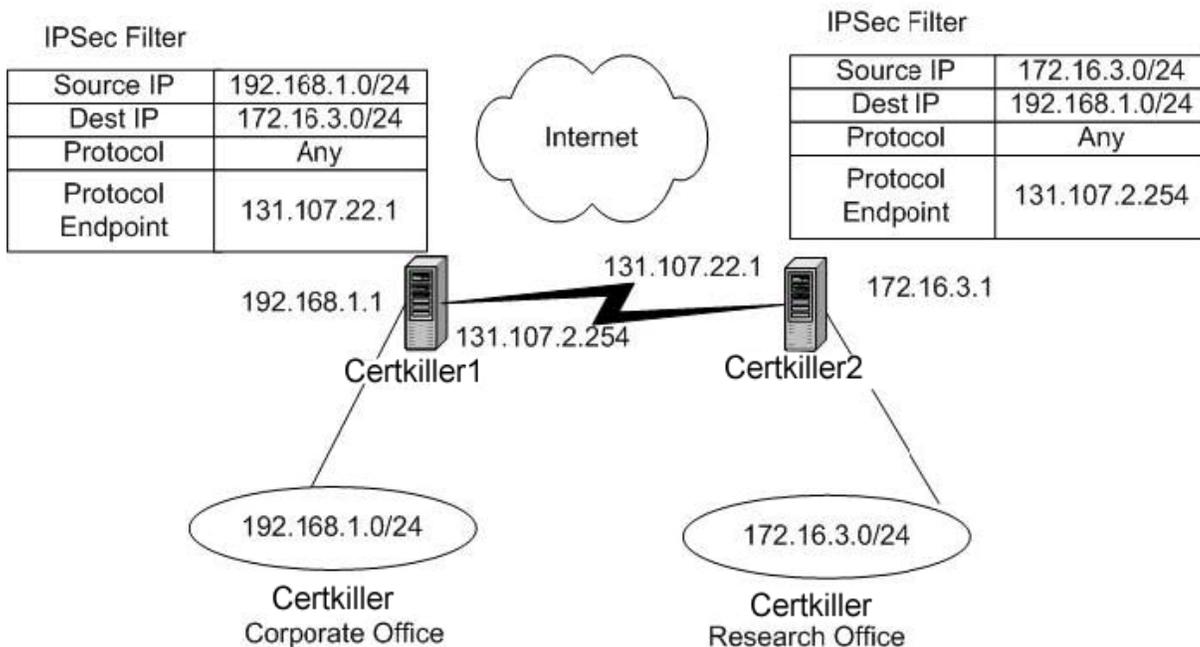
A, B: NAT destroys the IP header used by L2TP/IPSec. We must therefore use a public Internet address on Certkiller 3 so that we don't use NAT anymore.

C: We must allow connections that use ESP and IKE. We do not have to allow connections that L2TP connections as they are encapsulated within the ESP packets.

QUESTION 129:

You are a network administrator for Certkiller .

The relevant portion of the network configuration and configured IPsec filters are shown in the exhibit.



Written security policies for Certkiller require that all traffic passing between the main office and the research office pass through an IPsec tunnel. Routing and Remote Access is enabled on both Certkiller 1 and Certkiller 2. Static routes are defined in Routing and Remote Access for Windows 2000, allowing data to be transmitted between the offices.

Certkiller 1 is configured to route all traffic from the main office network to the research office network by using 131.107.22.1 as the gateway address. Certkiller 2 is configured to route all traffic from the research office network to the main office network by using 131.107.2.254 as the gateway address. However, data does not pass successfully between the main and research offices.

You must ensure that data can pass securely over the Internet when data is transferred between the main and research offices.

What should you do?

A. Change the static routes that are defined through Routing and Remote Access.

The gateway address applied at Certkiller 1 should be 192.168.1.1.

The gateway address applied at Certkiller 2 should be 171.16.3.1.

B. Change the tunnel endpoints in the IPSec filters.

The tunnel endpoint for the IPSec filter applied at Certkiller 1 should be 172.16.3.1.

The tunnel endpoint for the IPSec filter applied at Certkiller 2 should be 192.168.1.1.

C. Change the IP addresses issued on the main office network from 192.168.1.0/24 to 131.107.1.0/24 and the IP addresses issued on the research office network from 172.16.3.0/24 to 131.107.3.0/24.

Then, change the IPSec filters and routing tables at Certkiller 1 and Certkiller 2 to reflect the new IP addresses.

D. Define an additional IPSec filter at both Certkiller 1 and Certkiller 2.

At Certkiller 1, define that traffic from the 172.16.3.0/24 network to 192.168.1.0/24 network uses tunnel endpoint 131.107.2.254.

At Certkiller 2, define that traffic from the 192.168.1.0/24 network to the 172.16.3.0/24 network uses tunnel endpoint 131.107.22.1.

Answer: D

Explanation:

To properly construct a tunnel, you actually need two rules on each end: one for inbound traffic, and one for outbound traffic. Microsoft warns against using mirroring on tunnel rules; instead, if you want to link two networks (Main Office and Research Office), you'd need to specify a rule that has two filter lists. The Main Office filter lists specify a filter for outgoing traffic that has the Research Office router as a tunnel endpoint, then another filter for incoming traffic from any IP subnet that points back to the Main Office tunnel endpoint. In conjunction with these filter lists, of course, you'd specify a filter action that provided whatever type of security was appropriate for the connection.

Reference:

Sybex - Windows 2000 Network Infrastructure Administration (70-216) Study Guide
Incorrect Answers

A: We should not use the IP address of Certkiller 1 as the default gateway on Certkiller 1 itself. The same goes for the Certkiller 2.

B: No the end point must be applied to the external network adapters. NOT the internal adapters.

C: There is no need to change the IP addresses at the Corporate Office or the Research Office. the tunnel will still not work

QUESTION 130:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. All client computers run Windows 2000 Professional. All servers run Windows 2000 Server. All company and user data is stored on servers. Administrators perform remote administration by using Terminal Services connections to the servers. Remote administration is performed from the internal network during business hours and from remote locations after business hours. Users do not use Terminal Services connections.

Users in the accounting department report that several confidential files have been modified or deleted by an unknown user during the night. You discover that the files were modified or deleted by the user account of a former employee in the accounting department. You suspect that the former employee gained access to the data folder by means of a Web-based Terminal Services connection from outside the network. You disable the user account. You need to ensure that only authorized administrators can connect to Terminal Services outside the network. What should you do? (Each correct answer presents part of the solution. Choose two)

- A. On the firewall server, disable inbound HTTP connections.
- B. On the firewall server, disable inbound Terminal Services connections.
- C. On all servers, disable Internet Information Services (IIS).
- D. On all servers, configure Terminal Services to use a nonstandard port. Enable this port for inbound access on the firewall server.
- E. Configure a Routing and Remote Access server as a virtual private network (VPN) server. Grant only administrators remote access permission and configure the firewall server to allow inbound VPN connections.

Answer: B, E

Explanation:

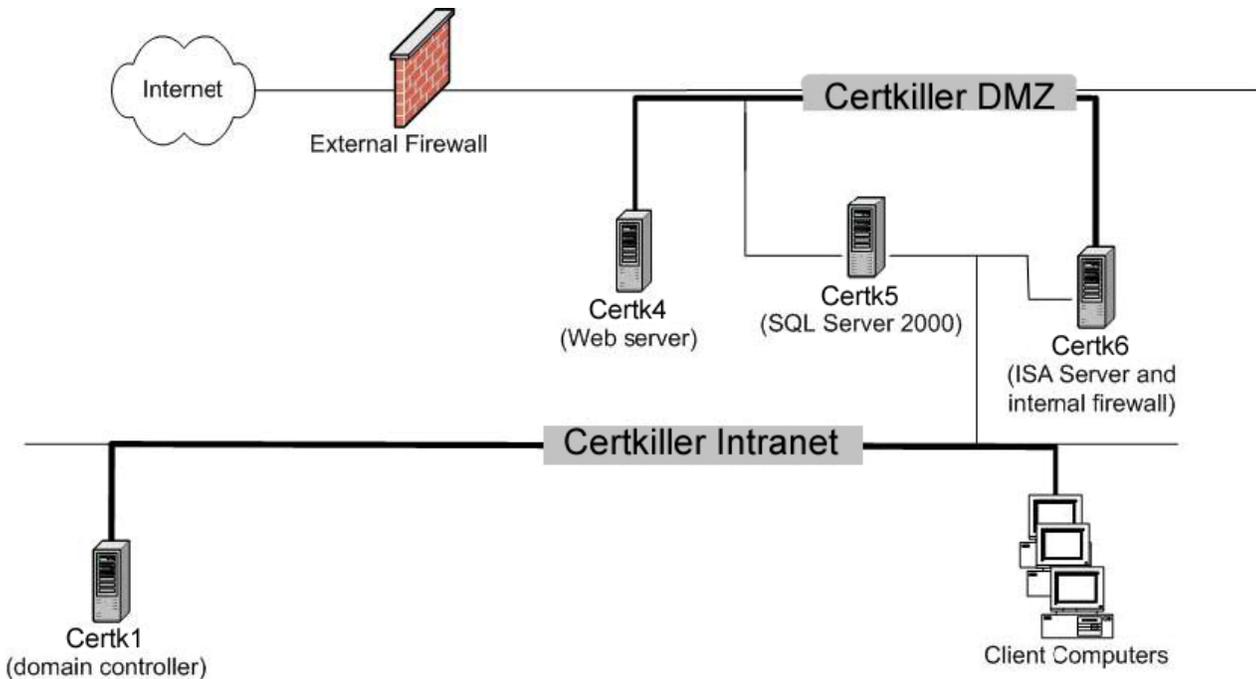
- B: We should disable inbound Terminal Services connections.
- E: We set up VPN and only administrators inbound VPN connections.

Incorrect Answers

- A: Inbound HTTP connections should still be allowed.
- C: It is not necessary to disable IIS. IIS is not relevant to the problem at hand.
- D: Use of a non-standard port improves security, however terminal sessions would still be possible.

QUESTION 131:

You are the network administrator Certkiller Inc. The network consists of a Windows 2000 Active Directory domain Certkiller .com. All servers run Windows 2000 Server. All client computers run Windows 2000 Professional. The relevant portion of the network is shown in the exhibit.



Certkiller 6 runs Microsoft Internet Security and Acceleration (ISA) Server. CertK 5 is a multihomed Microsoft SQL Server 2000 computer that has a connection to Certkiller intranet and the perimeter network (also known as the DMZ). CertK 5 hosts an order-processing database. External users access this database by means of a Web application that runs on CertK 4.

The written security policy for Certkiller does not allow external users to directly access CertK 5. However, the SQL Server logs on CertK 5 reveal that external users are logging in to SQL Server and accessing data.

CertK 5 also hosts four other databases, which only internal users are allowed to access. CertK 5 is administered from client computers that are located on Certkiller intranet and are running SQL Enterprise Manager.

You need to configure CertK 5 to comply with the written policy, while maintaining its connectivity to CertK 4 and internal client computers.

What should you do?

- A. Remove the second network adapter in CertK 5.
Move CertK 5 to the DMZ.
Create a rule on CertK 6 that allows internal client computers to communicate with CertK 5.
- B. Remove the second network adapter in CertK 5.
Move CertK 5 to Certkiller intranet.
Create a rule on CertK 6 that allows CertK 4 to communicate with CertK 5.
- C. Change the server role for CertK 5 to a stand-alone server.
Configure CertK 5 to use Windows Integrated authentication.
Create a rule on Certkiller 6 that allows internal client computers to communicate with CertK 5.
- D. Change the server role for CertK 5 to a stand-alone server.
Configure the MSSQLServer service account to use the local system account.

Configure Certkiller 4 to use SSL when accessing CertK 5.

Answer: B

Explanation:

By putting CertK 5 on the intranet we make it inaccessible for external users. There is no use for two network adapters, so we should remove one of them. We must also configure the firewall so that it allows communication between the Web Server and CertK 5.

Incorrect Answers

A: We should not put CertK 5 in the DMZ. Resources in the DMZ can be accessed by external users.

C, D: We cannot allow CertK 5 to be directly connected to the DMZ, as external users can directly access resources in the DMZ. We must remove the second network adapter and move CertK 5 into the DMZ.

QUESTION 132:

You are the network administrator for Certkiller . The network consists of two Windows 2000 Active Directory domains: Certkiller .com and research. Certkiller .com. Certkiller 's research department uses the research. Certkiller .com domain, which contains 25 user accounts. Other company departments use the Certkiller .com domain, which contains 150 user accounts.

Each department has a wireless LAN that provides network connectivity for users from that department. All wireless LAN in Certkiller use Wired Equivalent Privacy (WEP). All wireless access points serve as bridges to wired LANs. The wired LANs contain departmental file servers. All users have portable computers that run Windows XP Professional. Users often roam one wireless LAN to another.

Research department data must be kept as secure as possible when it is transmitted on the wireless LAN. The written security policy for Certkiller states that only users in the research department should be able to connect to the research department's wireless LAN or view the wireless LAN in the list of available wireless networks.

You need to configure the wireless LAN in the research department to comply with the written policy. You also need to ensure that the portable computers in other departments can continue to operate without configuration changes.

What should you do?

- A. Configure the wireless LAN in each department to use a unique SSID.
Disable SSID Broadcast for the wireless access point of each department.
Enable MAC Filtering for the wireless access point of the research department.
- B. Configure the wireless LAN in each department to use public as its SSID.
Enable SSID Broadcast for the wireless access point of each department.
Disable MAC Filtering for the wireless access point of the research department.
- C. Configure the wireless LAN in the research department to use a unique SSID.
Disable SSID Broadcast for the wireless access point of the research department.
Enable MAC Filtering for the wireless access point of the research department.
- D. Configure the wireless LAN in the research department to use a unique SSID.

Enable SSID Broadcast for the wireless access point of the research department.
Disable MAC Filtering for the wireless access point of the research department.

Answer: C

Explanation:

Only the Research department needs a unique SSID.

As SSID broadcasts are sent in the clear we should disable it. When the SSID broadcasts are disabled, a wireless client computer cannot connect to the AP (Access point) with an "any" SSID; the correct SSID has to be specified on client computer.

We should enable MAC Filtering. MAC filtering lets you control which computers on your network can connect to your base station.

Note: SSID (Service Set Identifier), a 32-character unique identifier attached to the header of packets sent over a WLAN (wireless local-area network) that acts as a password when a mobile device tries to connect to the BSS (Basic Service Set). The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network.

An SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.

When one AP (Access Point) is connected to wired network and a set of wireless stations it is referred to as a Basic Service Set (BSS).

Incorrect Answers

A: Only the Research department needs a unique SSID.

B, D: We should disable SSID broadcasts

QUESTION 133:

You are the network administrator for Certkiller . The network consist of a Windows 2000 Active Directory domain. All client computers run Windows XP Professional.

You are deploying an 802.11b wireless LAN in the network. The wireless LAN will use Wired Equivalent Privacy (WEP) for all connections.

The written security policy for Certkiller states that company computers must be able to connect automatically to the wireless LAN. Unauthorized computers must not be able to connect to or view the wireless LAN in the list of available wireless networks.

You need to configure all wireless access points and client computers to comply with the written policy.

What should you do?

A. Set the authentication type for the wireless LAN to Shared Key.

Enable SSID Broadcast and MAC Filtering on all wireless access points.

On each client computer, add the SSID for the wireless LAN as an available network.

B. Set the authentication type for the wireless LAN to Shared Key.

Disable SSID Broadcast and enable MAC Filtering on all wireless access points.

On each client computer, add the SSID for the wireless LAN as a preferred network.

C. Set the authentication type for the wireless LAN to Open System.

Enable SSID Broadcast and disable MAC Filtering on all wireless access points.

On each client computer, add the SSID for the wireless LAN as an available network.

D. Set the authentication type for the wireless LAN to Open System.

Disable SSID Broadcast and MAC Filtering on all wireless access points.

On each client computer, add the SSID for the wireless LAN as a preferred network.

Answer: B

Explanation:

Share Key authentication provides access control. As SSID broadcasts are sent in the clear we should disable it. When the SSID broadcasts are disabled, a wireless client computer cannot connect to the AP (Access point) with an "any" SSID; the correct SSID has to be specified on client computer.

We should enable MAC Filtering. MAC filtering lets you control which computers on your network can connect to your base station.

Note: Wireless LANs have the following types of security: SSID, MAC address filtering, and WEP.

WEP (Wired Equivalent Privacy) has three levels of security:

1. Open system - WEP is disabled in this mode. There is no security.

2. Shared Key Authentication. Provides access control.

3. Encryption provides confidentiality to data on the network.

Incorrect Answers

A: If we enable SSID broadcasts any SSID can be used to connect to the Access Point.

C, D: Open system would disable WEP and there would be no security.

QUESTION 134:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains three Windows 2000 Server computers named Certkiller 1, Certkiller 2, and Certkiller 3 that are configured as domain controllers.

The Active Directory schema is modified to include several human resource department-related attributes. The permissions on the attributes are configured so that only members of the human resources department can read the attributes in Active Directory.

A custom LDAP application is used by the human resources department to modify human resources attributes of user objects. The written security policy of Certkiller requires that all human resources department-related data be protected against network inspection.

You must ensure that the written policy is enforced without preventing other clients from connecting to the domain controllers for authentication purposes.

What should you do?

A. Install computer certificates at all human resources computers and configure the

application to implement SSL when connecting to the domain controllers.

B. In the Default Domain Controllers policy, assign the Secure Server (Require Security) IPsec policy.

In the Local Security Policy of the human resources computers, assign the Client (Respond Only) IPsec policy.

C. Install domain controller certificates at all domain controllers and configure the application to implement SSL when connecting to the domain controllers.

D. In the Default Domain Controllers Policy, enable the Digitally Sign Server Communications (always) security option.

In the Default Domain Policy, enable the Digitally Sign Client Communications (always) security option.

Answer: D

Explanation:

SMB signing places a digital security signature into each SMB message, which is then verified by both the client and the server to deter impersonation and man-in-the-middle attacks. SMB signing must be enabled on both the client and the server before it can be used. It is not turned on by default in Windows 2000 Server. SMB signing requires that both parties trust the same CA.

A. If the client and the server do not trust the same CA, SMB signing won't work. To use SMB signing, you must either enable it or require it on both the client and the server. If SMB signing is enabled on a server, clients that are enabled for SMB signing will use SMB signing when connecting to the server. If SMB signing is required on a server, a client will not be able to establish a session unless it is at least enabled for SMB signing. SMB signing is enabled in a Group Policy in the Security Options node under the Local Policies node.

We should assign the Secure Server (Require Security) IPsec policy to secure the domain controllers to meet the requirement above.

Incorrect Answers:

A,C: We must protect ALL human resources related data. Not only the application.

B: If we use the Secure Server (Require Security) IPsec policy on the domain controllers and the Client (Respond Only) IPsec policy on the Human Resources pc only, then other clients will not be able to connect to the domain controllers anymore.

QUESTION 135:

You are the network administrator for Certkiller. The network consists of Windows 2000 Server computers and Windows 2000 Professional client computers in a Windows 2000 Active Directory domain.

You want to ensure that file-sharing network traffic between the client computers and the servers uses mutual authentication. Company policy does not allow the use of IPsec on Certkiller network.

What should you do?

A. Create a Group Policy object (GPO) that applies to all client computers.

In the GPO, enable the Secure channel: Digitally sign secure channel data (when possible) setting.

B. Create a Group Policy object (GPO) that applies to all client computers.

In the GPO, enable the Digitally sign client communication (when possible) setting.

C. Create a Group Policy object (GPO) that applies to all servers.

In the GPO, enable the Digitally sign server communication (always) setting.

D. Create a Group Policy object (GPO) that applies to all servers.

In the GPO, configure the LAN Manager Authentication Level to use NTLMv2 only.

Answer: D

Explanation:

NTLM version 2 is the most secure.

Note: The LAN Manager authentication level determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers. The NTLM authentication package in Windows 2000 supports three methods of challenge/response authentication: LAN Manager (LM) which is least secure, NTLM version 1, NTLM version 2 which is the most secure.

By default, all three challenge/response mechanisms are enabled. You can disable authentication using weaker variants by setting the LAN Manager authentication level security option in local security policy for the computer.

Reference:

How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT, Microsoft Knowledge Base Article - Q239869

Incorrect Answers:

A: We do not need to enable the Secure channel

B: We do not need to enable the Digitally sign client

C: We do not need to enable the Digitally sign server

QUESTION 136:

You are the network administrator for Certkiller . The network consists of 12 Windows 2000 member servers, 40 Windows 2000 Professional client computers, and 60 Windows NT Workstation 4.0 computers. All the computers are part of a Windows 2000 Active Directory domain and have the latest service packs installed.

You want to ensure that file-sharing network packets between the client computers and the servers will be rejected when an attacker on the network alters those packets.

What should you do?

A. Enable Server Message Block (SMB) signing on all computers in the domain.

B. Restrict access over anonymous connections on all computers in the domain.

C. Configure the LAN Manager Authentication Level on all computers in the domain to use NTLMv2 only.

D. Configure all computers in the domain to use IPsec Authentication Header (AH) for

file share network communication.

Answer: A

Explanation:

SMB Signing puts a digital signature on SMB messages on the network. This can prevent man-in-the-middle attacks and message DOS attacks. If you use this feature, performance will be affected (10-15% loss) and only Windows 98/NT/2000 clients will be able to connect to the Server.

Incorrect Answers

B: Restricting anonymous access would increase security, but packets could still be tampered with.

C: NTLMv2 only affects authentication. Packets could still be tampered with.

D: IPSec Authentication Header (AH) only secures authentication, not data transfers.

QUESTION 137:

You are the administrator of a Windows 2000 Network. The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers. The client computers often connect to a Windows 2000 stand-alone server named Certkiller 1. The client computer can connect to Certkiller 1 only through a Network Address Translation (NAT) device. You want to ensure that Certkiller 1 will reject file sharing network packets when they are altered during transmission. What should you do?

- A. Configure the local Group Policy on Certkiller 1 to enable the Secure channel: Digitally encrypt or sign secure channel data (always) setting.
- B. Configure the local Group Policy on Certkiller 1 to enable the Digitally sign server communication (always) setting.
- C. On the client computers and on Certkiller 1, implement an IPSec policy that uses IPSec Authentication Header (AH).
- D. On the client computers and on Certkiller 1, implement an IPSec policy that uses a preshared key as the authentication method.

Answer: B

Explanation:

Digitally sign server communications (always) - The Windows 2000 Server Message Block (SMB) authentication protocol supports mutual authentication, which closes a "man-in-the-middle" attack, and supports message authentication, which prevents active message attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. In order to use SMB signing, you must either enable it or require it on both the SMB client and the SMB server. If SMB signing is enabled on a server, then clients that are also enabled for SMB signing will use the packet signing protocol during all subsequent sessions. If SMB

signing is required on a server, then a client will not be able to establish a session unless it is at least enabled for SMB signing.

Encryption of secure channels Member workstations and servers communicate with their domain controllers and domain controllers communicate with other domain controllers using secure channels. In addition to authentication, you can encrypt and check the integrity of these communications.

Note: SMB Signing puts a digital signature on SMB messages on the network. This can prevent man-in-the-middle attacks and message DOS attacks. If you use this feature, performance will be affected (10-15% loss) and only Windows 98/NT/2000 clients will be able to connect to the Server.

Reference:

Microsoft Windows 2000 Resource Kit Help

Incorrect Answers

A: Secure channel: Digitally encrypt or sign secure channel data (always)

- When a Windows 2000 system joins a domain, a computer account is created.

Thereafter, when the system boots, it uses the password for that account to create a secure channel with the domain controller for its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked and not all information is encrypted. This is the next best solution.

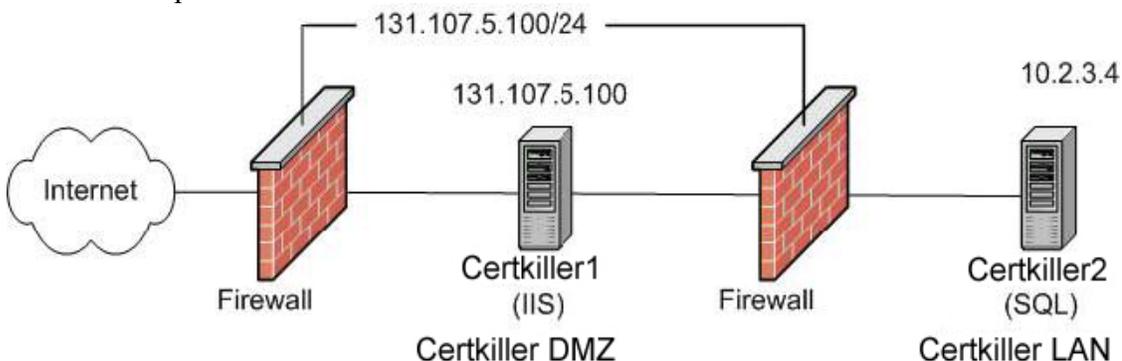
C: Authentication Header (AH) is used for authentication not for transfer of data.

D: We are required to secure transfer of data, not to define secure authentication.

QUESTION 138:

You are the network administrator for Certkiller . The Certkiller network is protected by a perimeter network (also known as DMZ). The DMZ contains two third-party firewall servers and a Windows 2000 Server computer named Certkiller 1. Certkiller 1 runs Internet Information Services (IIS) and hosts an application. The application writes data to a Windows 2000 Server computer named Certkiller 2. Certkiller 2 runs Microsoft SQL Server 2000.

The relevant portions of the network are shown in the exhibit.



All data that is gathered by means of the application must be encrypted as it is transmitted from Certkiller 1 to Certkiller 2. Certkiller 2 hosts databases that do not require encryption for SQL sessions.

You must secure the data transmitted from Certkiller 1 to Certkiller 2, but you are not allowed to modify the current network infrastructure.

What should you do?

- A. On Certkiller 1, install a Web server certificate.
Configure IIS to require SSL encryption for all connections to the application.
- B. On Certkiller 1, install a Web server certificate.
Configure IIS to require SSL encryption for the Default Web site.
- C. On Certkiller 2, install a Web server certificate.
On Certkiller 2, enforce SQL protocol encryption.
- D. On Certkiller 2, install a Web server certificate.
On Certkiller 1, enforce SQL protocol encryption.

Answer: A

Explanation:

We must install a Web server certificate on the web server, Certkiller 1. We should also configure SSL for all connections to the application.

Note: SQL Server can use the Secure Sockets Layer (SSL) to encrypt all data transmitted between an application computer and an instance of SQL Server.

Reference: SQL Server 2000 Books Online, Using Encryption Methods

Incorrect Answers

B: We must ensure encryption of the application, not of the default web site.

C, D: The Web server certificate should be installed on the Web Server not on the SQL Server.

QUESTION 139:

You are the network administrator for Certkiller . The LAN consists of a Windows 2000 Active Directory domain. The network also included a perimeter network (also known as the DMZ) that hosts all Internet-accessible services. The domain includes a Windows 2000 Server computer configured as an enterprise Certification Authority (CA) that issues IPsec certificates.

A Windows 2000 Advanced Server computer named Certkiller 1 runs Internet Information Services (IIS) 5.0. Certkiller 1 is a stand-alone server in a workgroup named Internet and is located in the DMZ.

The IT manager wants to allow external customers to connect to Certkiller 1 only by using HTTP or HTTPS protocols. However, administrators of Certkiller 1 need to connect to Certkiller 1 with protocols other than HTTP and HTTPS.

You create a custom IPsec policy named WebIPsec and assign the policy in the Local Security Policy of Certkiller 1. Then, you create two IPsec filters in the WebIPsec policy. You need to ensure that external customers can connect to Certkiller 1 only by using HTTP, HTTPS, and protocols not protected by IPsec. You also must ensure that administrators can connect to Certkiller 1 with all protocols.

What should you do?

- A. Configure the first filter to permit HTTP and HTTPS connections and the second filter to block all IP traffic.

Configure the WebIPSec policy to use Kerberos authentication.

B. Configure the first filter to permit HTTP and HTTPS connections and the second filter to negotiate security for all IP traffic.

Configure the WebIPSec policy to use Kerberos authentication.

C. Configure the first filter to permit HTTP and HTTPS connections and the second filter to negotiate security for all IP traffic.

Install an IPSec certificate on Certkiller 1.

Configure the WebIPSec policy to use certificate-based authentication.

D. Configure the first filter to negotiate security for HTTP and HTTPS connections and the second filter to block all IP traffic.

Install an IPSec certificate on Certkiller 1.

Configure the WebIPSec policy to use certificate-based authentication.

Answer: C

Explanation:

The first filter should permit HTTP and HTTPS traffic. As Certkiller 1 is a member server and there is CA in the domain we can use an IPSec certificate for Certkiller 1 and use certificate-based authentication.

Incorrect Answers

A: The second filter cannot block all IP traffic. We must allow the administrators to access Certkiller 1 with all protocols.

B: Certkiller 1 is a member of the domain, but not a domain controller. We cannot use Kerberos authentication on it.

D: We should not negotiate security for the filter.

QUESTION 140:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

Currently, five Windows 2000 member servers host the corporate Internet Web site.

These servers run Internet Information Services (IIS) 5.0.

You plan to enable authentication to access the Web site. Some customers who connect to the Web site use a certificate that you distribute to them. Other customers who do not have a valid certificate need to be prompted for a user name and password.

You have already installed a Web server certificate on the Web servers, and you have mapped all issued certificates to the correct user accounts. You want to ensure that users both with and without certificates are authenticated.

How should you configure each of the Web servers? (Each correct answer presents part of the solution. Choose two)

A. Change the authentication methods to disable Anonymous access.

B. Change the application protection level to High (Isolated).

C. Enable the Accept client certificates option.

D. Enable the Require client certificates option.

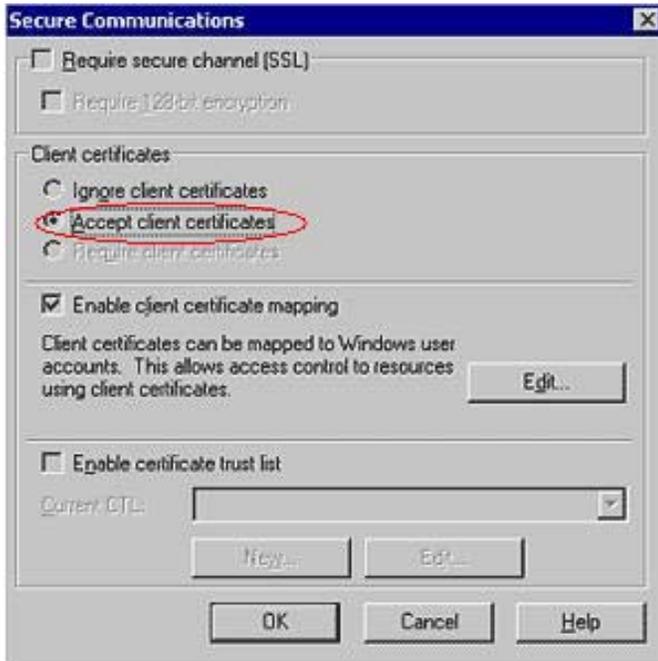
E. Enable the Require secure channel (SSL) option.

Answer: A, C

Explanation:

A: We should disable anonymous access.

C: We should enable client certificates.



Incorrect Answers

B: Running an application in High (Isolated) application protection level does not directly affect which authentication methods that are allowed.

D, E: We should not require either client certificates or secure channel (SSL).

QUESTION 141:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

A Windows 2000 Member server named Certkiller 1 hosts the corporate intranet Web site. Certkiller 1 runs Internet Information Services (IIS) 5.0. All files on Certkiller 1 are protected by NTFS permissions.

You want to allow users to use client certificates for authentication to the intranet Web site. You issue a certificate to all users and map each certificate to the correct domain user account. However, you cannot enable the Accept client certificates option for the intranet Web site.

What should you do?

A. Install a Certification Authority (CA) on Certkiller 1.

B. Install a Web server certificate on the intranet Web site.

- C. Configure the authentication methods of the intranet Web site to disable Anonymous access.
- D. Configure the local Group Policy on Certkiller 1 to assign the Store password using reversible encryption for all users in the domain policy.

Answer: B

Explanation:

We need a Web server certificate.

QUESTION 142:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains a Windows 2000 Server computer named Certkiller 1. Certkiller 1 runs Internet Information Services (IIS) and hosts intranet Web sites. All client computers run Windows 2000 Professional and use Microsoft Internet Explorer as their only Web browser.

The Payroll Web site is confidential. Only employees in the accounting department are allowed to connect to the Payroll Web site. Data transmitted to and from the Payroll Web site must be secure. The written security policy for Certkiller requires the strongest possible encryption and authentication on Certkiller 1.

You create a global group named Accounting_Users. The Accounting_Users group contains only user accounts for employees in the accounting department. You assign the Accounting_Users group NTFS permissions for the Payroll Web site. Now, you must ensure that Certkiller 1 complies with the written policy.

What should you do?

- A. On Certkiller 1, install a Web server certificate. Then, implement SSL security for the Default Web site, enforce 128-bit encryption, and enable only Basic authentication.
- B. On Certkiller 1, install a Web server certificate. Then, implement SSL security for the Payroll Web site, enforce 128-bit encryption, and enable only Integrated Windows authentication.
- C. On each client computer in the accounting department, install a computer certificate. On Certkiller 1, implement SSL security for the Default Web site, enforce 128-bit encryption, and enable only Basic authentication.
- D. On each client computer in the accounting department, install a computer certificate. On Certkiller 1, implement SSL security for the Payroll Web site, enforce 128-bit encryption, and enable only Integrated Windows authentication.

Answer: B

Explanation:

Integrated Windows authentication is also known as Windows NT Challenge/Response and NTLM. Integrated Windows authentication is fairly secure because it does not ever

transmit

actual passwords. Integrated Windows authentication uses either Kerberos or NTLM authentication protocols. Integrated Windows authentication enables the browser to use the current logon information to access secured data. If the user is already logged in to the network with a valid user name and password and tries to access web content that is secured using NTFS permissions, the browser can pass the logon information behind the scenes and authenticate the user without using any prompts for logon information. If the user has not logged on already, they are prompted for the logon information.

Further we need a certificate for the Web server, not for the clients.

Reference:

HOWTO: Set Up SSL Using IIS 5.0 and Certificate Server 2.0, Microsoft Knowledge Base Article - Q299525

Incorrect Answers

A,C : Basic authentication is supported by most browsers and most web servers in order to comply with HTTP specifications. When Basic authentication is implemented, IIS prompts users for a valid account and password that is then used to authenticate the user and to set file security so that the user is allowed to access data only according to permissions. A major security risk is associated with using Basic authentication: the logon information passes unencrypted.

D : We need a certificate for the Web server, not for the clients

QUESTION 143:

You are responsible for security for Certkiller network. The network consists of a Windows 2000 Active Directory domain. Certkiller uses Microsoft Exchange 2000 Server for e-mail services and implements the Key Management Services (KMS) to allow recover of e-mail private keys.

A consultant's portable computer is stolen during a business trip. No messages are lost due to the theft because the e-mail messages were stored on the mail server, named Certkiller 1.

You issue a new portable computer to the consultant. However, the consultant is unable to open previously encrypted e-mail messages and cannot send digitally signed messages to other employees in Certkiller .

You need to recover the e-mail messages and ensure that all e-mail sent from the consultant is digitally signed.

What should you do?

- A. Issue new digital signing and mail encryption certificates to the consultant.
- B. Issue a new mail encryption certificate to the consultant and have the consultant export the certificate and private key into a PKCS#12 format file.
- C. Recover the mail encryption private key and issue a new digital signing certificate to the consultant.
- D. Recover the mail encryption private keys from the KMS database and have the consultant export the certificate and private key into a PKCS#12 format file.

Answer: D

Explanation:

To recover the e-mail messages and to ensure that all e-mail sent from the consultant is digitally signed, we should recover the mail encryption private keys from the KMS database and have the consultant export the certificate and private key into a PKCS#12 format file.

QUESTION 144:

You are the network administrator for Certkiller . The network contains four Windows 2000 Server computers: Certkiller 1, Certkiller 2, Certkiller 3, and Certkiller 4. Certkiller 1, Certkiller 2, and Certkiller 3 run Routing and Remote Access and accept dial-up connections from company users. Each server is connected to a modem bank, which automatically directs an incoming phone number to the first free phone line. Certkiller 4 runs Internet Authentication Service (IAS). Certkiller 1, Certkiller 2, and Certkiller 3 are configured to use Certkiller 4 as a Remote Authentication Dial-In User Service (RADIUS) server. Certkiller 4 is configured to accept Certkiller 1, Certkiller 2, and Certkiller 3 as RADIUS clients.

You configure remote access policies on Certkiller 1 as shown in the following table.

Policy Order	Policy name	Policy condition
1	Allow_DU_Night	Allows Members of the Domain Users group to dial in between 5:00 P.M. and 11:00 P.M. each weekend
2	Allow_Admins	Allows members of the Domain Admins group to dial in at all times
3	Block_Weekend	Prevents all users from dialing in to the server on weekends

Members of the Domain Admins group report that they are sometimes able to connect on weekends. However, they can also connect at any time during the week. Members of the Domain Users group report that they are sometimes unable to connect during the week and are sometimes able to connect on weekends.

You need to ensure that all members of the Domain Users group can dial in only between 5:00 P.M. and 11: P.M. on weekdays and that all members of the Domain Admins group can dial in at any time. You also want to minimize the amount of time required to change or add remote access policies in the future.

What should you do?

- A. Configure Certkiller 4 to have the same remote access policies as Certkiller 1.
- B. Configure Certkiller 2 and Certkiller 3 to have the same remote access policies as Certkiller 1.

C. On Certkiller 1, move the Block_Weekend remote access policy to come before the Allow_Admins remote access policy.

D. On Certkiller 1, move the Block_Weekend remote access policy to come before the Allow_DU_Night remote access policy.

Answer: A

Explanation:

The Remote Access Policies (RAPs) on the RADIUS client Certkiller 1 are correctly configured. However, we need to use these RAPs on the RADIUS as well to ensure that they are applied to Certkiller 2 and Certkiller 3 as well.

Note:

Remote Access Policies are processed on by one in order. Only the first matching remote access policy is applied.

Incorrect Answers

B: We could apply the RAPs from Certkiller 1 on Certkiller 2 and Certkiller 3. However, if we in the future need to change the RAPs we would have to change them in three places.

We should administer the RAPs centrally on RADIUS server Certkiller 4.

C, D: There RAPs are ordered in the proper order. Furthermore, if we move Block_Weekend RAP before the Allow_admins or before the Allow_DU_Night, the Admins would not be able to get access on weekends.

QUESTION 145:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain and a Windows 2000 Server computer named Certkiller 1. Certkiller 1 is not a member of the domain. Certkiller 1 contains two network adapters. One network adapter is connected to Certkiller 's network, and the other is connected to the Internet. Certkiller 1 runs Routing and Remote Access and accepts virtual private network (VPN) connections from the Internet. Certkiller 1 is configured to audit all logon events and all account logon events. The security log on Certkiller 1 is configured with the default settings.

You review the Security log on Certkiller 1 and discover that a former employee named Jack establishes a VPN connection with Certkiller 1 every evening. The log reveals that Jack used her old user account to authenticate to Certkiller 1.

You need to secure the network against further access by Jack's user account and retain evidence of Jack's activity for Certkiller 's legal department. You also need to ensure that Certkiller 1 continues to function normally.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. On Certkiller 1, disable Jack's local user account.

B. On Certkiller 1, increase the size of the Security log to 1,024 KB.

C. On a domain controller, disable Jack's domain user account.

D. On Certkiller 1, save the contents of the Security log to a file named Certkiller 1Log.evt.

E. On Certkiller 1, stop Routing and Remote Access and set the startup mode to Disabled.

Answer: A, D

Explanation:

A: As Certkiller 1 is not a member of the domain we must disable Jack's local user account.

D: We must save the contents of the Security log before it is overwritten.

Incorrect Answers

B: We should immediately save the security log.

C: Certkiller 1 is not a member of the domain and Jack's domain user account cannot be used to access Certkiller 1.

E: We must ensure that Certkiller 1 functions normally. We cannot stop and disable the Routing and Remote Access service.

QUESTION 146:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain includes a Windows 2000 Server named Certkiller 1, which runs Routing and Remote Access. Certkiller 1 is configured to allow both dial-up and virtual private network (VPN) connections.

Certkiller issues smart cards. The smart cards will be used for both dial-in and VPN users.

All users who connect remotely to the network are issued Windows XP notebook computers with PC Card-based smart card readers. The users are required to use smart cards only when they connect to the network remotely. Smart card usage should not be enforced for local network authentication.

You need to implement a remote access solution that will enforce smart card access for all dial-up and VPN connections.

What should you do?

A. Enable the Smart card is required for interactive logon account option for all user accounts in the domain.

B. Issue a computer certificate to Certkiller 1.

Configure the Remote Access Policy at Certkiller 1 to accept only EAP-MD5 authentication and use the computer certificate for authentication.

C. Issue a user certificate to the Administrator account on Certkiller 1.

Configure the Remote Access Policy to accept only EAP-MD5 authentication and use the Administrator's user certificate for authentication.

D. Issue a computer certificate to Certkiller 1.

Configure the Remote Access Policy to accept only EAP-TLS authentication and use the computer certificate for authentication.

E. Issue a user certificate to the Administrator account on Certkiller 1.

Configure the Remote Access Policy to accept only EAP-TLS authentication and use the Administrator's user certificate for authentication.

Answer: D

Explanation:

For remote access connections, you must use the Extensible Authentication Protocol (EAP) with the Smart card or other certificate (TLS) EAP type, also known as EAP-Transport Level Security (EAP-TLS). To use smart cards for remote access authentication, you must do the following:

1. Configure remote access on the remote access server.
2. Install a computer certificate on the remote access server computer.
3. Enable a smart card logon process for the domain.
4. Enable the Extensible Authentication Protocol (EAP) and configure the Smart card or other certificate (TLS) EAP type on the remote access server computer.
5. Enable smart card authentication on the dial-up or VPN connection on the remote access client computer.

Reference:

Windows 2000 Server documentation, Using smart cards for remote access

QUESTION 147:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain is configured to audit logon events. Certkiller 's written security policy prohibits remote access to Certkiller network. All network services are in compliance with the written policy.

Jack is a user in the research department. On Friday, Jack leaves on a two-week vacation. The following Monday, you discover that the Security log on each domain controller in the domain contains the following event.

Event ID: 529 (0x0211)

Type: Failure Audit

Description: Logon Failure

Explanation: Unknown user name or bad password

User Name: Jack Domain: Certkiller

Logon Type: 3 Logon Process: NETLOGON

Authentication Package: NTLM Workstation Name: CK1

The event appears throughout the weekend in groups of three with 30-minute gaps between each appearance. As you are examining the log, the event occurs again three times in rapid succession.

You need to immediately prevent this security violation from succeeding. You do not want to affect other network users.

What should you do?

- A. Disable the domain computer account for CK1 .
- B. Disable the domain user account for Jack.
- C. Stop the Net Logon service on all domain controllers.
- D. Delete the domain user account that is used by the user of CK1 .

Answer: B

Explanation:

Someone is using Jack's user account in order to gain access to the network. We should disable the domain user account.

Incorrect Answers

A: We are interesting in preventing login using the user account. The computer account is not as important.

C: Stopping the Net Logon service would prevent all users from logging onto the domain.

D: It is better to just disable Jack's account. If we delete it we would have to recreate it with proper permissions and rights.

QUESTION 148:

You are the network administrator for you Certkiller Ltd. The network consists of a Windows NT 4.0 domain named Certkiller . The domain contains five Windows NT Server 4.0 computers that are configured as domain controllers. The PDC in the Certkiller domain is named CertK 3. The domain also includes a Windows NT Server 4.0 computer named CertK 1. CertK 1 runs Remote Access Service.

You upgrade Certkiller 1 to Windows 2000 Server. You upgrade CertK 3 to Windows 2000 Server. During the upgrade, you configure permissions on CertK 3 that are compatible with Windows 2000 Server computers.

Certkiller acquires another company that has a Windows NT 4.0 domain. You join the Windows NT Server 4.0 computer named CertK 2 to your domain. CertK 2 is running Remote Access Service. After CertK 2 joins the new domain, users report that they fail to authenticate to CertK 2 when they use a dial-up connection. You need to ensure users can use CertK 2 for remote access connections.

What should you do?

- A. Add the Everyone group to the Pre-Windows 2000 Compatible Access group.
- B. Add CertK 2 to the DNSUpdateProxy group.
- C. Import the Dcup.inf security template to the Local Security Policy on CertK .
- D. Import the Defltdc.inf security template to the Local Security Policy on CertK

Answer: A

Explanation:

By adding the Everyone special group as a member of the Pre-Windows 2000 Compatible Access group, any RAS caller is enabled to be authenticated by the Windows NT 4.0 RAS server.

Reference:

HOW TO: Add Users to the Pre-Windows 2000 Compatible Access Group, Microsoft Knowledge Base Article - Q303973

HOW TO: Restore the Default NTFS Permissions for Windows 2000, Microsoft Knowledge Base Article - Q266118

Incorrect Answers

B: The DNSUpdateProxy group is used to enable DHCP servers to update DNS records

that other DHCP servers in the DNSUpdateProxy group owns. It does not apply to this scenario,

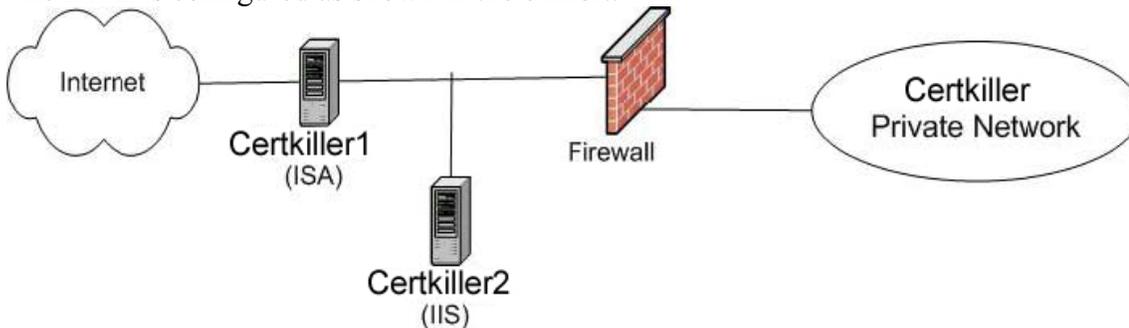
C: Dcup.inf should only be applied to Windows NT 4.0 domain controllers that have been upgraded to Windows 2000.

D: The Defltdc.inf security template is used on Windows 2000 domain controllers to apply default settings for NTFS permissions, registry permissions, default user rights, and so on. It does not apply here.

QUESTION 149:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain named Certkiller .com. The network contains a Microsoft Internet Security and Acceleration (ISA) Server computer named Certkiller 1 that protects the perimeter network (also known as DMZ) from the Internet. The DMZ contains a Windows 2000 Server computer named Certkiller 2. Certkiller 2 runs Internet Information Services (IIS) and is accessible from the Internet.

The DMZ is configured as shown in the exhibit.



Certkiller 2 hosts a Web-based application that requires SSL encryption. The written security policy for Certkiller requires that Certkiller 1 inspect all inbound traffic from the Internet.

To implement SSL encryption, you acquire a certificate named www. Certkiller .com from a commercial Certification Authority (CA). You install it on Certkiller 2. DNS correctly resolves the certificate's subject name with the Internet-accessible IP address for Certkiller 2.

You need to enable SSL encryption on the Web site and allow content inspection on all traffic that passes through Certkiller 1.

What should you do?

A. Export the certificate to a .cer-formatted file.

Import the .cer file to Certkiller 1.

Configure a firewall rule at Certkiller 1 that redirects SSL requests as HTTP requests.

B. Export the certificate and private key to a .pfx-formatted file.

Import the .pfx file to Certkiller 1.

Configure a firewall rule at Certkiller 1 that redirects SSL requests as HTTP requests.

C. Export the certificate to a .cer-formatted file.

Import the .cer file to Certkiller 1.

Configure a firewall rule at Certkiller 1 that redirects SSL requests as SSL requests.

D. Export the certificate and private key to a .pfx-formatted file.

Import the .pfx file to Certkiller 1.
Configure a firewall rule at Certkiller 1 that redirects SSL requests as SSL requests.

Answer: B

Explanation:

We must export the Personal Information Exchange, the .pfx file, from the IIS server to the ISA server. Furthermore we must configure the ISA server to redirect SSL requests as HTTP requests.

Note: The Internet Data Center architecture implementation of Secure Sockets Layer (SSL) bridging is designed to offload the processing of SSL packets from the IIS Web servers, and have the ISA Server 2000 computers manage the SSL sessions with Internet clients. Because the HTTPS connection will terminate at the ISA Server computers (and not at the Web servers), the Web server's certificate must be installed on each ISA Server computer. You must either obtain a new certificate from a certification authority or export an existing certificate from the IIS servers.

Incorrect Answers

A, C: We must export the Personal Information Exchange, the .pfx file, not the .cer file.

D: We must redirect the SSL requests as HTTP requests.

QUESTION 150:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains a Windows 2000 Server computer named Certkiller Srv. Certkiller Srv runs Microsoft SQL Server 2000 and contains databases that are used by all company employees. Certkiller Srv is configured as shown in the following table.

Configuration option	Parameter
Server role	Domain member server
SQL Authentication mode	Mixed mode
MSSQLServer service account	LocalSystem
SQL system administrator account name	sa
SQL system administrator account password	password

Certkiller Srv is configured to use domain groups as login accounts. Company users access Certkiller Srv by means of membership in the appropriate domain group. The written security policy for Certkiller prohibits the use of SQL Server login accounts on Certkiller Srv.

The written policy also prohibits any user from accessing Certkiller Srv by means of the sa login account.

You need to ensure that Certkiller Srv complies with the written policy, while continuing to allow access to authorized users.

Which action or actions should you take? (Choose all that apply)

- A. Configure Certkiller Srv to use Windows authentication.
- B. Configure Certkiller Srv as a member of a workgroup.
- C. Configure the MSSQLServer service in Certkiller Srv to use the local Administrator account.
- D. Configure the MSSQLServer service on Certkiller Srv to use the local non-administrative accounts.

Answer: A, C

Explanation:

A: By changing SQL Authentication mode from Mixed Mode to Windows Authentication mode sql logins, including the sa login, could not be used to access the SQL Server computer.

C: As Certkiller 1 is a Domain member server we should use the local Administrator account, not the LocalSystem, account for the MSSQLServer service.

Reference:

SQL Server Books Online, Authentication Modes

Incorrect Answers

B: The SQL Server computer is already a member of the domain. We should not make it a member of a workgroup.

D: Certkiller Srv needs local administrative rights and permissions.

QUESTION 151:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain.

The engineering department has several computers that run BSD UNIX. One of the engineers, Bruno, works from home two days a week and requires full access to the network over a dial-up connection.

All dial-up connections to the network are made through a Windows 2000 Server computer named Certkiller 1, which runs Routing and Remote Access. Certkiller 1 has the latest security updates applied.

Bruno's BSD UNIX client computer can authenticate to Certkiller 1 only by using CHAP authentication. You must allow Brunt to authenticate to Certkiller 1 by using CHAP but not allow other users to authenticate with CHAP authentication.

Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

- A. Create a new Remote Access Policy named UNIXChap on Certkiller 1. Modify the UNIXChap policy to allow only CHAP authentication.

Create a domain security group named AllOtherUsers and modify the UNIXChap policy to apply only to members of AllOtherUsers.

Add all user accounts except Bruno's account to the AllOtherUsers group.

Deny remote access permission for the remote access policy if the conditions are met.

B. Create a new Remote Access Policy named UNIXChap on Certkiller 1.

Modify the UNIXChap policy to allow only CHAP authentication.

Create a domain security group named UNIXUsers and modify the UNIXChap policy to apply only to members of UNIXUsers.

Add Bruno's user account to the UNIXUsers group.

Grant remote access permission for the remote access policy if the conditions are met.

C. Sort the Remote Access Policies on Certkiller 1 so that the default Remote Access Policy is first on the list.

D. Sort the Remote Access Policies on Certkiller 1 so that the default Remote Access Policy is last on the list.

E. Modify Bruno's user account to enable the Store Password using reversible encryption option.

Then, have Bruno change his password.

F. Modify Bruno's user account to enable the Account is trusted for delegation option.

Then, have Bruno change his password.

Answer: B, D, E

Explanation:

A remote network user trying to connect to the RRAS server will go through several steps that take an extremely short time to happen. The process is well documented in many places, but it deserves some attention here. The high-level steps are as follows:

(1). RRAS tries to match a policy with the conditions of the current connection attempt.

It starts from the top of the list of policies and goes down. If it finds a policy that matches the conditions, it uses that policy to determine permissions. If no policy is found that matches the conditions, the connection is denied.

(2). If a policy is found that matches the conditions, RRAS processes it for permissions.

This works as follows:

(a). If the account Dial-In tab is set to Allow Access, the connection can proceed.

(b). If the account Dial-In tab is set to Deny Access, the connection is denied.

(c). If the account Dial-In tab is set to Control Access Through Remote Access Policies, the permissions section of the policy is evaluated and processed according to its Grant or Deny permissions.

(3). The profile is applied to the connection. If the connection does not meet a parameter in the profile, the connection is denied.

As you can see, making the connection work properly involves many considerations.

Troubleshooting RAS policies can be easy if you keep these steps in mind and remember that

RRAS evaluates each policy in order starting from the top and going down. If RRAS finds a

match to the conditions and the connection fails because of permissions or profile constraints,

RRAS will not attempt to find another policy that might also match further down the list. Store password using reversible encryption - The intent of this policy is to provide support for applications which use protocols that require knowledge of the user password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing clear-text versions of the passwords. For this reason, this policy should never be enabled unless application requirements outweigh the need to protect password information.

Account is trusted for delegation - The user or object that is granted this privilege must have write access to the account control flags on the user or computer object. A server process running on a computer (or under a user context) that is trusted for delegation can access resources on another computer using a client's delegated credentials, as long as the client's account does not have the Account cannot be delegated account control flag set.

Reference:

Moc - Windows 2000 Network Infrastructure Administration (70-216) (Course 2153b)

QUESTION 152:

You are the network administrator for Certkiller . The network has a Windows 2000 Active Directory domain named Certkiller .com. Certkiller also has a UNIX Kerberos realm named kerb. Certkiller .com. Most client computers use Certkiller .com for network authentication. The remaining clients must use the Kerberos realm kerb. Certkiller .com. All computers on the network use the same DNS servers. All users have accounts in the Kerberos.com realm, and the users' passwords have been synchronized. Active Directory user accounts are mapped to the Kerberos account names in the Kerberos realm. You must provide access to resources shared within the Active Directory domain to the users of Windows 2000 Professional client computers when they authenticate to the kerb. Certkiller .com realm.

What should you do? (Each correct answer presents part of the solution. Choose two)

- A. Configure Certkiller .com to trust the kerb. Certkiller .com realm.
- B. Use KSetup to add the kerb. Certkiller .com to the Certkiller .com directory database.
- C. Map the root account from kerb. Certkiller .com to the administrator account of Certkiller .com.
- D. Use Kinit to obtain a ticket-granting ticket for your domain controllers.
- E. Use the Smbclient utility on kerb. Certkiller .com to map a drive to the Sysvol share on the Active Directory domain.
- F. Install Services for UNIX on the domain controllers.

Answer: E, F

Explanation :

Microsoft offers utilities and tools that allow UNIX clients to access a Windows 2000-based network. UNIX clients must be authenticated to maintain the security of your network. You must secure the common software, file systems, and protocols that UNIX clients use to access resources on a network. Three of the most common and most important file systems and protocols are Server Message Block (SMB), Network File

System (NFS), and Transmission

Control Protocol/Internet Protocol (TCP/IP).

Microsoft Services for UNIX version 2.0 includes tools that integrate UNIX and Windows networks. You can use Services for UNIX to improve the interoperability between UNIX clients and a Windows 2000 network. To connect from Unix to a windows 2000 machine we would use the SMBclient.

Reference :

<http://www.cs.washington.edu/lab/sw/uwcesamba.html>

QUESTION 153:

You are the administrator of a Windows 2000 Active Directory domain Certkiller .com. The domain contains 3,000 Windows Professional client computers and 250 Windows 2000 Server computers. Administrators of the domain is delegated to a group named DomainManagers.

The DomainManagers group has 12 user accounts in an organizational unit (OU) named Managers.

You need to ensure that the 12 user accounts in the DomainManagers group cannot be used by applications.

What should you do?

- A. Change the properties of the 12 user accounts to enable the Accounts is trusted for delegation option.
- B. Change the properties of the 12 user accounts to enable the Account is sensitive and cannot be delegated option.
- C. Create a new Group Policy object (GPO) and link it to the Managers OU. Configure the GPO to configure the Kerberos Maximum lifetime for server tickets and the Maximum lifetime for user tickets policies to 30 minutes. Assign the Apply Group Policy permission of the GPO to only the DomainManagers group.
- D. Create a new Group Policy object (GPO) and link it to the Managers OU. Configure the GPO to enable the Kerberos Enforce user logon restrictions policy. Assign the Apply Group Policy permission on the GPO to only the DomainManagers group.

Answer: B

Explanation:

Select the Account is sensitive and cannot be delegated option if this account cannot be assigned for delegation by another account.

Incorrect Answers

A: We must prevent that accounts will be delegated.

C: Maximum lifetime for server tickets - Determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service

D: Enforce user logon restrictions - Determines whether the Kerberos Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of

the target computer. Validation of each request for a session ticket is optional because the extra step takes time and may slow network access to services. By default, this setting is enabled in the Default Domain Group Policy object (GPO).

QUESTION 154:

You are the network administrator for Certkiller . The research department employees store all research-relates documents on a file server named Certkiller 1.

The research department manager mandates that all documents stored in the Research share on Certkiller 1 be encrypted by using the Encrypting File System (EFS) to prevent unauthorized access to the documents. You issue Basic EFS certificates to all research department members. You implement an EFS Recover Agent policy that enables EFS encryption. At Certkiller 1, you enable EFS encryption for the folder that is shared as Research.

When a user attempts to save a file to Research on Certkiller 1, the attempt fails. You verify that NTFS and share permissions are correctly configured.

You must enable EFS encryption for the Research share on Certkiller 1 and ensure that users can continue to access their files.

What should you do?

A. In the Active Directory Users and Computers console, modify the properties of Certkiller 1 to enable the Trust computer for delegation attribute.

B. In the Active Directory Users and Computers console, modify the properties of all research department user accounts to enable the Account is trusted for delegation attribute.

C. Modify the process so that research department users save the files to a different share on Certkiller 1 that does not implement EFS encryption.

At Certkiller 1, configure a batch file that copies the files into the encrypted Research share on Certkiller 1.

D. Modify the process so that research department users save the files locally to an EFS encryption-enabled folder.

Instruct the research department users to move their encrypted file to the Research share on Certkiller 1.

Answer: A

Explanation:

You cannot store encrypted files or folders on a remote server that is not trusted for delegation. to do this you must enable Trust computer for delegation.

Reference:

HOW TO: Encrypt a File in Windows XP, Microsoft Knowledge Base Article - Q307877

Incorrect Answers

B: The Account is trusted for delegation attribute is not useful here.

C,D: These are not an elegant solutions.

QUESTION 155:

You are the administrator of a Windows 2000 Active Directory domain. The domain consists of Windows 2000 Professional client computers and Windows 2000 Server computers.

You plan to deploy a new multitiered database application. The application consists of a client part that is run by users on the client computers, a service that runs on a Windows 2000 member server named Certkiller 1, and the database service that runs on multiple other Windows 2000 member servers. The client application connects to the service on Certkiller 1. The service on Certkiller 1 connects to the database service. The services for the new database application run on Certkiller 1, and the database servers run under LocalSystem.

The documentation for the new application states that it supports Kerberos proxy tickets to authenticate users to the database servers. You want to configure the network so that users can use this new application.

What should you do?

- A. Change the properties of the user accounts to enable the Account is trusted for delegation option.
- B. Change the properties of the Certkiller 1 computer account to enable the Trust computer for delegation option.
- C. Add the computer accounts of the database servers to the Pre-Windows 2000 Compatible Access group.
- D. Change the Kerberos policy in the Default Domain Policy to disable the Enforce user logon restrictions option.

Answer: B

Explanation:

Using Proxy Tickets the client can get a ticket for the back-end server and then give it to the front-end server.

To configure a service's account for delegation than runs under the Local System account, right-click the computer object in Active Directory Users and Computers, click Properties, then click the General tab. Check Trust computer for delegation.

Note: Multitier client/server applications present a special situation for the Kerberos protocol. In this kind of application, a client may connect to a server that must itself connect to a second server on the back end. For this to happen, the first server must have a ticket to the second. Ideally, the ticket should limit the first server's access on the second server to whatever the client, rather than the server, is authorized to do.

The protocol deals with this situation through a mechanism known as delegation of authentication. . Essentially, the client delegates authentication to a server by telling the KDC that the server is authorized to represent the client.

Delegation can be done two ways: either with proxy tickets or with forward tickets.

Reference:

White Paper, Windows 2000 Kerberos Authentication

Incorrect Answers

A: We should configure the computer account, not the user account, for delegation.

Note: To configure a client's account for delegation, right-click the object that represents the end user in Active Directory Users and Computers, click Properties, then the Account tab. In the Account options list, look for the option Account is sensitive and cannot be delegated. Make sure this option is not checked.

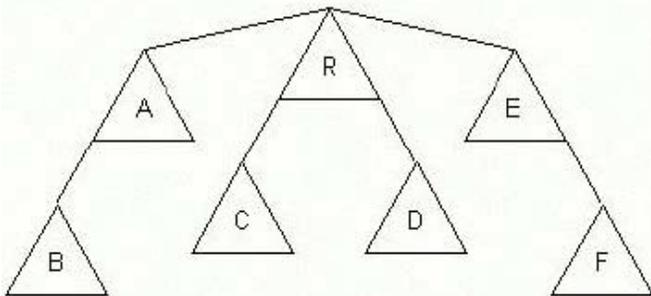
C: The Pre-Windows 2000 Compatible Access group has no use here.

D: Logon restrictions are not useful here

QUESTION 156:

You are the administrator of a Windows 2000 network. The network consists of a Windows 2000 forest with three domain trees.

The forest, domains, and domain relationships are shown in the exhibit.



Users in domains E and F often access resources in domains A and B. For performance and fault-tolerance reasons, you want to ensure that users from domains E and F can be authenticated in domains A and B without having to access domain controllers in root domain R.

What should you do?

- A. Create a shortcut trust relationship from domain A to domain E.
- B. Create a shortcut trust relationship from domain A to domain F, and create a shortcut trust relationship from domain B to domain E.
- C. Create a shortcut trust relationship from domain B to domain F.
- D. Create shortcut trust relationships from domain B to domain C, from domain C to domain D, and from domain D to domain F.

Answer: A

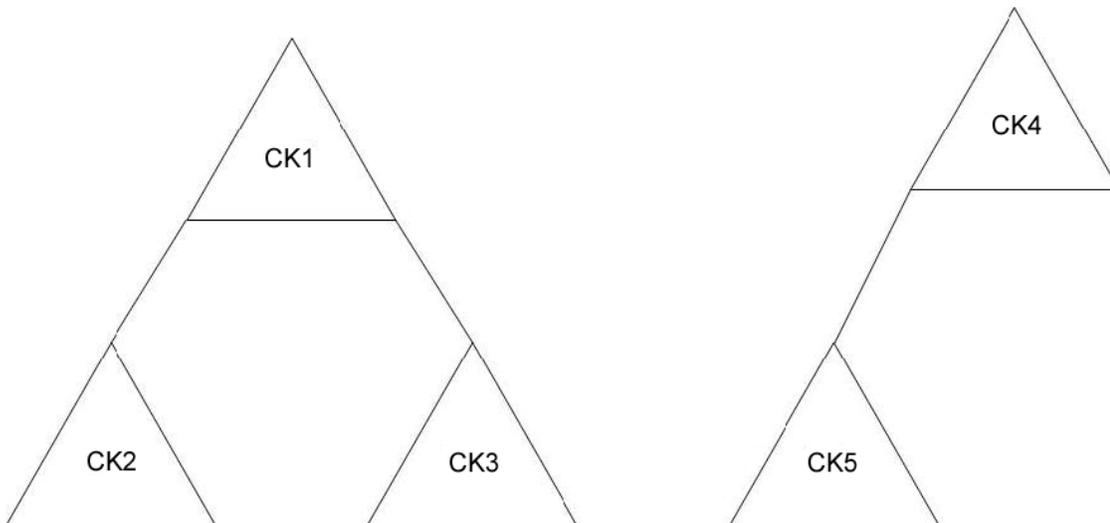
Explanation:

To solve the problem, we only need to create a shortcut trust relationship from domain A to domain E since they are root domains.

QUESTION 157:

You are the administrator of a Windows 2000 network. The network consists of two Windows 2000 forests with five Windows 2000 Domains.

The two forests, the domains, and domain relationship are shown in the exhibit.



You want to meet the following criteria:

- * Ensure that users from domain CK3 can access resources in domain CK4 and CK5 . Create trust relationships between the domains so that the necessary permissions and user rights can be granted.
 - * Create the least number of trust relationships.
- What should you do?

- A. Create a trust relationship from domain CK4 to domain CK1 , and create a trust relationship from domain CK1 to domain CK4 .
- B. Create a trust relationship from domain CK4 to domain CK3 , and create a trust relationship from domain CK5 to domain CK3 .
- C. Create a trust relationship from domain CK3 to domain CK4 , and create a trust relationship from domain CK3 to domain CK5 .
- D. Create a trust relationship from domain CK1 to domain CK4 , and create a trust relationship from domain CK1 to domain CK5 .

Answer: B

Explanation:

When a user attempts to gain access to a resource in another domain, the Kerberos V5 protocol must determine whether the trusting domain, which is the domain containing the resource to which the user is trying to gain access (CK4 & CK5), has a trust relationship with the trusted domain, which is the domain to which the user is logging on (CK3). To determine this relationship, the Kerberos V5 security protocol travels the trust path between the domain controller in the trusting domain to the domain controller in the trusted domain. Keep in mind that between separate forests the NTLM authentication protocol is used and not the Kerberos protocol. So we need to create the following trusts :

- * CK4 trusts CK3
- * CK5 trusts CK3

In the Active Directory Domain and trusts MMC on CK3 do the following:

- * In the : Domains that trust this domain section enter : CK4 and CK5

In the Active Directory Domain and trusts MMC on CK4 do the following:

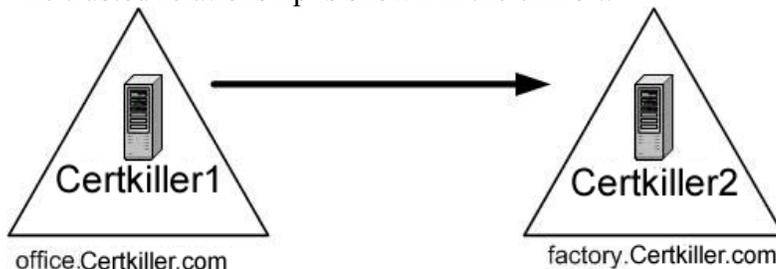
- * In the : Domains trusted by this domain section enter : CK3
- In the Active Directory Domain and trusts MMC on CK5 do the following:
- * In the : Domains trusted by this domain section enter : CK3

QUESTION 158:

You are the network administrator for Certkiller . The network consists of two Windows 2000 Active Directory forests: office. Certkiller .com and factory. Certkiller .com. Each forest consists of a Windows 2000 Active directory domain.

The two domains have a one-way external trust relationship in which office. Certkiller .com trusts factory. Certkiller .com.

The trusted relationship is shown in the exhibit.



The written security policy of Certkiller requires that Certkiller 1 must use IPSec to encrypt data to Certkiller 2. You configure a custom IPSec policy in the Local Security Policy on Certkiller 1 and on Certkiller 2. The custom IPSec policy implements Encapsulating Security Payload (ESP) for all data that is transmitted between Certkiller 1 and Certkiller 2. You also configure the IPSec security association to use Kerberos authentication.

After the IPSec security policies are assigned to Certkiller 1 and Certkiller 2, you discover that IP traffic between Certkiller 1 and Certkiller 2 is not encrypted. What should you do?

- A. Create a one-way external trust relationship in which factory. Certkiller .com trust office. Certkiller .com.
- B. Enable the Trust Computer for delegation option in the computer account properties on Certkiller 1 and on Certkiller 2.
- C. Modify the custom IPSec policies to use certificate-based authentication, and acquire IPSec certificates for Certkiller 1 and Certkiller 2 from a common root Certification Authority (CA).
- D. Create a computer account for Certkiller 1 in factory. Certkiller .com and a computer account for Certkiller 2 in office. Certkiller .com. Configure the new accounts to use Kerberos name mapping to map the new account name to existing computer account in the other forest.

Answer: A

Explanation:

Windows 2000 uses domain trusts, which are relationships that are established between domains that enable users in one domain to be authenticated by a domain controller in the

other domain. There are four types of domain trusts:

* Two-way: A link between domains in which each domain trusts user accounts in the other domain to use its resources.

* One-way: A single trust relationship where domainA trusts domainB. All one-way relationships are nontransitive.

* Transitive: The trust relationship that is extended to one domain is automatically extended to all other domains that trust that domain.

* Nontransitive: This trust relationship is bounded by the two domains in the trust relationship and does not flow to any other domains in the forest. You must explicitly create nontransitive trusts. Nontransitive trusts are one-way by default, although you can also create a two-way relationship by creating two one-way trusts.

Each trust relationship must use an authentication protocol to validate the trust as well as users. Windows 2000 supports two authentication protocols:

* Kerberos: An authentication protocol that is used to verify user or host identity. The Kerberos V5 authentication protocol is the default authentication service for Windows 2000.

* NTLM: A challenge/response authentication protocol. The NTLM authentication protocol is the default for network authentication in Microsoft Windows NT version 4.0 and earlier. The protocol continues to be supported in Windows 2000, but this protocol is no longer the default.

Windows 2000 does not support Kerberos trust relationships between two forests.

Kerberos trust relationships are used and created by default between parent and child domains in the same forest, or between tree root domains that are in the same forest.

Windows 2000 only performs cross-realm authentication with non-Windows Kerberos realms such as MIT Kerberos realm. For more information, refer to the "Step-by-Step Guide to Kerberos 5 (krb5 1.0) Interoperability" white paper that is located at the following Microsoft Web site:

<http://www.microsoft.com/windows2000/techinfo/planning/security/kerbsteps.asp>

Use an external trust relationship when a trust between two forests is required. This trust relationship uses NLTM authentication.

Reference:

Q274438 - Cannot Use Kerberos Trust Relationships Between Two Forests in Windows 2000

QUESTION 159:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain includes Windows 2000 Server computers, Windows 2000 Professional client computers, and Windows NT Workstation 4.0 client computers. All domain controllers run Windows 2000 Server.

Certkiller 1 is a Windows 2000 Server computer running Routing and Remote Access. Certkiller 1 accepts dial-up connections from remote Certkiller employees. Currently, all domain user accounts have dial-up access.

New written security policies for Certkiller require that only remote Certkiller employees be able to dial in to Certkiller 1 during company business hours. On weekends, only administrators are permitted to dial in.

You configure the remote access policies on Certkiller 1 to comply with the written

policies. However, when you attempt to modify the domain user accounts to use the remote access policies, the option is unavailable.

You need to ensure that the remote access policies on Certkiller 1 will be used to control dial-up access to Certkiller 1.

What should you do?

- A. Convert the domain to native mode.
 - B. Make Certkiller 1 a member of the RAS and IAS Servers group.
 - C. Add the Everyone group to the Pre-Windows 2000 Compatible Access group.
 - D. Install Internet Authentication Service (IAS) on Certkiller 1.
- Configure Routing and Remote Access to use IAS for authentication.

Answer: A

Explanation:

In the access-by-policy administrative model for a Windows 2000 native-mode domain, the remote access permission on every user account is set to Control access through Remote Access Policy and remote access permissions are determined by the remote access permission setting on the remote access policy. Therefore, the remote access permission setting on the remote access policy determines whether remote access permission is allowed or denied.

Note: In the access-by-policy administrative model for a Windows2000 mixed-mode domain, the remote access permission on every user account is set to Allow access, the default remote access policy is deleted, and separate remote access policies are created to define the types of connections that are allowed. On a remote access server running Windows2000 that is a member of a Windows2000 mixed-mode domain, the Control access through Remote Access Policy option is not available for remote access permission on the user account. If a connection attempt matches the conditions of a policy subject to the profile and user account dial-in settings, then the connection is accepted.

Reference:

Windows 2000 Server Documentation, Remote access policy administrative models

Incorrect Answers

B: People are able to access the network through RRAS. This makes it unnecessary to add Certkiller 1 to the RAS and IAS Servers group. Certkiller 1 must already be a member of this group.

C: By adding the Everyone special group as a member of the Pre-Windows 2000 Compatible Access group, any RAS caller is enabled to be authenticated by a Windows NT 4.0 RAS server. This does not apply in the current scenario since the RRAS is a Windows 2000 Server.

D: IAS is not required.

QUESTION 160:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains a Windows 2000 Server computer

named Certkiller 1. Certkiller 1 runs Internet Information Services (IIS). Certkiller 1 also hosts an intranet Web site that allows employees to use a Web interface to update address information. All client computers run Windows 2000 Professional and use Microsoft Internet Explorer as their default Web browser.

The written security policy of Certkiller requires that certificates be used when authenticated with the intranet Web site. To comply with the written policy, you must configure certificate authentication on Certkiller 1. Each user who connects to the Web site has an account in Active Directory. Certkiller 1 has a Web server certificate installed. You need to ensure that the written policy is enforced.

What should you do?

A. Install a computer certificate on each client computer.

On Certkiller 1, configure IIS to implement name mapping and require client certificates. Clear all authentication methods for the Web site.

B. Install a computer certificate on each client computer.

On Certkiller 1, configure IIS to use the Windows directory service mapper to implement name mapping and require client certificates.

Require Integrated Windows authentication for the Web site.

C. Request a user certificate for each user account.

On Certkiller 1, configure IIS to implement name mapping and require client certificates.

Require Integrated Windows authentication for the Web site.

D. Request a user certificate for each user account.

On Certkiller 1, configure IIS to use the Windows directory service mapper to implement name mapping and require client certificates,

Clear all authentication methods for the Web site.

Answer: B

Explanation :

Since we have only active directory users it is easier to use the Window Directory Service mapper then the name mappings . We should use a computer user certificate and Integrated Windows Authentication.

Reference:

HOW TO: Configure Client Certificate Mappings in Internet Information Services (IIS) 5.0

QUESTION 161:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

A Windows 2000 member server named Certkiller 1 hosts the corporate intranet Web site.

Certkiller 1 runs Internet Information Services (IIS) 5.0. Users on the network use an anonymous connection to connect to the intranet Web site.

The corporate security department has given you a custom security template for the Web server. You have applied the security template to Certkiller 1.

For the intranet Web site directory named Employees, you want to use a specific

anonymous account named AnonWeb. You create a new local user account named AnonWeb on Certkiller 1, remove the account from the Users group, and add it to the Guests group.

You configure IIS to use the AnonWeb account as the Anonymous user account for the Employees directory. You enable the Allow IIS to control password option for this account.

You want to ensure that AnonWeb is used by IIS as the anonymous user account when users connect to the Employees directory on the intranet Web site.

What should you do?

- A. Disable the local IUSR_ Certkiller 1 user account.
- B. Reset the password for the AnonWeb user account.
- C. Configure the AnonWeb user account to enable the User must change password at next logon option.
- D. Grant the AnonWeb user account the Access this computer from the network user right on Certkiller 1.

Answer: A

Explanation:

We must disable the default anonymous account on Certkiller 1 which is named IUSR_ Certkiller 1.

QUESTION 162:

You are the administrator of a Windows 2000 Server computer named Certkiller 1. Certkiller 1 runs Routing and Remote Access and is connected to several modems. Company employees dial in to Certkiller 1 to access Certkiller network. The network includes a Windows 2000 Active Directory domain, which contains user accounts for all company employees. All company employees use client computers that are running Windows 2000 Professional or Windows XP Professional.

Bruno reports that he cannot log on to Certkiller 1 by using his domain user account, although he does hear his modem dial in and connect. You reset Bruno's password and instruct him to try again. Bruno tries again and reports that he still cannot log on. You ask Bruno to verify his dial-up settings and discover that he is not using the correct phone number when he dials in.

You provide Bruno with the correct phone number. You need to ensure that Bruno's security credentials are not compromised. You also need to ensure that other employees' security credentials will not be compromised if they configure their client computers with an incorrect dial-in phone number.

What should you do? (Each correct answer presents part of the solution. Choose two)

- A. Instruct Bruno to change his domain password.
- B. Instruct Bruno to delete and re-create his dial-up connection.
- C. Enable callback on all domain user accounts that are authorized for dial-in access.
- D. Configure all employees' computers to require MS-CHAP v2 authentication for dial-in

connections.

E. Configure all employees' computers to require SPAP authentication for dial-in connections.

Answer: C, D

Explanation:

To ensure that Bruno's security credentials are not compromised and that of other employees', we must enable callback on all domain user accounts.

MS-CHAPv2 is the best idea for authentication.

Incorrect Answers

A: We need to enable callback.

B: This will not solve the issue

E: This will not solve the issue

QUESTION 163:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain includes a Windows 2000 Server computer named Certkiller 1, which runs Routing and Remote Access. Server is configured to allow PPTP connections to the network. Certkiller 1 is installed at the network perimeter.

Employees who work from home connect to Certkiller 1 to gain access to Certkiller network.

Employees connect to the network by using Windows 95, Windows 98, and Windows NT Workstation 4.0 client computers. Employees connect to Certkiller 1 by using their domain credentials to authenticate with the network.

The IT manager wants to ensure that the strongest form of authentication is used. You must configure Certkiller 1 to enforce the strongest authentication common to all connecting client computers.

You want to create a Connection Manager package that ensures that the strongest form of authentication is required for PPTP connections to Certkiller 1.

What should you do?

A. Install the Microsoft Directory Services Client software on all Windows 95, Windows 98, and Windows NT Workstation 4.0 client computers.

Configure the Connection Manager package to use only MS-CHAP v2 authentication.

Configure a Remote Access Policy on Certkiller 1 to accept only MS-CHAP v2 authentication.

B. Install the High Encryption Pack software on all Windows 95, Windows 98, and Windows NT Workstation 4.0 client computers.

Configure the Connection Manager package to use only MS-CHAP v2 authentication.

Configure a Remote Access Policy on Certkiller 1 to accept only MS-CHAP v2 authentication.

C. Install the Microsoft Directory Services Client software on all Windows 95, Windows 98, and Windows NT Workstation 4.0 client computers.

Configure the Connection Manager package to use only EAP-MD5 authentication.

Configure a Remote Access Policy on Certkiller 1 to accept only EAP-MD5 authentication.

D. Install the High Encryption Pack software on all Windows 95, Windows 98, and Windows NT Workstation 4.0 client computers.

Configure the Connection Manager package to use only EAP-MD5 authentication.

Configure a Remote Access Policy on Certkiller 1 to accept only EAP-MD5 authentication.

Answer: D

Explanation:

We need to install the High Encryption pack. We should use EAP-MD5 authentication for highest security.

Note 1: Message Digest 5 Challenge Handshake Authentication Protocol (EAP-MD5 CHAP) is an EAP type that uses the same challenge-handshake protocol as PPP-based CHAP, but the challenges and responses are sent as EAP messages. A typical use for EAP-MD5 CHAP is to authenticate the credentials of remote access clients by using user name and password security systems. You can also use EAP-MD5 CHAP to test EAP interoperability.

Note 2: The Internet Explorer High Encryption Pack gives you 128-bit encryption, the highest level of protection possible for all your Internet communications, including credit card use and financial transactions.

Note 3: To automate the configuration of large numbers of dial-up clients, a Connection Manager service profile is used on a Connection Point Services (CPS) server to create the client connection software that is installed on the client. The connection software provides the configuration for the dial-up connection that provides single-click access to the intranet. To provide cost-effective implementation, access support is outsourced to an Internet service provider (ISP), which provides the access numbers to the enterprise for incorporation into the client software.

Incorrect Answers

A, C: Microsoft Directory Services Client software will not help improve authentication security.

Note: Microsoft has developed extensions for the Microsoft Windows 95, Microsoft Windows 98, and Microsoft Windows NT 4.0 operating systems that allow those client platforms to take advantage of features provided by the Windows 2000 Active Directory service. These client extensions were developed for customers who wish to deploy Windows 2000 Server in environments with existing Windows 95-, Windows 98-, and Windows NT 4.0-based client workstations.

B: MS-CHAP v2 is not as secure as EAP-MD5.

Note: MS-CHAP v2, which provides mutual authentication between the remote access client and the remote access server. MS-CHAP v2 works with Windows 95 (with the Dial-Up Networking 1.3 Upgrade) or Windows 98 as well as Windows 2000.

QUESTION 164:

You are the network administrator for Certkiller . Certkiller consists of a main office and

branch office. Both offices are connected to the Internet through the same Internet service provider (ISP). The network in each office contains a Windows 2000 Active Directory domain, five Windows 2000 Server computers, and 100 Windows XP Professional computers. Employees at each office cannot connect to the network resources at the other office.

You install Routing and Remote Access on a Windows 2000 Server computer at each office and configure the servers to connect to one another by using PPTP. Employees report that they still cannot connect to network resources at the other office. You examine the two Routing and Remote Access servers and discover that neither one can connect to the other.

You connect both servers to a test subnet temporarily and verify that they can connect to each other. However, when you reconnect the servers to the office networks, they still cannot connect to each other.

You need to ensure that the two servers can connect to each other in order to provide access to network resources in each office. You also need to ensure that employees can continue to access network resources in their own office.

What should you do?

- A. Instruct your ISP to allow the PPTP port and the Generic Route Encapsulation (GRE) IP protocol between the two offices.
- B. Ensure that the network routers between the two offices are configured to support multicast traffic.
- C. Configure the client computers in each office to connect directly to the Routing and Remote Access server in the other office by using PPTP.
- D. Install the Internet Authentication Service (IAS) on both Routing and Remote Access servers.

Answer: C

Explanation:

To ensure that the two servers can connect to each other in order to provide access to network resources in each office and to ensure that employees can continue to access network resources in their own office, we must configure the client computers in each office to connect directly to the Routing and Remote Access server

Reference:

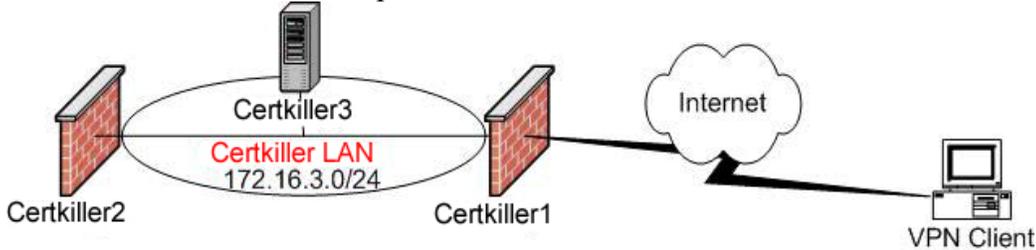
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg1001.asp>

QUESTION 165:

You are the network administrator for Certkiller . The network includes a perimeter network (also known as DMZ) that hosts all Internet-accessible services. The DMZ includes a Windows 2000 Server computer named Certkiller 3. Certkiller 3 runs Routing and Remote Access and is Certkiller 's virtual private network (VPN) server.

The written security policy for Certkiller requires that the addressing scheme used in the DMZ not be advertised on the Internet. The DMZ is protected by two third-party firewalls: Certkiller 1 and Certkiller 2. Certkiller 1 currently performs Network Address

Translation (NAT) on all traffic entering and exiting the DMZ.
The DMZ infrastructure components are shown in the exhibit.



Currently, VPN client computers can connect to Certkiller 3 by using PPTP connections. All VPN client computers are upgraded to Windows 2000 Professional from Windows 95, Windows 98, and Windows NT Workstation 4.0. The written security policy for Certkiller was recently modified to require L2TP/IPsec for VPN connections. To meet the written policy requirements, you configure Certkiller 3 to allow L2TP/IPSec VPN connections.

In tests using the current DMZ infrastructure, all L2TP/IPSec connections fail. You must allow L2TP/IPSec VPN connections to reach Certkiller 3.

What should you do?

- A. Disable the NAT services at Certkiller 1 and change the network-addressing scheme in the DMZ to use the 192.168.1.0/24 network address.
- B. Install a second network card at Certkiller 3 and connect the network card to the network segment attached to the Internet.
- C. Implement packet filters at Certkiller 1 that allow all connections that use L2TP to reach Certkiller 3.
Change the network-addressing scheme in the DMZ to use a public Internet address.
- D. Implement packet filters at Certkiller 1 that allow all connections that use Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) to reach Certkiller 3.
Change the network-addressing scheme in the DMZ to use a public Internet address.

Answer: D

Explanation:

We have to configure Certkiller 1 to disable NAT. A second common problem that prevents a successful IPsec session is the use of a Network Address Translator (NAT). Many small networks use a router with NAT functionality to share a single Internet address among all the computers on the network. The original version of IPsec drops a connection that goes through a NAT because it detects the NAT's address-mapping as packet tampering. Home networks frequently use an NAT, which blocks the use of L2TP/IPSec unless the client and VPN gateway both support the emerging NAT Transparency standard for IPsec. A good solution to this problem will be to give the DMZ zone public internet addresses.

Reference:

How to Troubleshoot a Microsoft L2TP/IPSec Virtual Private Network Client Connection,

<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q325/0/34.a>

S

Incorrect Answers:

A: The 192.168.x.x is also a private network address. So still we won't be able to use L2TP/IPsec because the firewall will still use NAT.

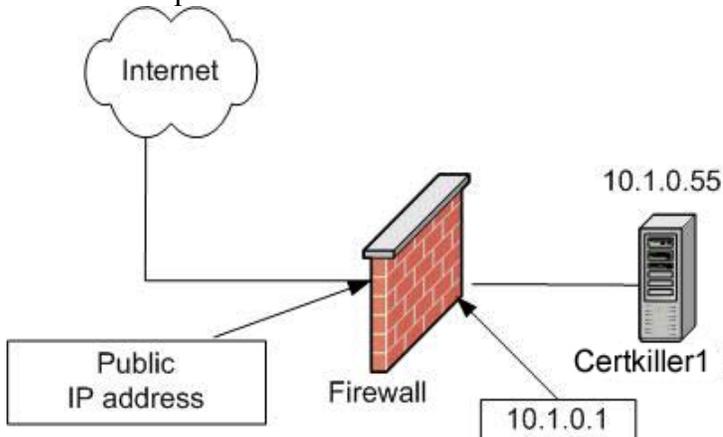
B: We do not need a second NIC. We would destroy our firewall solution.

C: This is the next best solution.

QUESTION 166:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain, a firewall, and a Windows 2000 Server computer named Certkiller 1. All Certkiller employees use portable computers that run Windows 2000 Professional and are members of the domain.

The relevant portion of the network is shown in the exhibit.



Certkiller 1 runs Routing and Remote Access. You configure Certkiller 1 to accept virtual private network (VPN) connections from Certkiller employees by means of the Internet. You configure Certkiller 1 to accept only VPN connections that use L2TP protocol. You also configure the firewall to route incoming VPN traffic directly to Certkiller 1. The firewall performs network address translation.

Certkiller employees report that when they attempt to establish a VPN connection to Certkiller 1, their portable computers display the following error message: "Unable to connect to server." You verify that the portable computers are configured with the default VPN settings.

You need to ensure that company employees can establish VPN connections to Certkiller 1 by means of the Internet. You also need to ensure that Certkiller 1 remains in a secure location on your network.

What should you do?

- A. Configure Certkiller 1 to accept only PPTP connections.
- B. Configure Certkiller 1 to have a computer certificate.
- C. Configure all portable computers to use only L2TP.
- D. Configure all portable computers to have a Hosts file that contains the IP address used by Certkiller 1.

Answer: A

Explanation:

We cannot combine NAT and L2TP/IPSec in Windows 2000. We must use PPTP instead of L2TP.

Note: If the Virtual Private Network (VPN) client is behind any network device performing Network Address Translation (NAT), the L2TP session fails because encrypted IPsec Encapsulating Security Payload (ESP) packets become corrupted.

Reference:

Basic L2TP/IPSec Troubleshooting in Windows, Microsoft Knowledge Base Article - Q259335

Incorrect Answers

B: The scenario does not require a certificate for the VPN server.

C: Both L2TP and PPTP are enabled by default. We need to disable L2TP.

D: This is not a name resolution problem.

QUESTION 167:

You are the network administrator for a branch office of Certkiller. The network consists of a Windows 2000 Active Directory domain and a Windows 2000 Server computer named Certkiller 1. Certkiller 1 runs Routing and Remote Access and uses PPTP connection by means of the Internet to connect to a Routing and Remote Access server at Certkiller's main office.

Bill is an employee in the branch office. When he works from home, Bill uses a Windows 2000 Professional computer to establish a PPTP connection to Certkiller 1. He reports that whenever he attempts to connect, he receives an error message.

You examine the System log on Certkiller 1 and discover the following error message: "The user Bill, attempting to connect on 2, was disconnected because of the following reason: A Remote Access Client attempted to connect over a port that was reserved for Routers only."

You need to ensure that Bill can use PPTP to connect to Certkiller 1. You also need to ensure that Certkiller 1 continues to provide a PPTP connection to the main office. What should you do?

- A. On Certkiller 1, open the properties of the virtual private network (VPN) port and set the Maximum ports property to 0.
- B. On Certkiller 1, open the properties of the virtual private network (VPN) port and select the Remote access connections (inbound only) check box.
- C. On Bill's computer, disable automatic virtual private network (VPN) protocol selection and ensure that only PPTP connections can be created.
- D. On Bill's computer, configure the Certificate Trust List (CTL) to include the Certification Authority (CA) that issued the computer certificate for Certkiller 1.

Answer: B

Explanation:

This behavior occurs because the server's RAS port is not configured to accept remote

access connections. To resolve this problem, use the following steps:

1. Start the Routing and Remote Access administrative tool.
2. Expand the options under your RAS server's name.
3. Click Ports, and then click Properties on the Action menu.
4. Click the appropriate port (L2TP, Modem, PPTP, LPT1, and so on), and then click Configure.
5. Click to select the Remote access connections (inbound only) check box, and then click OK.
6. Click Apply, and then click OK.

Reference:

RAS Clients Cannot Connect to Windows 2000 Demand-Dial Router, Microsoft Knowledge Base Article - Q262357

Incorrect Answers

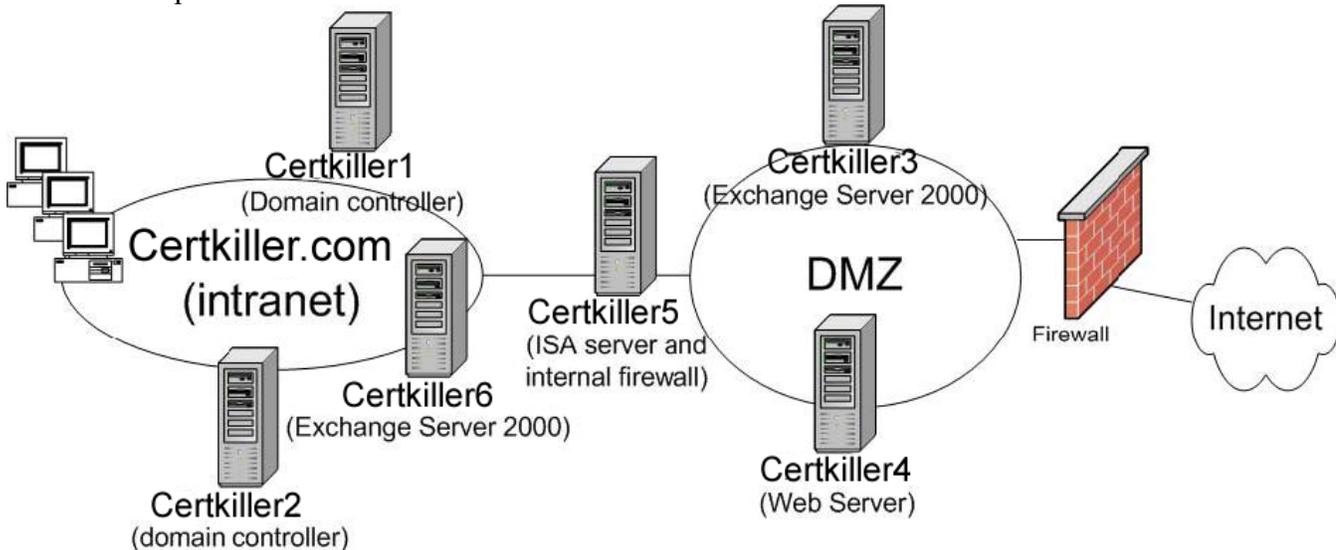
A, C: These procedures would not resolve the problem at hand.

D: There is no indication in the scenario that computer certificates are in use.

QUESTION 168:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. All servers run Windows 2000 Server. All client computers run Windows 2000 Professional.

The relevant portion of the network is shown in the exhibit.



Certkiller 5 runs Microsoft Internet Security and Acceleration (ISA) Server. Certkiller 3 runs Microsoft Exchange Server 2000. Certkiller 3 does not contain any user mailboxes. Certkiller 3 is used to send and receive e-mail via the Internet. All incoming e-mail is forwarded to Certkiller 6, which contains Certkiller 's mailboxes. A firewall rule on Certkiller 5 permits traffic between Certkiller 3 and Certkiller 6.

Certkiller Internet service provider (ISP) reports that it receives hundreds of complaints from Internet users who received unsolicited e-mail from Certkiller . You examine an unsolicited e-mail message and discover that it was sent through Certkiller 3 but that it was not sent by a user in Certkiller .

You need to ensure that Internet users cannot use Certkiller 's Exchange Server 2000 computer to send unsolicited e-mail. You also need to ensure that company users can continue to send and receive e-mail via the Internet.

What should you do?

- A. Configure Certkiller 5 to allow only outgoing e-mail from Certkiller 6.
- B. Configure Certkiller 3 to disallow mail relaying from unauthenticated users.
- C. Configure Certkiller 3 so that the HTTP, POP2, and IMAP4 protocols are disabled.
- D. Configure Certkiller 3 so that SMTP messages can be sent only from IP addresses on the intranet.

Answer: B

Explanation:

Relaying is when the machine sending the e-mail message is not your local machine and the machine receiving the e-mail message is also not your local machine. Spammers relay millions of e-mail messages through an open relay to disguise the source of SPAM. This is why blocking relaying is a good thing.

Reference:

Q310380 - HOW TO: Prevent Exchange 2000 from Being Used as a Mail Relay in Windows 2000

QUESTION 169:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. All client computers run Windows 2000 Professional. The network uses TCP/IP as its only transport protocol. All servers use static IP configuration settings. All client computers use DHCP to obtain their TCP/IP configuration. Each company department has a dedicated subnet, and the network DHCP server contains a scope for each subnet.

Users in Certkiller 's research department report that they cannot connect to the network. No users in other departments are reporting similar problems.

You view the System logs on each affected computer in the research department. In each case, the affected computer reports an IP address conflict with a computer in the network named CK1 . CK1 belonged to a user who recently left Certkiller . You examine CK1 and discover that the user had manually assigned all available IP addresses for the research department subnet to CK1 . You shut down CK1 , but when users attempt to renew their addresses, the renewal does not complete successfully.

You need to restore connectivity for the users in the research department, while minimizing the impact on users in other departments.

What should you do?

- A. On the DHCP server, delete each BAD_ADDRESS lease entry from the Address Leases list.
Instruct all research users to run the ipconfig /renew command on their computers.
- B. On the DHCP server, delete the DHCP database and disable IP address conflict

detection.

Instruct all research users to run the ipconfig /renew command on their computers.

C. On the DHCP server, stop and restart the DHCP Server service, and then disable support for BOOTP clients.

Instruct all research users to run the ipconfig /renew command on their computers.

D. On the DHCP server and on all client computers, disable gratuitous Address Resolution Protocol (ARP).

Instruct all research users to run the ipconfig /renew command on their computers.

Answer: A

Explanation:

The DHCP server detects conflicts (if enabled through the DHCP console via the DHCP server property sheet) by pinging an IP address before offering that address to clients. If the ping is successful (a response is received from a computer, meaning a conflict exists), a conflict is registered and that address is not offered to clients requesting a lease from the server. The address is marked with a BAD_Address value in the active leases. The address remains as a BAD_Address, and can be deleted from the active leases after the conflict is resolved, or remains for the lease duration of the scope and is then returned to the available pool. The DHCP server pings only addresses that have not been previously leased.

Note: The number of times the server tests an address for conflicts defaults to 0 (disabled). To change the value of this entry, use the DHCP console. Right-click the name of the server, click Properties, and then click the Advanced tab. For Conflict detection attempts, type a number greater than 0 (zero), and then click OK.

Reference:

Best Practises for Enterprise Security, Name Resolution for Administrative Authority DHCP Assigns "Bad_Address" to "Host Unreachable", Microsoft Knowledge Base Article - Q187802

[QUESTION 170:](#)

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain.

Mr Bill is an employee in the sales department. Bill uses a Windows 2000 Professional computer named CK1 . CK1 is a member of the domain.

On Tuesday morning, Bill reports that he logged off his computer when he left work on Monday at 6:00 P.M. However, when he returned to the office a few hours later, he was unable to log on to his computer.

Bill reports that he was able to log on to his computer on Tuesday morning.

You examine the Security log on a domain controller and discover the following event.

Event ID: 530 (0x0212)
Type: Failure Audit
Description: Logon Failure
Reason: Account logon time restriction violation
User Name: CERT Domain: CERTKILLER
Logon Type: 2 Logon Process: NETLOGON
Authentication Package: NTLM Workstation Name: CK1

You verify that the written security policy for Certkiller allows Bill to use his computer and network resources at any time. You need to ensure that Bill is able to log on to his computer at any time.

What should you do?

- A. Ensure that the Windows Time service on CK1 is configured to start automatically.
- B. Move the domain computer account for CK1 to the Computers container.
- C. Modify the properties of Bill's domain user account so that all logon hours are permitted.
- D. Ensure that the Windows Time service on CK1 is configured to log on by using the local system account.

Answer: C

Explanation:

The security log indicate that the Logon Failure was due to Account logon time restriction violation. We should modify Bill's domain user account so that he can logon at these late hours.

[QUESTION 171:](#)

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain and a Windows 2000 Server computer named Certkiller 1. Certkiller 1 runs Routing and Remote Access and accepts PPTP connections.

Two hundred company employees use portable computers that are running Windows XP Professional. These employees use PPTP connections to connect to Certkiller 1 by means of the Internet.

You reconfigure Certkiller 1 to accept only L2TP connections. You install a user and an IPsec computer certificate on each portable computer and configure the computers to use the certificate to authenticate to Certkiller 1. Users immediately report that they cannot connect to Certkiller 1 and that their portable computers display the following error message: "Error 792: The L2TP connection attempt failed because security negotiation times out."

You verify that the IPsec Policy Agent service is started on Certkiller 1. You need to ensure that users can establish L2TP connections with Certkiller 1.

What should you do?

- A. Reset the domain user account passwords of the employees who use portable computers.

- B. On the portable computers, disable automatic protocol selection, and then configure the computers to use only L2TP connections.
- C. On Certkiller 1, install a computer certificate that is issued by the same Certification Authority (CA) that issued the user certificates installed on the portable computers.
- D. On Certkiller 1, add the Certification Authority (CA) that issued the user certificates to a Certificate Trust List (CTL).
- Stop and restart the Routing and Remote Access service.

Answer: C

Explanation:

This issue can occur because of one of the following reasons:

- * The certificate on the virtual private networking (VPN) server is not a valid machine certificate or is missing. If the VPN server got a certificate during the Certificate Authority installation, this certificate is not valid for IPsec machine authentication.
- * The IPsec Policy Agent service is stopped and started without stopping and starting the Routing and Remote Access service on the remote computer.
- * The IPsec Policy Agent service is not running when you start the Routing and Remote Access service.

To resolve this issue, do one of the following:

- * Install a valid machine certificate on the VPN server.
- * Stop and start the IPsec Policy Agent service, and then stop and start the Routing and Remote Access service on the remote computer.

Reference:

Event ID 20111, Error 792 or Error 781 When Establishing an L2TP/IPsec Connection, Microsoft Knowledge Base Article - Q247231

Incorrect Answers

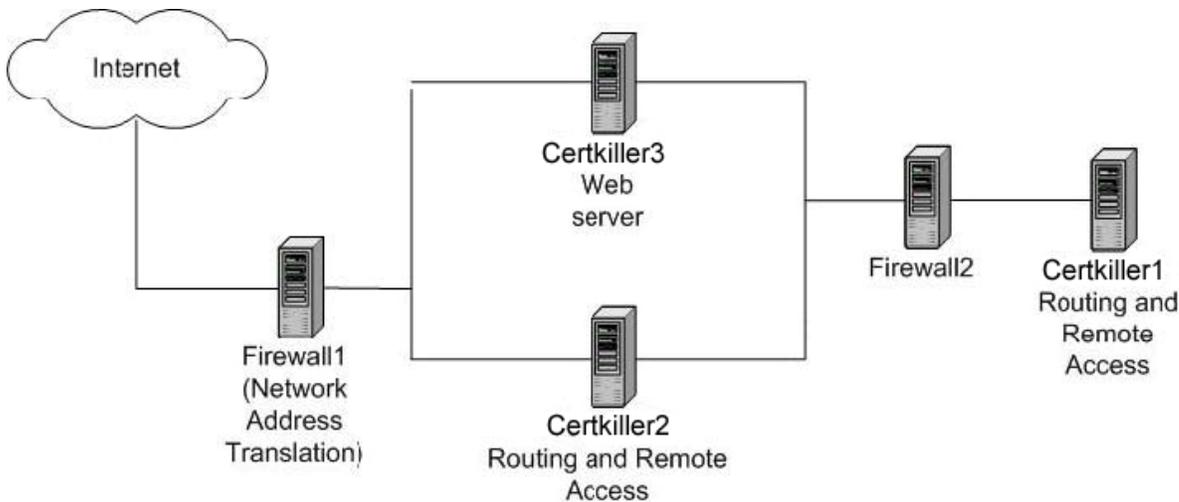
A, B: Has no effect in this scenario.

D: Incomplete procedure.

QUESTION 172:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain and five Windows 2000 Server computers.

The relevant portion of the network is shown in the exhibit.



All company employees use portable computers that are running Windows XP Professional. You want to configure the network so that Certkiller employees can use L2TP to connect to the network by means of the Internet. Which server should you configure to accept L2TP connections?

- A. Firewall1
- B. Firewall2
- C. Certkiller 1
- D. Certkiller 2
- E. Certkiller 3

Answer: A

Explanation:

L2TP with IPsec requires the following protocols: Encapsulating Security Payload (ESP), Internet Key Exchange (IKE), and L2TP.

Assuming there is a firewall protecting the intranet from the Internet, the placement of the L2TP server directly affects what IP filters are required on the firewall. If the L2TP server is outside of the firewall, the firewall will have to filter IKE and L2TP. If the L2TP is within the intranet, the firewall will have to filter IKE and ESP. The filtering configuration is required because the L2TP packets are encapsulated with the ESP packets.

QUESTION 173:

You are the network administrator for Certkiller. The network contains a Windows 2000 Active Directory domain and a Windows 2000 Server computer named Certkiller 1. Certkiller 1 runs Routing and Remote Access and is configured to accept virtual private network (VPN) connections by means of the Internet.

Jack is a member of the sales department. When she works from home, Jack uses a portable computer running Windows 2000 Professional. Jack asks you to configure her portable computer so that she can log on directly to the domain from home. You verify that Jack's Internet service provider (ISP) is configured to allow VPN traffic

to Certkiller network.

You create a new dial-up connection named Corp-VPN on Jack's computer. You configure the Corp-VPN connection to establish a VPN connection to Certkiller 1. The next day, Jack reports that she cannot log on to the domain from home because the Corp-VPN connection is not included in the list of dial-up connections on the Windows 2000 logon screen. However, she can log on to the domain when she is in the office.

You need to ensure that the logon screen on Jack's computer includes Corp-VPN in its list of dial-up connections.

How should you configure Jack's computer?

- A. Add Jack's domain user account to the local Power Users group.
- B. Log on by using the local Administrator account.

Create a new Corp-VPN connection that is available for all users.

- C. Install a user certificate.

Configure the computer's Certificate Trust List (CTL) to include the Certification Authority (CA) that issued the certificate.

- D. Instruct Jack to log on by using his domain user account.

Then, instruct Jack to create a new connection named Corp-VPN2.

Provide Jack with the TCP/IP address for Certkiller 1, and instruct him to accept the defaults for all other settings.

Answer: B

Explanation:

The VPN connection that was created is only available for the the network administrator (you). It must be created with the Local Administrator's account. It must also be made available for all users.

Reference:

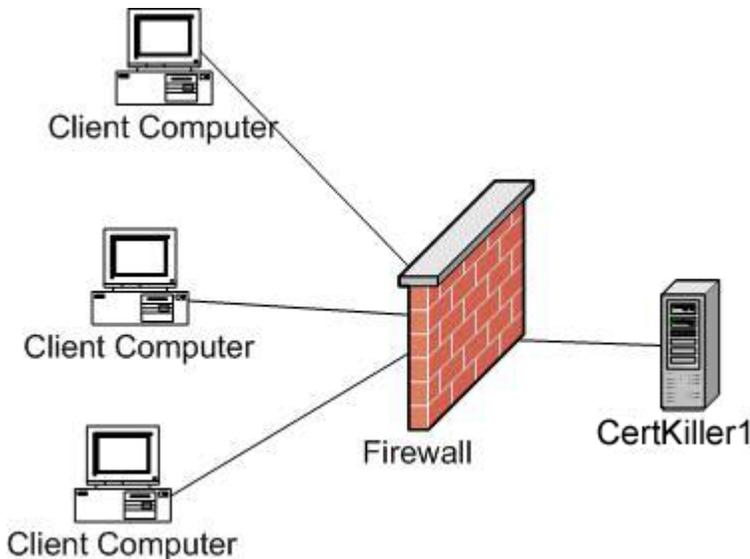
VPN Connection Is Not Available for Logon with Dial-Up Networking, Microsoft Knowledge Base Article - Q231426

[QUESTION 174:](#)

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains a Windows 2000 Server computer named Certkiller 1. Certkiller 1 runs Microsoft Exchange Server 2000.

Several client computers do not run Microsoft operating systems. These computers connect to Certkiller 1 by using POP3 client software. A third-party firewall protects Certkiller 1 and performs network address translation between Certkiller network and the Internet. The firewall forwards POP3 and SMTP requests to Certkiller 1.

The relevant portion of the network is shown in the exhibit.



During a security audit, you discover that using POP3 on the network is a security risk. The user information and password entered in the POP3 client software are transmitted to Certkiller 1 from the client computers in clear text format. You must secure POP3 client authentication to prevent the interception of user names and passwords. What should you do?

- A. Install an IPsec certificate on Certkiller 1 and on each client computer that requires POP3 access. Then, on each client computer, create and assign an IPsec policy that applies Encapsulating Security Payload (ESP) encryption to all traffic sent to the POP3 port on Certkiller 1.
- B. Install an IPsec certificate on Certkiller 1 on each client computer that requires POP3 access. Then, on each client computer, create and assign an IPsec utility that applies Encapsulating Security Payload (ESP) encryption to all traffic sent to the POP3/S port on Certkiller 1.
- C. Install a Web server certificate on Certkiller 1. Configure Exchange Server 2000 to use the certificate to enable POP3 over SLL connections. Configure the POP3 client software to connect to Certkiller 1 by using the POP3/S port.
- D. Install a Web server certificate on Certkiller 1. Configure Exchange Server 2000 to use the certificate to enable POP3 over SLL connections. Configure the POP3 client software to use Secure Password Authentication (SPA).

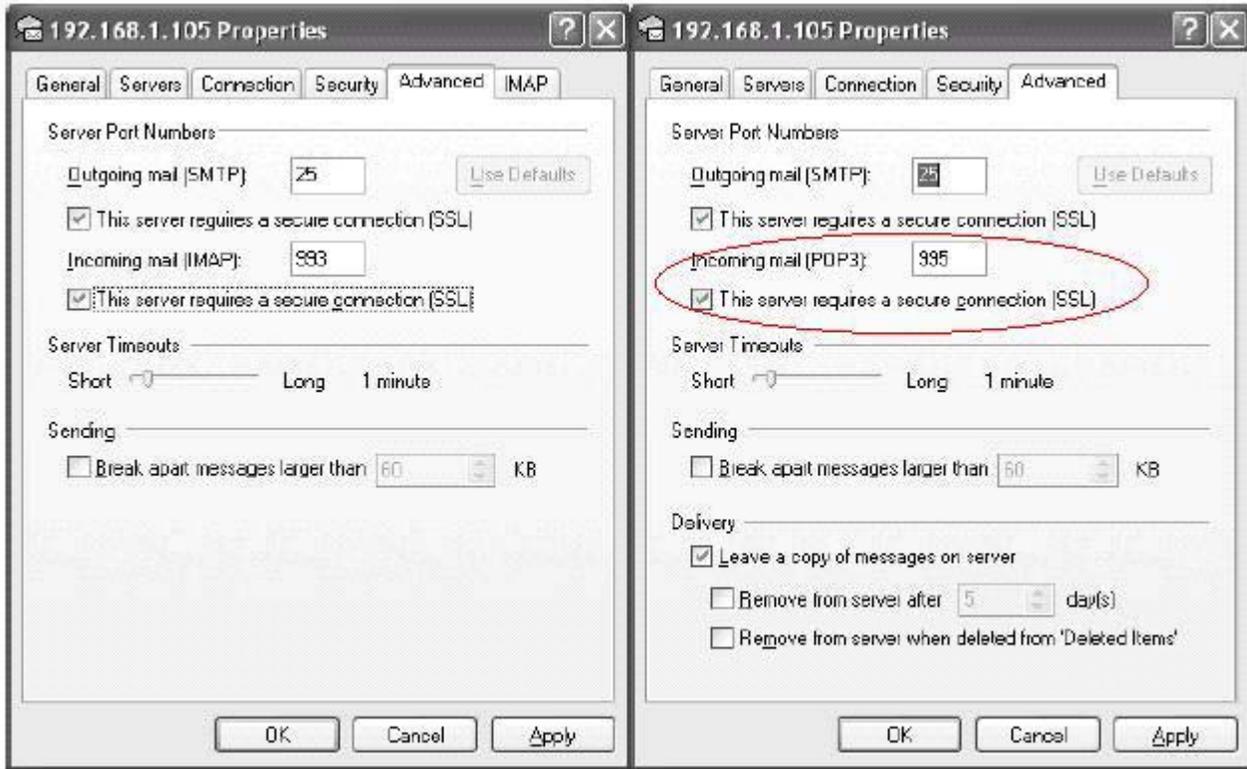
Answer: C

Explanation:

Many companies set up POP3 for their external e-mail users that want to use Outlook or Outlook Express from home to read and respond to their e-mail. Using POP3, though,

you need to be careful in configuring the e-mail client so that it does not download all of your e-mail from the e-mail server. If you are not careful, the next time the user is in the office, they will find an empty e-mail box and may then ask for it to be restored from tape.

Just like IMAP4, the main problem with using POP3 to download e-mail to an external e-mail client is that the messages travel in the clear. This means that the e-mail and all its contents, including attachments, can be captured off the Internet and viewed by a potential hacker. To prevent this, you need to use SSL to secure POP3 from these unintended viewers.



Reference:

<http://www.microsoft.com/technet/community/columns/cableguy/cg0802.msp>

Incorrect Answers

D: As answer D states we have configured the Exchange Server to user Secure POP 3 and not for SPA so we can NOT use SPA for the clients as well.

A, B: Network Address Translation (NAT) allows a device that supports NAT to intercept all traffic bound for the Internet from the intranet and replace the source IP in the packet with its own source IP address. When the packet response returns from the destination and reaches the NAT device or service, NAT then replaces the destination IP with the IP address of the internal device.

NAT is a strong solution because it hides the originator's IP address from the Internet.

NAT is also nice from the standpoint of ISPs that can now reduce the number of IP addresses leased to most companies since they can use NAT devices or services. Using NAT allows most companies to use private IP address ranges for all internal networks.

The major problem with NAT is that it is not able to properly handle all IP packets going

from the internal network out to the Internet. One of the biggest problems with NAT is that it cannot support L2TP/IPSec tunneling because the IPSec Encapsulating Security Payload (ESP) packets become corrupted. VPN servers and VPN clients cannot use L2TP/IPSec tunneling if any of them are behind NAT devices or servers using NAT.

QUESTION 175:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain and include five Windows 2000 Server computers that are used as dial-up servers by 6,000 remote company employees. These employees use portable computers running Windows 95, Windows 98, Windows NT Workstation 4.0, or Windows 2000 Professional.

Each portable computer is configured to contain five dial-up connections. Each connection dials the phone number associated with a specific dial-up server. If a dial-up server has no free phone lines, employees must select a different connection.

Your phone company informs you that the area code and prefix used by Certkiller 's dial-up servers will be changing. You decide to implement a single dial-up phone number, which will automatically seek a free phone line. The new phone number will coexist with the old phone numbers for 30 days.

You need to provide a new dial-up configuration to each portable computer. Each portable computer must use this new configuration. You also want to minimize the amount of administrative time required to provide the new configuration.

What should you do?

- A. Create a new dial-up connection named Redirect on each dial-up server. Configure the Redirect connection with the new dial-up phone number.
- B. Create a new connection profile by using the Connection Manager Administration Kit. Send the resulting file to all remote employees via e-mail, and instruct them to run the file on their computers.
- C. Create a new connection profile by using the Connection Manager Administration Kit. Save the resulting file in the Sysvol folder on a domain controller.
- D. Create a new dial-up connection that uses the new phone number. Use Regedit.exe to export the registry key that contains the dial-up connection settings. Send the resulting registry file to all remote employees via e-mail, and instruct them to run the file on their computers.

Answer: B

Explanation:

We need to create a new connection profile by using the Connection Manager Administration Kit and send the resulting file to all remote employees via e-mail, and instruct them to run the file on their computers to provide a new dial-up configuration to each portable computer.

Reference:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itcommunity/chats/trans/win2ksrv/sw2062>

0

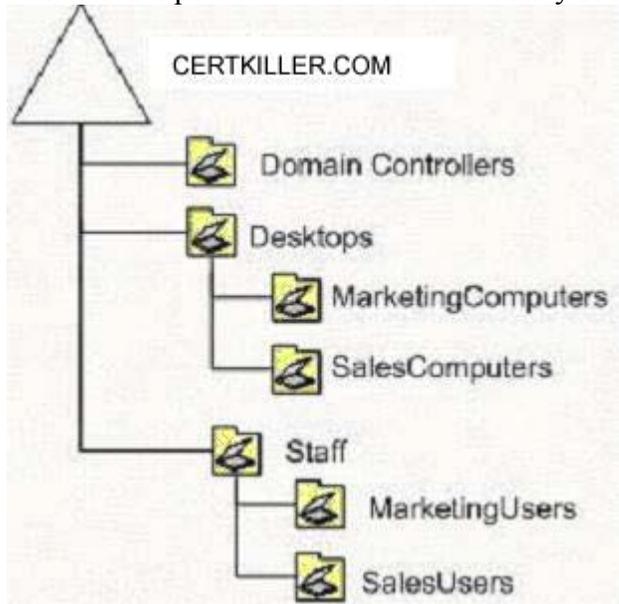
Incorrect Answers:

- A: We must use the Connection Manager Administration Kit
- C: We cannot just save the file into the Sysvol folder
- D: We must use the Connection Manager Administration Kit

QUESTION 176:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain named Certkiller .com. All client computers run Windows 2000 Professional and are domain members.

The relevant portion of the Active Directory structure is shown in the exhibit.



The written security policy of Certkiller allows departments to implement separate Encrypting File System (EFS) Recovery Agents. The EFS Recover Agent policies are defined in Active Directory, as shown in the following table.

Group Policy container	EFS Recovery Agent
Certkiller .com domain	Certkiller \DomainEFS
Domain Controllers OU	Certkiller \DCEFS
Desktops OU	Certkiller \OtherEFS
SalesUsers OU	Certkiller \SalesEFS

The EFS recover agent certificates and private keys are exported to PKCS#12 files and stored in a safe on the IT department. The private keys are removed from the original user's profile during the export process.

A user in the Sales department named Bruno has several EFS-encrypted files on his portable computer. Bruno's computer account is located in the SalesComputers OU and

his user account is located in the SalesUsers OU.

The operating system on Bruno's portable computer was reinstalled last week and now he cannot open any of his EFS-encrypted files. You must recover the encrypted files on Bruno's portable computer.

What should you do?

- A. Import the DCEFS certificate and private key into your domain user account on Bruno's computer and decrypt the encrypted files.
- B. Import the DomainEFS certificate and private key into your domain user account on Bruno's computer and decrypt the encrypted files.
- C. Import the OtherEFS certificate and private key into your domain user account on Bruno's computer and decrypt the encrypted files.
- D. Import the SalesEFS certificate and private key into your domain user account on Bruno's computer and decrypt the encrypted files.

Answer: D

Explanation:

To recover the encrypted files on Bruno's portable computer, we should Import the SalesEFS certificate and private key into your domain user account on Bruno's computer and decrypt the encrypted files.

The best way to bring the encrypted files together with the recovery certificates is to begin by backing up the encrypted files. Remember that the backup process preserves the files because it doesn't attempt to decrypt or re-encrypt the file as a part of the process. Once you've made a backup of the secure files, send the backup file to the recovery agent via secure E-mail. When the recovery agent receives the E-mail, they can restore the backup file and begin the recovery process. Remember that the designated recovery agent must restore the backup onto an NTFS version 5 partition or the operation won't work. Another way to bring the recovery certificates and the encrypted files together is for the recovery agent to physically travel to the computer that contains the encrypted files and then import his or her recovery certificates.

Reference:

http://www.brienposey.com/kb/recovering_encrypted_data.asp

Incorrect Answers:

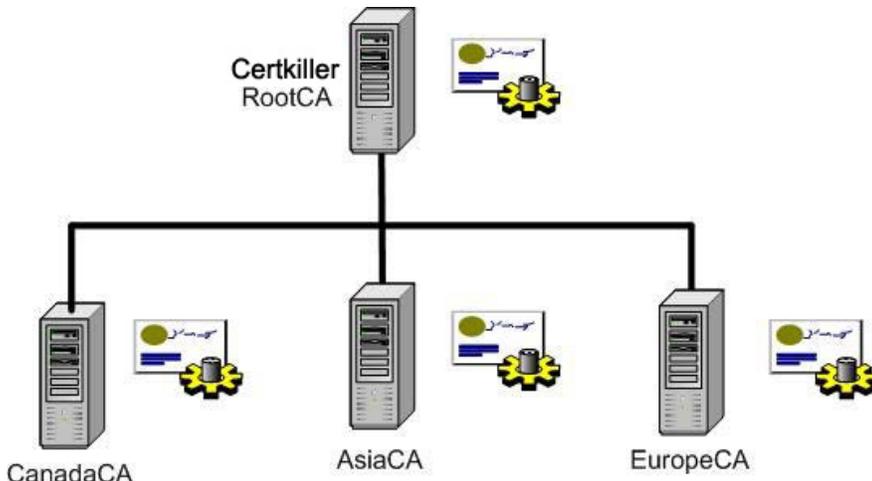
- A: We must import the SalesEFS certificate
- B: We must import the SalesEFS certificate
- C: We must import the SalesEFS certificate

QUESTION 177:

You are responsible for Public Key Infrastructure (PKI) management for the network of Certkiller . The network consists of three Windows 2000 Active Directory domains in a single forest.

You are in charge of deploying a PKI to facilitate certificate issuance within the Certkiller company.

You deploy the Certification Authority (CA) hierarchy shown in the exhibit.



You install RootCA with a stand-alone policy and remove it from the network. You attempt to issue certificates to the users and computers in the three domains, but all attempts fail. You inspect the event logs and see events that indicate that RootCA is not a trusted root CA in Certkiller . You need to issue certificates to users and computers in all three domains. What should you do?

- A. In the forest domain, modify the Default Domain Policy to define RootCA as a Trusted Root Certification Authority.
- B. Run the certutil command from any of the CanadaCA, AsiaCA, or EuropeCA computers to publish the RootCA certificate in Active Directory.
- C. Run the certreq command from any of the CanadaCA, AsiaCA, and EuropeCA computers to submit a certificate request to the RootCA.
- D. E-mail the RootCA certificate to all company employees and instruct them to double-click the certificate attachment and import the certificate to the default location.

Answer: B

Explanation:

Certutil.exe is a command-line program that is installed as part of Certificate Services in Windows 2000 Server. This is a useful tool for administrators who are managing CAs and troubleshooting certificate-related issues. Certutil can be used to

1. display certificate services configuration information
2. revoke certificates,
3. publish or retrieve a certificate revocation list
4. determine the validity of a certificate
5. verify public/private key pairs
6. resubmit or deny pending certificate requests
7. display certificates in the certificate store import issued certificates
8. shut down the server

Reference:

Using Certutil.exe to Manage and Troubleshoot Certificate Services

<http://www.microsoft.com/windows2000/techinfo/administration/security/certutil.asp>

Incorrect Answers

A: We must apply the certificates in each domain separately.

C: Certreq.exe is used to request certificates from a C

A. However, the RootCA has been removed from the network.

D: We cannot depend on the end users to configure the certificates.

QUESTION 178:

You are responsible for Public Key Infrastructure (PKI) management for the network of Certkiller . The network consists of a Windows 2000 Active Directory domain. A Group Policy object (GPO) named GetCertificates implements automatic certificate request settings to deploy IPsec certificates.

Your manager wants to implement IPsec between all Windows 2000 computers on the network. You must develop a method for deploying the IPsec certificates that requires the least amount of user input during the certificate enrollment process.

What should you do?

A. Install an enterprise Certification Authority (CA).

Grant Read and Enroll permissions for the IPsec certificate template to the Domain Users global group.

Link the GetCertificates GPO to the domain.

B. Install a stand-alone Certification Authority (CA).

Grant Read and Enroll permissions for the IPsec certificate template to the Domain Users global group.

Link the GetCertificates GPO to the domain.

C. Install an enterprise Certification Authority (CA).

Grant Read and Enroll permissions for the IPsec certificate template to the Domain Computers global group.

Link the GetCertificates GPO to the domain.

D. Install a stand-alone Certification Authority (CA).

Grant Read and Enroll permissions for the IPsec certificate template to the Domain Computers global group.

Link the GetCertificates GPO to the domain.

Answer: C

Explanation:

As we are using IPsec within the Windows 2000 domain only we should use an enterprise C

A. Furthermore, we should deploy the IPsec certificate template to computers not to users.

Note: By default, any user account you create in a domain is automatically added to the Domain Users group and any computer account you create is automatically added to the Domain Computers group.

Reference: Step-by-Step Guide to Internet Protocol Security (IPsec)

Incorrect Answers

A: We should deploy the IPsec certificate template to computers not to users.

B: As we are using IPsec within the Windows 2000 domain only we should use an enterprise CA, not a stand-alone CA.

D: As we are using IPsec within the Windows 2000 domain only we should use an enterprise CA, not a stand-alone CA.

QUESTION 179:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain and does not implement a Public Key Infrastructure (PKI). Several consultants participate in the network and use Windows 2000 Professional portable computers that are not members of the Active Directory domain.

You maintain accounting software that only domain members can access. A

Windows 2000 Server computer named Certkiller 1 runs the accounting software.

You must create a solution that ensures that only domain members can connect to Certkiller 1. The solution must not introduce any new network services to Certkiller 's network.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Configure the custom IPsec policy to implement Encapsulating Security Payload (ESP) for all IP traffic connecting to Certkiller 1.

Configure the IPsec policy to use certificate-based authentication to authenticate domain member computers connecting to Certkiller 1.

B. Configure the custom IPsec policy to implement Encapsulating Security Payload (ESP) for all IP traffic connecting to Certkiller 1.

Configure the IPsec policy to use Kerberos authentication to authenticate domain member computers connecting to Certkiller 1.

C. Configure the custom IPsec policy to implement Authentication Header (AH) for all IP traffic connecting to Certkiller 1.

Configure the IPsec policy to use certificate-based authentication to authenticate domain member computers connecting to Certkiller 1.

D. Configure the custom IPsec policy to implement Authentication Header (AH) for all IP traffic connecting to Certkiller 1.

Configure the IPsec policy to use Kerberos authentication to authenticate domain member computers connecting to Certkiller 1.

E. In the Local Security Policy of Certkiller 1, enable the Digitally sign server communications (always) security policy.

F. Create a new Group Policy object (GPO) and link it to the domain.

Configure the GPO to which enable the Digitally sign client communications (always) security policy.

Answer: B, F

Explanation:

B: We secure all IP traffic with ESP and use Kerberos for authentication.

F: Digital signing places a digital signature into each SMB, which is then verified by both the client and the server. We must enable the Digitally sign client communications (always) security policy throughout the domain so we should configure a GPO with this policy and link it to the domain.

Incorrect Answers

A: Certificate based authentication would require the additional certification service to be run.

C, D: Authentication Header (AH) would only ensure secure authentication, not secure traffic.

E: We must configure the clients, not only the server, for digital signing.

QUESTION 180:

You are responsible for Public Key Infrastructure (PKI) management for the network of Certkiller. The network consists of a Windows 2000 Active Directory domain. The network includes a Certification Authority (CA) named Certkiller 1 that was originally installed in Windows NT 4.0 as a stand-alone C

A. You upgrade Certkiller 1 to Windows 2000.

You need to convert Certkiller 1 to an enterprise CA and ensure that Certkiller 1 can manage all existing certificates issued by the CA.

What should you do?

A. Perform a System State backup of Certkiller 1.

Remove Certificate Services from Certkiller 1.

Reinstall Certificate Services as an enterprise CA by using a new key pair and certificate.

Restore the CA database from the System State backup.

B. Perform a System State backup of Certkiller 1.

Export the existing private key and certificate of the CA.

Remove Certificate Services.

Reinstall Certificate Services as an enterprise CA by using the existing key pair and certificate.

Restore the CA database from the System State backup.

C. Backup the CA by using the Certification Authority console.

Remove the Certificate Services.

Reinstall Certificate Services as an enterprise CA by using a new key pair and certificate.

Restore the CA database in the Certification Authority console.

D. Backup the CA by using the Certification Authority console.

Remove Certificate Services.

Reinstall Certificate Services as an enterprise CA by using the existing key pair and certificate saved by the backup from the Certification Authority console.

Restore the CA database in the Certification Authority console.

Answer: D

Explanation:

We must reinstall Certificate Services. First we backup Certificate Services from the Certification Authority console. We must ensure that we use preserve the existing key pair and certificate, and use this when Certificate Services is installed, since we want to perform an upgrade.

Procedure to back up the Certificate Services:

To backup the service

1. In the > Certification Authority console, right-click the name of the CA.
2. Point to > All Tasks on the context menu, and then click Backup CA.
3. The Certification Authority Backup Wizard starts. Read the message, and then click Next.
4. Check the boxes for the items to be included in the backup. (In this case, you will back up both the Key/Certificate and log/queue.) Click the > Private key and CA certificate check box. Also, click the Issued certificate log and pending certificate request queue check box. Specify a folder for the backup in the text box by typing the name or by clicking Browse. Then, click Next
5. Finish the wizard.

Reference:

Step-by-Step Guide to Administering Certificate Services

<http://www.microsoft.com/windows2000/techinfo/planning/security/adminca.asp>

Incorrect Answers

A, B: A system state backup would not backup the Certificates Services.

C: Since we want to upgrade Certificates Services we should not discard the existing key pair and certificate.

QUESTION 181:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory forest.

A Windows 2000 Server computer named Certkiller 1 runs Internet Information Services (IIS) and hosts a Web site that allows customers to purchase Certkiller 's goods. To protect the transactions, Certkiller 1 requires a Web server certificate and must implement SSL encryption.

The written security policy for Certkiller requires that all customers use certificate-based authentication when they connect to a secured Webs site. The application running on the Web server requires the existence of a custom Object Identifier (OID) in the presented certificate. You need to map the digital certificates to Active Directory user accounts by using one-to-one certificate mapping.

You need to acquire a Web server certificate and user certificates that comply with the written policy.

What should you do?

- A. Obtain the certificates from a commercial Certification Authority (CA).
- B. Obtain the certificates from a private Certification Authority (CA) that is hosted on Certkiller network.

C. Obtain the Web Server certificate from a commercial Certification Authority (CA) and the user certificates from a private CA that is hosted on Certkiller network.

D. Obtain the user certificates from a commercial Certification Authority (CA) and the Web server certificate from a private CA that is hosted on Certkiller network.

Answer: C

Explanation:

The web server must use a certificate from a commercial public CA, since the Web server will be accessed by clients outside the Windows 2000 domain.

The user certificates, on the other hand, should be obtained from a private CA since they are going to be mapped using one-to-one certificate mapping to Active Directory user accounts.

Note: An OID (Object identifier) is a globally (i.e., worldwide) unique identifier required by Open System Interconnection (OSI) International Standards and Recommendations to identify an X.500 object.

Incorrect Answers

A: We need to map the digital certificates to Active Directory user accounts by using one-to-one certificate mapping. We should therefore not use a commercial Certification Authority (CA) for the user certificates.

B: A private Certification Authority (CA) can not be used since customers, which are not part of the Windows 2000 domain, will access the Web server.

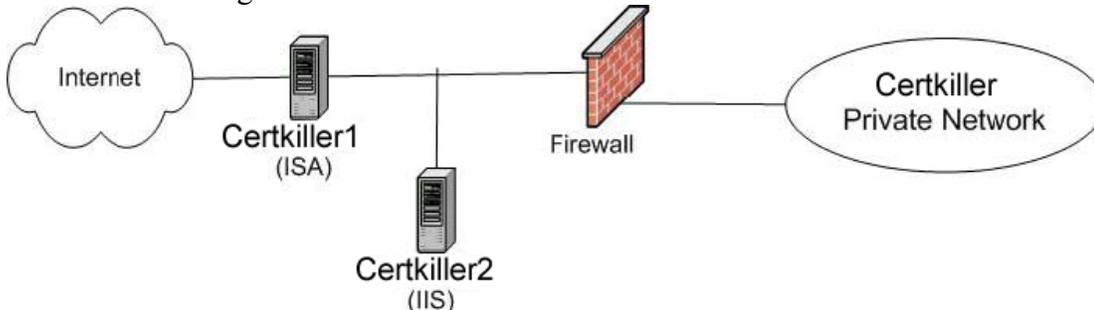
D: The Web server must use a public Web server certificate.

QUESTION 182:

You are the network administrator for Certkiller. The network consists of a Windows 2000 Active Directory domain named Certkiller.com. The network contains a Microsoft Internet Security and Acceleration (ISA) server named Certkiller 1.

Certkiller 1 protects the perimeter network (also known as the DMZ) from the Internet. The DMZ contains a Windows 2000 Advanced Server computer named Certkiller 2. Certkiller 2 runs Internet Information Services (IIS). Users can access Certkiller 2 from the Internet by using the DNS name Certkiller 2.Certkiller.com.

The DMZ is configured as shown in the exhibit.



Certkiller 2 hosts a Web-based application that requires SSL encryption. To implement SSL encryption, you acquire a certificate named www.Certkiller.com from a commercial Certification Authority (CA). You install the certificate on Certkiller 2.

DNS correctly resolves the certificate's subject name with the Internet-accessible IP

address for Certkiller 2.

The written security policy of Certkiller requires that the end-to-end encryption be provided for all access to the Web-based application and that the application support failover in the event of server failure. To meet the written policy, you configure a Web cluster that contains Certkiller 2 and two other Windows 2000 Advanced Server computers: Certkiller 3 and Certkiller 4. You modify the www. Certkiller .com DNS resource record to reference the address of the Web cluster. On Certkiller 1, you modify the existing firewall rule to redirect SSL requests to the IP address of the Web cluster.

Customers now report that they cannot always access the application when connecting to www. Certkiller .com.

You need to make sure that customers can always connect to the Web cluster. What should you do?

- A. On Certkiller 1, modify the firewall rule to redirect SSL requests to the IP addresses of the computers in the Web cluster as HTTP requests.
- B. Export the www. Certkiller .com certificate from Certkiller 2 to a .cer file. Import the .cer file to Certkiller 3 and Certkiller 4. On each computer in the Web cluster, configure IIS to use the www. Certkiller .com certificate for SSL encryption.
- C. Export the www. Certkiller .com certificate and private key from Certkiller 2 to a .pfx file. Import the pfx file to Certkiller 3 and Certkiller 4. On each computer in the Web cluster, configure IIS to use the www. Certkiller .com certificate for SSL encryption.
- D. Acquire two additional Web server certificates named www. Certkiller .com from the commercial CA. Install the certificates on Certkiller 3 and Certkiller 4. On each computer in the Web cluster, configure IIS to use the www. Certkiller .com certificate for SSL encryption.

Answer: C

Explanation:

Customers now report : "that they cannot always access the application when connecting to www. Certkiller .com." So sometimes they can connect. The reason for this is that we have installed a Certificate on Certkiller 2, but not on Certkiller 3 and Certkiller 4. We have to implement the Certificate thats on Certkiller 2 to Certkiller 3 and Certkiller 4.

When you use Internet Information Services (IIS) version 5.0, you may want to restore a server certificate, for example, if you are migrating one Web site to another server in a Web farm. In order to complete this operation, you must have a backup of the server certificate (and private key) contained in a PFX file (PKCS #12 (.pfx))

Reference:

How to Import a Server Certificate for Use in Internet Information Services 5.0,
Microsoft Knowledge Base Article - Q232137

Prescriptive Architecture Guide I, Chapter 7 - Deploying the Firewalls, Configuring SSL Bridging

Incorrect Answers

A: If we intended to configure SSL bridging the ISA server would have to use the IIS server certificate.

Note: The Internet Data Center architecture implementation of Secure Sockets Layer (SSL) bridging is designed to offload the processing of SSL packets from the IIS Web servers, and have the ISA Server 2000 computers manage the SSL sessions with Internet clients. Because the HTTPS connection will terminate at the ISA Server computers (and not at the Web servers), the Web server's certificate must be installed on each ISA Server computer. You must either obtain a new certificate from a certification authority or export an existing certificate from the IIS servers. This will be the Web server certificate that clients receive when they establish an HTTPS session, so it should include the fully qualified domain name (FQDN) of your Web site.

B: DER uses .cer files, Base-64 uses .cer files , and PKCS #7 uses (.p7b) files. In this example we must export the private key and certificate. And this implies PKCS #12.

D: We must use the same Web certificate on all Web servers in the cluster

QUESTION 183:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

A Windows 2000 Member served named Certkiller 1 host the corporate Internet Web site. Certkiller 1 runs Internet Information Services (IIS) 5.0. Users on the Internet connect to the corporate Internet Web site by using an anonymous SSL connection.

The corporate security department has given you a test custom security template for the Web server. You have applied the security template to Certkiller 1. You also want to improve security by requiring users to authenticate to the Web site. You configure IIS on Certkiller 1 to require Basic authentication and disallow Anonymous access. You create a new user account for each user who needs to gain access to the Internet Web site. You configure the accounts so that the passwords never expire. You provide logon credentials to each user.

However, these users report that they receive the error message "HTTP 401.1 - Unauthorized: Logon Failed" when they attempt to connect to the Internet Web site with the credentials you provided to them.

You want to ensure that these users can use Basic authentication to connect to the corporate Internet Web site.

What should you do?

A. Enable the Trust computer for delegation option for the Certkiller 1 computer account in Active Directory.

B. Configure IIS on Certkiller 1 to enable the Accept client certificates option.

C. Configure IIS on Certkiller 1 to enable the Enable client certificate mapping option.

D. Grant the new user accounts the Log on locally user right on Certkiller 1.

E. Configure Certkiller 1 to set the Number of previous logons to cache option to 0.

F. Configure Certkiller 1 to set the LAN Manager Authentication level to Send LM and NTLM responses.

Answer: D

Explanation:

If users with Basic Authentication rights are having trouble accessing your site, please check that the users have been given the right to log on locally.

Reference:

Users Cannot Access FTP or Web Site

<http://support.microsoft.com/support/kb/articles/q185/3/77.asp>.

Incorrect Answers:

A: Enabling the Trust computer for delegation option will not allow users to log on locally

B: Configuring IIS on Certkiller 1 to enable the Accept client certificates option is not necessary, since we desire to use Basic Authentication

C: Configuring IIS on Certkiller 1 to enable the Enable client certificate mapping option is not necessary.

E: Configuring Certkiller 1 to set the Number of previous logons to cache option has nothing to do with allowing them to log on locally.

F: Configuring Certkiller 1 to set the LAN Manager Authentication level to Send LM and NTLM responses will not solve the problem.

QUESTION 184:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain on three Windows 2000 Server computers.

One of these computers is named Certkiller 1. Certkiller 1 acts as a firewall and can also act as a virtual private network (VPN) server. Certkiller 1 is connected to the Internet and to the internal network.

The network also contains 500 portable computers running Windows 95, Windows 98, Windows Me, Windows 2000 Professional, or Windows XP Professional. All Windows 95, Windows 98, and Windows Me computers use the Microsoft Directory Services Client.

You want to ensure that all company employees can use their portable computers to connect to Certkiller network by means of the Internet without using third-party software.

You also want to connections to be as secure as possible, while maintaining the same solution for all computers.

What should you do?

A. Configure the portable computers to use L2TP and IPSec.

Configure the portable computers and Certkiller 1 to use a shared secret.

B. Configure Certkiller 1 to accept PPTP connections.

Configure the portable computers to connect to Certkiller 1 by using PPTP.

C. Install a computer certificate on Certkiller 1.

Configure the portable computers to trust the Certification Authority (CA) that issued the certificate.

D. Install a computer certificate on each portable computer.

Configure Certkiller 1 to trust the Certification Authority (CA) that issued the certificates.

Answer: B

Explanation:

L2TP is similar to PPTP in that its primary purpose is to create an encrypted tunnel through an untrusted network. L2TP differs from PPTP in that it provides tunneling but not encryption. L2TP provides a secure tunnel by cooperating with other encryption technologies such as IPsec. This was introduced in Windows 2000.

PPTP offers encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection and is an extension of PPP.

Reference:

How to Install Virtual Private Networking in Windows Me/98,
<http://support.microsoft.com/default.asp?scid=kb;en-us;288779>

Using the Microsoft L2TP/IPsec VPN Client with Windows 98, Windows Millennium Edition, and Windows NT 4.0

<http://support.microsoft.com/default.asp?scid=kb;en-us;325032>

HOW TO: Configure Packet Filter Support for PPTP VPN Clients in Windows 2000

<http://support.microsoft.com/default.asp?scid=kb;en-us;310111>

VPN Tunnels - PPTP Protocol Packet Description and Use

<http://support.microsoft.com/default.asp?scid=kb;en-us;241252>

Incorrect Answers:

A: We cannot use L2TP since the clients cannot support it.

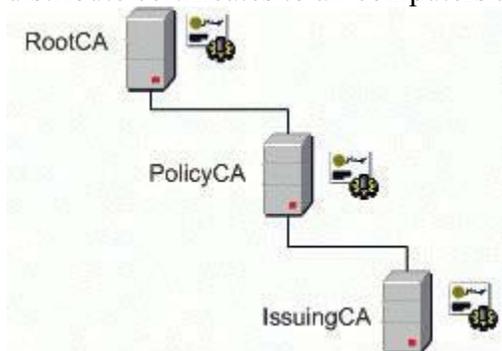
C: PPTP is a better alternative compared to computer certificates.

D: PPTP is a better alternative compared to computer certificates.

QUESTION 185:

You are responsible for Public Key Infrastructure (PKI) management of the network for Certkiller. The network consists of a Windows 2000 Active Directory domain.

You establish the Certification Authority (CA) hierarchy shown in the exhibit to distribute certificates to all computers and users in Certkiller.



RootCA and PolicyCA are removed from the network. IssuingCA issues all certificates to the users and computers on your network.

IssuingCA and Web server named Certkiller 1 are accessible from the Internet. External customers who do not have computer accounts in Certkiller's domain must access Certkiller 1 by using certificate-based authentication with certificates issued by IssuingCA.

For each external customer, you create a user account that the External customer must use to request a user certificate from IssuingC

A. You create a global group named

ExternalUsers and grant the group Read and Enroll permissions for the user certificate template. You add all external customer user accounts to the ExternalUsers group.

You must allow external users to request user certificates from the Internet. You must also ensure that Certkiller 1 and the external customers can perform Certificate Revocation List (CRL) checking for the certificates issued by IssuingCA.

What should you do?

A. Publish the CRL for IssuingCA to Certkiller 1.

Have external customers request personal certificates from IssuingCA by using the Certificate Request Wizard in the Certificates snap-in at their client computers.

B. Publish the CRL for IssuingCA to Certkiller 1.

Have external customers request personal certificates from IssuingCA by using the Web enrollment pages hosted on IssuingCA.

C. Publish the Root Certification Authority and Subordinate Certification Authority certificates and CRLs for IssuingCA, PolicyCA, and RootCA to Certkiller 1.

Have external customers request personal certificates from IssuingCA by using the Web enrollment pages hosted on IssuingCA.

D. Publish the Root Certification Authority and Subordinate Certification Authority certificates and CRLs for IssuingCA, PolicyCA, and RootCA to Certkiller 1.

Have external customers request personal certificates from IssuingCA by using the Certificate Request Wizard in the Certificate snap-in at their client computers.

Answer: C

Explanation :

We must Publish the Root Certification Authority and Subordinate Certification Authority certificates and CRLs for IssuingCA, PolicyCA, and RootCA to Certkiller 1.

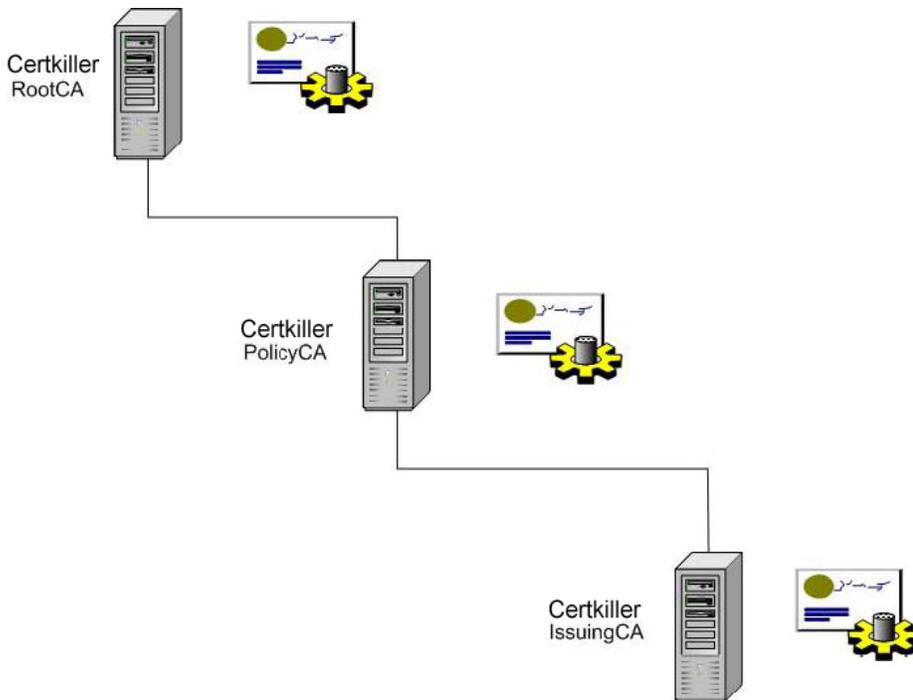
Have external customers request personal certificates from IssuingCA by using the Web enrollment pages hosted on IssuingCA.

QUESTION 186:

You are responsible for Public Key Infrastructure (PKI) management for your network at Certkiller Inc. The network consists of a Windows 2000 Active Directory domain. The network contains a Microsoft Internet Security and Acceleration (ISA) Server computer that accepts virtual private network (VPN) connections. The network also contains a Windows 2000 Server named Certkiller 1, which runs Internet Information Services (IIS). Certkiller 1 is accessible from the Internet.

The written security policy for Certkiller requires L2TP/IPSec connections.

To distribute the required certificates for L2TP connections, you deploy the Certification Authority (CA) hierarchy shown in the exhibit.



RootCA and PolicyCA use stand-alone CA policies and are removed from the network. IssuingCA issues the IPsec certificates. IPsec certificates are successfully issued to all remote client computers and the ISA Server.

The Certificate Revocation Lists (CRL) for RootCA, PolicyCA, and IssuingCA are published to Active Directory. The CRL Distribution Point (CDP) extensions are modified to reference the Active Directory location of all three CAs.

When remote client computers attempt to connect to the ISA Server, their connection attempts fail. At all remote client computers, this error message appears: "The client was unable to verify the identity of the server."

You must ensure that the remote client computers can connect to the ISA Server with an L2TP/IPsec VPN connection.

What should you do?

A. Modify the CDP extension on IssuingCA to include an HTTP URL that references Certkiller 1.

Manually publish the CRL to the referenced CDP URLs at Certkiller 1.

Renew the IssuingCA certificate.

B. Modify the CDP extension on RootCA, PolicyCA, and IssuingCA to include an HTTP URL that references Certkiller 1.

Manually publish the CRLs to the referenced CDP URLs at Certkiller 1.

Renew the RootCA, PolicyCA, and IssuingCA certificates.

C. Modify the CDP extension on IssuingCA to include an HTTP URL that references Certkiller 1.

Manually publish the CRL to the referenced CDP URLs at Certkiller 1.

Revoke all currently issued certificates.

Reissue the IPsec certificates to the ISA Server and the remote client computers.

D. Modify the CDP extensions on RootCA, PolicyCA, and IssuingCA to include an HTTP URL that references Certkiller 1.

Manually publish the CRLs to the referenced CDP URLs at Certkiller 1.
Revoke all currently issued certificates.
Reissue the IPSec certificates to the ISA Server and the remote client computers.

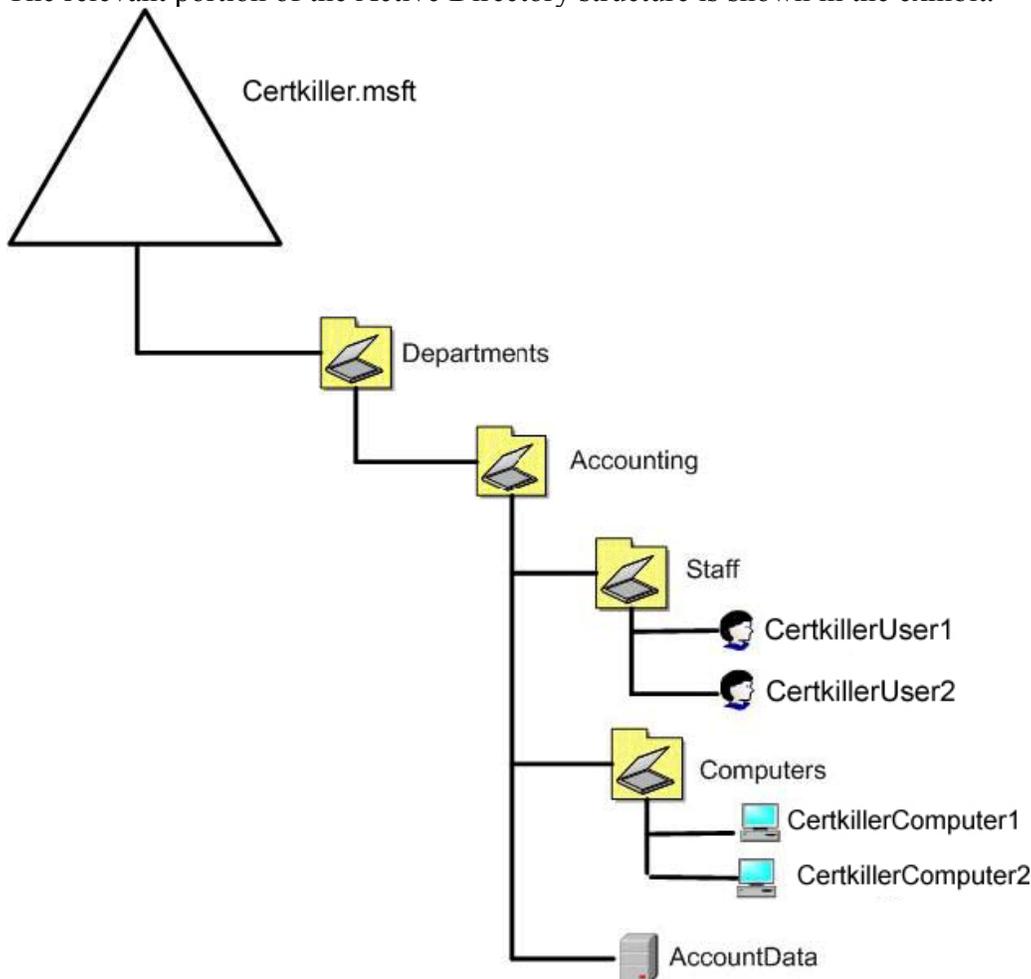
Answer: B

Explanation:

We need to modify the CDP extension on ALL CA's. Publish the CRL's and then renewing ALL the CA's. There is no need to revoke & reissue the certificates.

QUESTION 187:

You are a network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain named Certkiller .msft. The relevant portion of the Active Directory structure is shown in the exhibit.



The written security policy of Certkiller requires that all communication between the AccountData server and the computers in the accounting department be encrypted. To implement IPSec communication between AccountData and the accounting department client computers, you configure the network in the following way:

* All user accounts in the accounting department are members of the

Accounting_Department global group.

* All computer accounts in the accounting department are members of the Accounting_Department_Computers global group.

* The IPsec certificate template permissions are defined to grant the Accounting_Department global group Read and Enroll permissions.

* A Group Policy object (GPO) named GetCertificates is created and linked to the Accounting organizational unit (OU) to issue the IPsec certificate template by using the Automatic Certificate Request Settings option.

* A GPO named AccountingServer is created and linked to the Accounting OU.

The AccountingServer GPO assigns the Secure Server (Require Security) IPsec policy.

* A GPO named AccountingComputers is created and linked to the Computers OU.

The AccountingComputers GPO assigns the Client (Respond Only) IPsec policy.

The accounting department employees can connect to every computer on the network except AccountData. You must ensure that the employees in the accounting department can connect to AccountData under the written policy.

What should you do?

A. Change the AccountingServer GPO to assign the Secure Server (Request Security) IPsec policy.

B. Change permissions on the IPsec certificate template to grant Read and Enroll permissions to the Accounting_Department_Computers global group.

C. Change the AccountingComputers GPO to assign the Secure Server (Require Security) IPsec policy.

D. Unlink the GetCertificates GPO from the Accounting OU and link the GetCertificates GPO to the Computers OU.

Answer: D

Explanation:

IPsec should be applied to computers, not to users.

Incorrect Answers

A: This would weaken security. The written security policy requires that all communication with the server should be secure.

B: Read and Enroll permissions to security template do not apply.

C: Client (Respond Only) - This policy is for computers that do not require secure communications. If secure communications are requested, this policy instructs the computer to respond in a positive fashion. All communication between the client computers are not required to be encrypted. The client computers already have an appropriate IPsec policy.

QUESTION 188:

You are responsible for Public Key Infrastructure (PKI) management of the network for Certkiller. You have installed an offline root Certification Authority (CA) named RootCA and an offline intermediate CA named PolicyC

A. You must install an enterprise

subordinate CA named IssuingCA that is subordinate to PolicyCA.

Before installation of Certificate Services on IssuingCA, you synchronize the clock on IssuingCA with the clock on PolicyC

A. You now install Certificate Services on

IssuingCA, generate a certificate request, and submit the certificate request to PolicyCA.

After submitting the certificate request, you are unable to start Certificate Services on IssuingCA.

You must get Certificate Services started on IssuingCA.

What should you do? (Each correct answer presents part of the solution. Choose two)

A. Have a local administrator of RootCA issue the pending certificate request.

B. Have a local administrator of PolicyCA issue the pending certificate request.

C. Have a local administrator of IssuingCA issue the pending certificate request.

D. Install the issued certificate in the Certification Authority console and start Certificate Services.

E. Install the issued certificate in the Certificates snap-in and start Certificate Services.

Answer: B, D

Explanation:

B: As the PolicyCA is offline we must have a local administrator of PolicyCA issue the pending certificate request.

D: After the certificate for the child CA is issued, you can install the certificate for the child CA by using the Certification Authority console.

Reference:

Step-by-Step Guide to Administering Certificate Services,

<http://www.microsoft.com/windows2000/techinfo/planning/security/adminca.asp>

Incorrect Answers

A, C: The pending certificate request must be issued at the PolicyCA.

E: We should use the Certification Authority console, not the Certificates snap-in to install the issued certificate.

QUESTION 189:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional computers.

A Windows 2000 Member server named Certkiller 1 hosts the corporate intranet Web site.

Certkiller 1 runs Internet Information Services (IIS) 5.0. You have configured the Web server to require Basic authentication in combination with Secure Sockets Layer (SSL).

All users on the network use Internet Explorer as their default browser to connect to the intranet Web site.

Users report that they receive a dialog box prompting them for authentication credentials when they access the intranet Web site. You want to change the authentication method

uses to access the intranet Web site to ensure that users no longer receive that dialog box.

You also want to ensure that you can track users' access to the intranet Web site, based

on user name.

What should you do?

- A. Configure IIS to map exactly one client certificate to each user.
- B. Configure IIS on Certkiller 1 to enable the Accept client certificates option.
- C. Configure IIS on Certkiller 1 to enable the Enable client certificate mapping option.
- D. Configure the IIS authentication methods on Certkiller 1 to require Integrated Windows authentication only.
- E. Configure the IIS authentication methods on Certkiller 1 to require Digest authentication only.

Answer: D

Explanation:

Since the Web server is used only the corporate LAN we can safely use Integrated Windows authentication only. Users would never be prompted for login credentials when accessing the Web server. Tracking of the access would also be possible.

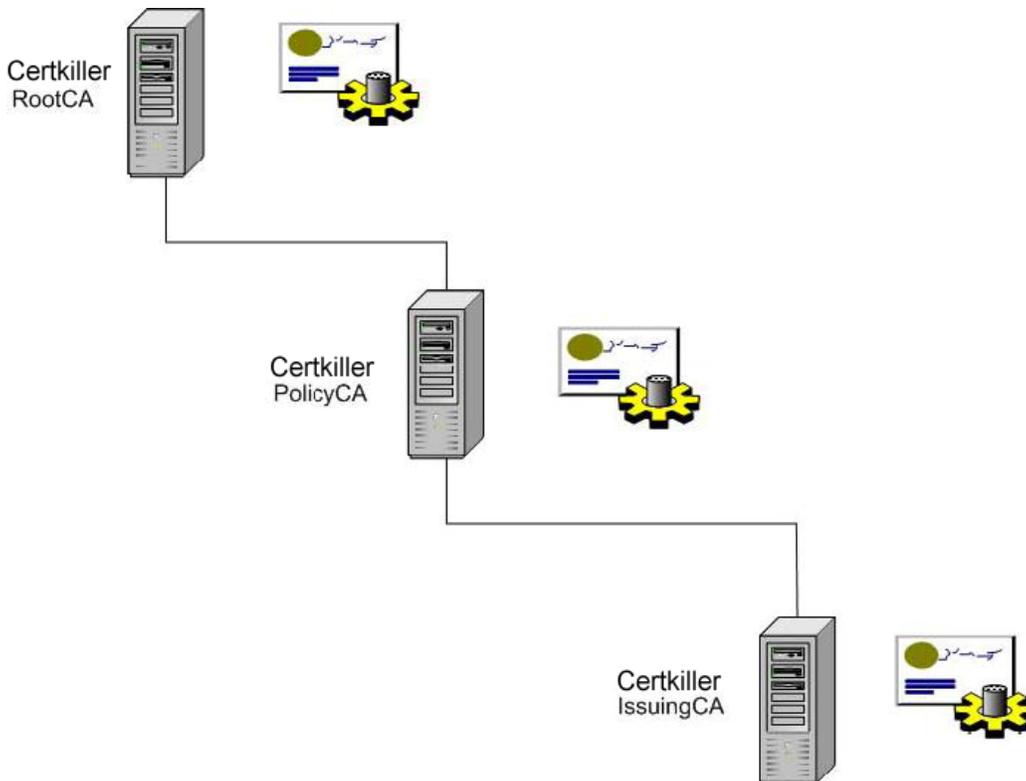
Incorrect Answers

A, B; C: If we want to be able to track users' access based on user name we should not use certificate authentication.

E: Digest Authentication requires the IIS server to have access to the Active Directory. However, since Certkiller 1 is a member server it does not access to the Active Directory.

QUESTION 190:

You are responsible for Public Key Infrastructure (PKI) management of the network for Certkiller . The network consists of a Windows 2000 Active Directory domain. You deploy the PKI hierarchy by using Windows 2000 Server computers as shown in the exhibit.



RootCA and PolicyCA are removed from the network. The following certificate lifetimes are implemented for the CAs in the CA hierarchy.

- * RootCA is a stand-alone-CA Certification Authority (CA) with a certificate lifetime of 20 years.
- * PolicyCA is a stand-alone CA with a certificate lifetime of 3 years.
- * IssuingCA is a stand-alone CA with a certificate lifetime of 6 years.

A new written security policy for Certkiller requires that an internal application use certificates with a five-year validity period.

What should you do to meet the written policy and prevent the re-usage of existing certificates?

- A. Renew the PolicyCA certificate by using the same key pair and specify a validity period of five years.
- B. Renew the PolicyCA certificate by using a new key pair and specify a validity period of five years.
- C. Renew the IssuingCA certificate by using the same key pair and specify a validity period of five years.
- D. Renew the IssuingCA certificate by using a new key pair and specify a validity period of five years.

Answer: D

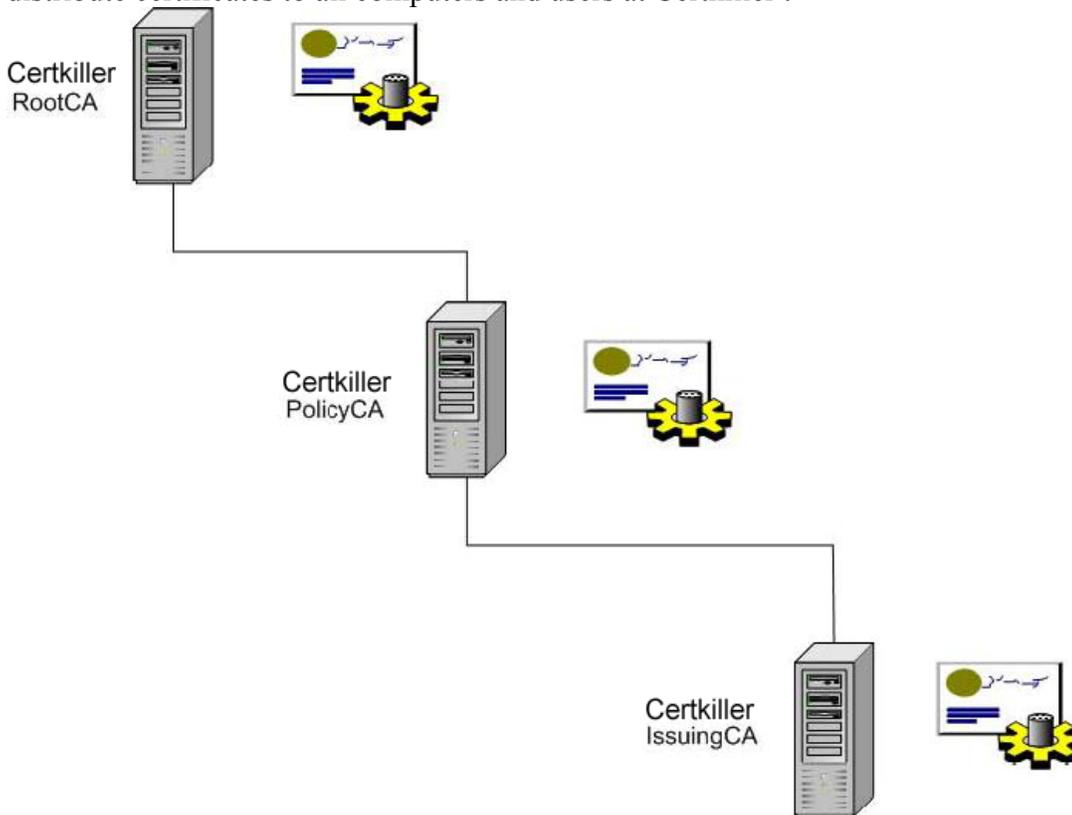
Explanation:

We should renew the IssuingCA certificate. We must use a new key pair to prevent the re-usage of existing certificates.

Note: Normally certificate lifetimes are nested. In other words, an issued certificate (of a users or a CA) expires before the certificate of the CA that issued it. Otherwise, after the CA's expiration, the issued certificate becomes invalid, even if it hasn't expired itself. Microsoft CAs enforce this nesting in their certificate issuing, but other CA products don't necessarily do that.

QUESTION 191:

You are the administrator of Certkiller 's network. The network consists of a Windows 2000 Active Directory domain. The domain contains a Windows 2000 Server computer that runs Internet Information Services (IIS) and hosts an extranet research Web site. You establish the Certification Authority (CA) hierarchy shown in the exhibit to distribute certificates to all computers and users at Certkiller .



RootCA and PolicyCA are removed from the network. IssuingCA issues all certificates to the users and computers in your network. IssuingCA publishes its Certificate Revocation List (CRL) every seven days. Certificates issued by IssuingCA are associated with user accounts in Active Directory by defining certificate mappings at the IIS server.

A user named Jack in the research department leaves Certkiller . You must ensure that she can no longer access the network or connect to the extranet research Web site by using her user certificate from IssuingCA.

What should you do?

- A. Delete the certificate mapping at the IIS server that hosts the Research Web site. Publish the latest version of the Root Certification Authority and Subordinate

Certification Authority certificates to the Authority Information Access (AIA) of IssuingCA.

B. Delete the certificate mapping at the IIS server that hosts the Research Web site.

Publish the latest version of the CRL to the CRL Distribution Points (CDPs) of IssuingCA.

C. Disable Jack's domain user account.

Revoke all certificates issued to Jack by IssuingCA in the Certification Authority console.

Publish the latest version of the Root Certification Authority and Subordinate Certification Authority certificates to the Authority Information Access (AIA) of IssuingCA.

D. Disable Jack's domain user account.

Revoke all certificates issued to Jack by IssuingCA in the Certification Authority console.

Publish the latest version of the CRL to the CRL Distribution Points (CDPs) of IssuingCA.

Answer: D

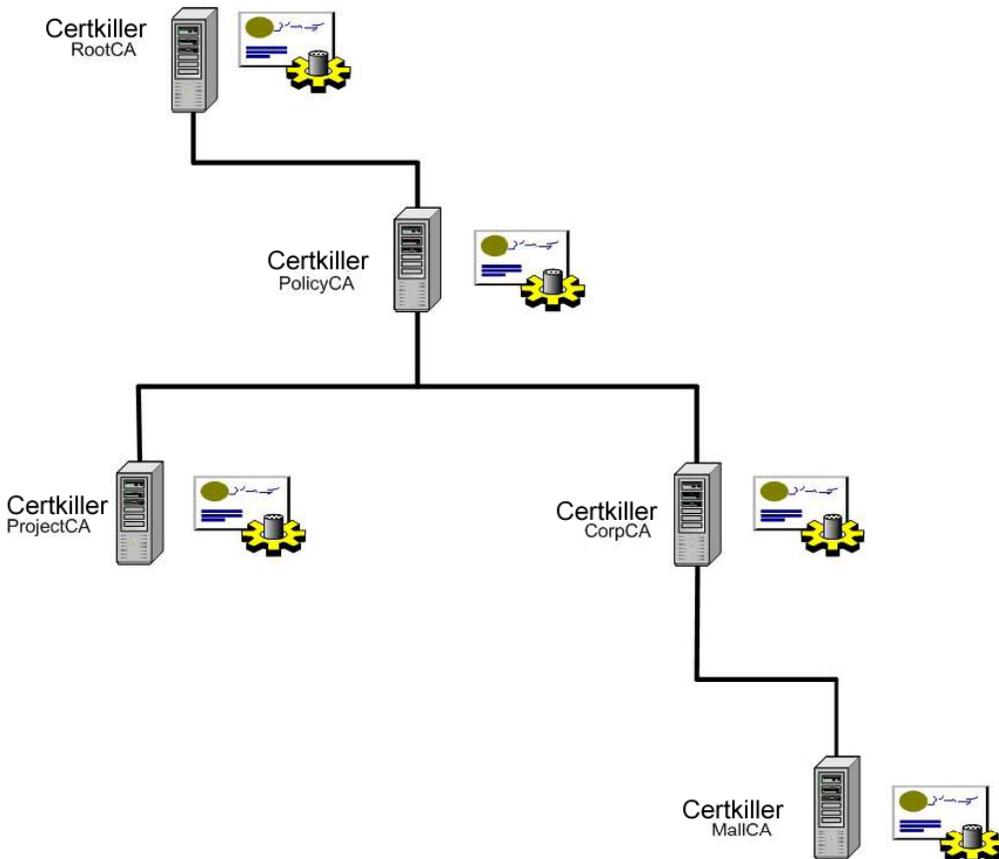
Explanation:

We should disable Jack's domain user account, revoke all certificates issued to Jack, and publish the latest CRL (Certification Revocation List).

QUESTION 192:

You are a network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain.

You deploy the Windows 2000 Certification Authority (CA) hierarchy shown in the exhibit.



RootCA and PolicyCA are removed from the network to increase the security of the CA hierarchy. CorpCA issues computer and user certificates for a company-wide applications, including Encrypting File System (EFS) and IPsec. MailCA issues certificates for Microsoft Exchange Server 2000.

ProjectCA issues certificates to users and computers involved in several Public Key Infrastructure (PKI) pilot projects. These certificates are issued with short lifetimes to ensure that the certificates are not used when a PKI project moves to a production application. Multiple projects utilize ProjectCA simultaneously.

At the conclusion of a pilot project, you discover that the pilot project users continue to use the certificates issued by ProjectCA, rather than the new certificates issued by CorpC

A. You need to ensure that certificates issued by ProjectCA are no longer used when a pilot project terminates.

What should you do when a project terminates?

- A. Revoke the CA certificate of ProjectCA at ProjectCA.
- B. Revoke the CA certificate of ProjectCA at PolicyCA.
- C. Revoke the individual certificates issued to the users and computers participating in the pilot project at ProjectCA.
- D. Export the certificates issued by ProjectCA for the pilot project and publish an updated Certificate Revocation List (CRL).

Answer: B

Explanation:

We only need to revoke the certificate for the ProjectC

A. All the certificates issued by

ProjectCA will be revoked automatically. We must revoke the certificate higher in the CA hierarchy, at PolicyCA.

QUESTION 193:

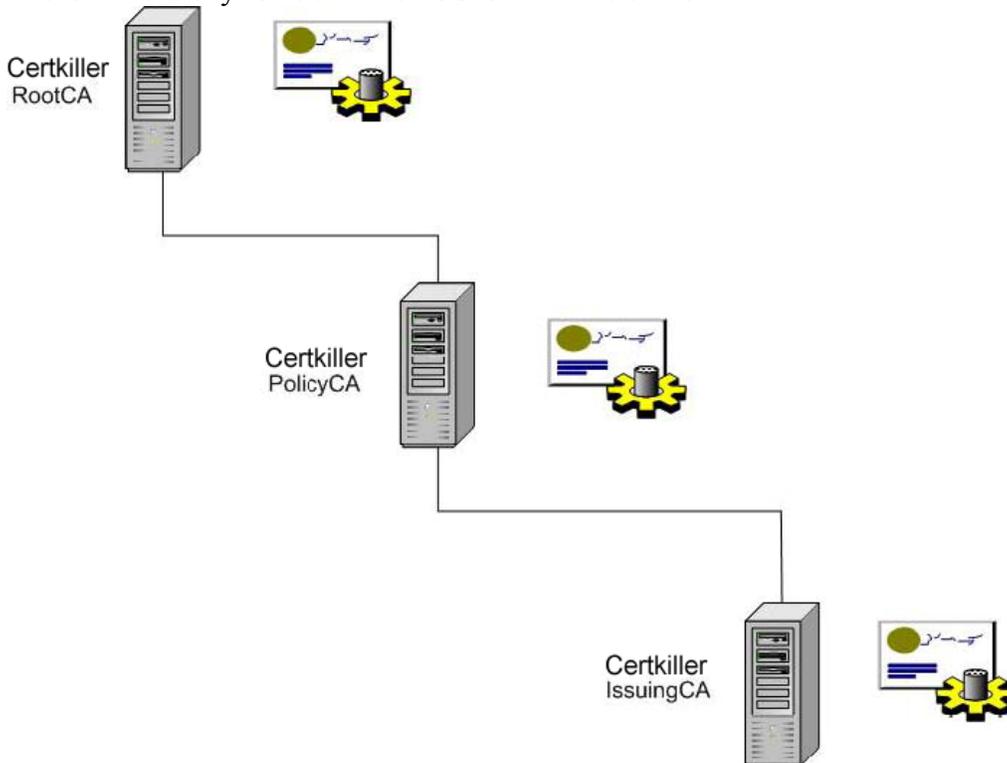
You are the network administrator for Certkiller . The network consists of three Windows 2000 Active Directory domains in a single Active Directory forest. Each domain represents a region in Certkiller . All client computers in the network run Windows XP Professional and are members of the domain for their region. Certkiller has a subsidiary named CertKiller. The CertKiller network consists of a Windows 2000 Active Directory domain that is not part of Certkiller 's Active Directory forest.

Employee in both companies must access a Windows 2000 Server computer named Certkiller 1, which runs Internet Information Services (IIS). Certkiller 1 is a member of the CertKiller domain and is physically located at the CertKiller's main office.

Certkiller 1 hosts a Web-based application that requires SSL encryption. Certkiller 1 contains a Web server certificate that was issued by a Certification Authority (CA) named IssuingC

A. IssuingCA is located on the CertKiller network.

The CA hierarchy for CertKiller is shown in the exhibit.



To allow validation of the Web server certificate, the network administrator for CertKiller publishes the Certificate Revocation List (CRL) and CA certificate for each CA in the CA hierarchy to an externally accessible Web location. When users

from Certkiller connects to Certkiller 1, a security alert appears that contains the following text: "The security certificate was issued by a company you have not chosen to trust."

You want to make sure that the users do not receive this error in the future. What should you do?

- A. Import the CA certificate for RootCA to the configuration naming context of Certkiller 's forest by running the certutil -dspublish command at a Windows XP computer.
- B. Import the CA certificate for IssuingCA to the configuration naming context of Certkiller 's forest by running the certutil -dspublish command for the certificate at a Windows XP computer.
- C. Import the CA certificates for IssuingCA to the Trusted Root Certification Authorities policy of the Default Domain Policy Group Policy object (GPO) in the forest root domain.
- D. Import the CA certificate for RootCA to the Trusted Root Certification Authorities policy of the Default Domain Policy Group Policy object (GPO) in the forest root domain.

Answer: D

Explanation:

We import a root certificate into a GPO and deploy the whole domain forest.

Incorrect Answers

A, B: We should use a GPO to issue the certificate throughout the domain. This cannot be achieved by importing the certificate on a single Windows XP Professional computer.

C: We must import the certificate for the RootCA, not the IssuingCA.

QUESTION 194:

You are the network administrator of Certkiller 's network. The network consists of a Windows 2000 Active Directory domain. All client computers run Windows 2000 Professional and are domain members.

The consulting manager wants to implement Encrypting File System (EFS) on the C:\Projects folder on each consultant's portable computer. The IT manager wants to disable EFS for all other computers in Certkiller . You must ensure that both of these objectives are met.

What should you do?

- A. In the Default Domain Controllers Policy, delete the EFS Recovery policy. Create an organizational unit (OU) named Consultants that contains all of the consultants' user accounts. Create a Group Policy object (GPO) and link it to the Consultants OU. Configure the GPO to implement an EFS Recover Agent.
- B. In the Default Domain Controllers Policy, implement an empty EFS Recovery policy. Create an organizational unit (OU) named Consultants that contains all of the consultants'

portable computer accounts.

Create a Group Policy object (GPO) and link it to the Consultants OU.

Configure the GPO to implement an EFS Recover Agent.

C. In the Default Domain Policy, delete the EFS Recover policy.

Create an organizational unit (OU) named Consultants that contains all of the consultants' user accounts.

Create a Group Policy object (GPO) and link it to the Consultants OU.

Configure the GPO to implement an EFS Recover Agent.

D. In the Default Domain Policy, implement an empty EFS Recover policy.

Create an organizational unit (OU) named Consultants that contains all of the consultants' portable computer accounts.

Create a Group Policy object (GPO) and link it to the Consultants OU.

Configure the GPO to implement an EFS Recover Agent.

Answer: D

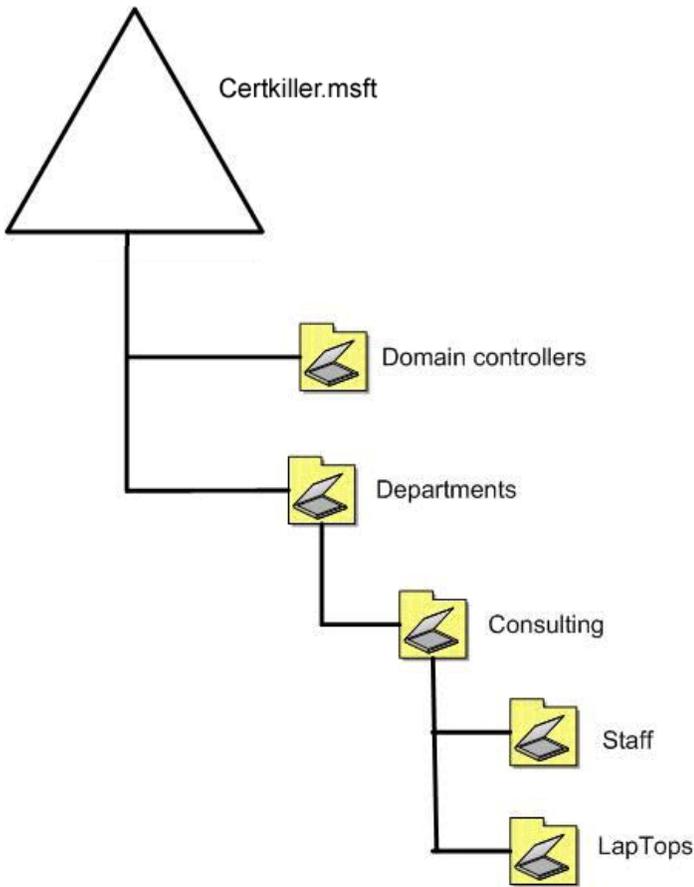
Explanation:

By implementing an empty EFS Recover policy and creating an organizational unit (OU) named Consultants that contains all of the consultants' portable computer accounts, we can implement Encrypting File System (EFS) on the C:\Projects folder on each consultant's portable computer and at the same time, disable EFS for all other computers in Certkiller .

QUESTION 195:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain named Certkiller .msft. The network includes Windows 2000 Professional client computers. All consultants' portable computers run Windows 2000 Professional.

The relevant portion of the Active Directory structure is shown in the exhibit.



Within the organizational unit (OU) structure, the consulting department user objects are located in the Staff OU. The consultants' portable computer objects are located in the Laptops OU.

Certkiller's written security policy requires that Encrypting File System (EFS) be enabled for the consultants. The written policy requires that EFS encryption be disabled for any other employees of Certkiller.

You must ensure that the written policy is enforced.

What should you do?

- A. Create a Group Policy object (GPO) and link it to the Staff OU. Configure the GPO to define an EFS Recovery Agent. Define an empty EFS Recovery Agent policy in the Default Domain Policy at the domain.
- B. Create a Group Policy object (GPO) and link it to the Laptops OU. Configure the GPO to define an EFS Recovery Agent. Define an empty EFS Recovery Agent policy in the Default Domain Policy at the domain.
- C. Create a Group Policy object (GPO) and link it to the Staff OU. Configure the GPO to define an EFS Recovery Agent. Define an empty EFS Recover Agent policy in the Default Domain Controllers Policy at the Domain Controllers OU.
- D. Create a Group Policy object (GPO) and link it to the Laptops OU.

Configure the GPO to define an EFS Recovery Agent.
Define an empty EFS Recovery Agent policy in the Default Domain Controllers Policy at the Domain Controllers OU.

Answer: B

Explanation:

We define an EFS Recovery agent in a GPO. We link the GPO to the Laptops OU. This ensures that EFS will be enabled for the consultants computers.

An empty EFS Recovery Agent policy for the Default Domain Policy ensures that EFS is not used for the rest of the users.

Incorrect Answers

A: EFS applies to computers, not to users. We should link the EFS GPO to the Laptops OU, not the Staff OU.

C: EFS applies to computers, not to users. Furthermore, we should apply the GPO with the empty EFS Recovery Agent policy to the whole domain, not only to the domain controllers.

D: We should apply the GPO with the empty EFS Recovery Agent policy to the whole domain, not only to the domain controllers.

QUESTION 196:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers. The network also contains Macintosh client computers.

You want to deploy an intranet Web site for employees of a new international branch office. You will hire the employees for the new branch office over the next few months. The new branch will include both Windows 2000 Professional and Macintosh client computers.

You install the intranet Web site on a Windows 2000 member server named Certkiller 1. The server runs Internet Information Services (IIS) 5.0. You configure IIS to use Digest authentication when users connect to the intranet Web site.

You want to ensure that the new users in the branch office will be able to use Digest authentication to successfully connect to the intranet Web site.

What should you do?

A. Use the Internet Information Services console to install a server certificate on the intranet Web site.

B. Run the dcpromo command to promote Certkiller 1 to domain controller.

C. When you create the new user accounts, place them in a new group named BranchUsers.

Grant BranchUsers the Log on locally user right on Certkiller 1.

D. Create a Group Policy object (GPO) and link it to the domain.

Configure the GPO to enable the Store password using reversible encryption for all users in the domain option.

Answer: D

Explanation:

We need to store the passwords using reversible encryption for all users in order to enable the Macintosh client computer to use Digest authentication.

Note: Store password using reversible encryption for all users in the domain weakens, rather than strengthens, passwords. If you enable this policy, then user passwords are stored in clear text in Active Directory (AD), and anybody can read them. This policy exists to support applications that require Knowledge of the user password; the most common example is the AppleTalk protocol. Unless your domain consists entirely of Macintosh computers, this policy is dangerous to set across the domain. Instead, apply this policy on a user-by-user basis by opening the appropriate user account object in Active Directory Users and Computers. By enabling this policy in each user's Account tab, the setting will affect only specified users instead of the entire domain.

Reference:

Setting Up Digest Authentication for Use with Internet Information Services 5.0,
Microsoft Knowledge Base Article - Q222028

Incorrect Answers

A: A server certificate is not required for digest authentication.

B: As we were able to configure the IIS server to use Digest Authentication it has already access to the Active Directory.

Note: In order to use Digest Authentication in Windows 2000, the server must have access to an Active Directory Server that is set up for Digest Authentication. If the server running IIS is not a Active Directory Server, or does not have access to the Active Directory, this authentication will not work.

C: This has no effect in this scenario.

QUESTION 197:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

Certkiller uses a Windows 2000 member server named Certkiller 1 as a file server for users on the network.

A user named Jack is Certkiller auditor.

You want to allow Jack to assign audit access control entries on files and folders on Certkiller 1. You do not want Jack to have excessive privileges on Certkiller 1.

What should you do?

A. Add the Jack user account to the Power Users group on Certkiller 1.

B. Assign the Jack user account Allow - Full Control permission on all files and folders on Certkiller 1.

C. Grant the Jack user account the Manage auditing and security log user right on Certkiller 1.

D. Grant the Jack user account the Generate security audits user right on Certkiller 1.

Answer: A

Explanation:

Power Users can enable auditing on a particular file and folders.

Note: Power Users can:

1. Run legacy applications in addition to Windows 2000 certified applications.
2. Install programs that do not modify operating system files or install system services.
3. Customize system-wide resources including Printers, Date/Time, Power Options, and other Control Panel resources.
4. Create and manage local user accounts and groups.
5. Stop and start system services which are not started by default.

Reference:

HOW TO: Enable and Apply Security Auditing in Windows 2000, Microsoft Knowledge Base Article - Q300549

Incorrect Answers

B: Jack is not required to get Full Control permission.

C: By default, only members of the Administrators group have privileges to configure auditing. You can delegate the task of configuring auditing of server events to another user account by granting the Manage Auditing and Security Log right in Group Policy. However, in this scenario Jack does not need these rights. She only need the right to enable auditing on a particular file or folder.

D: The Generate security audits right allows writing of events to the security logs.

QUESTION 198:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain includes five Windows 2000 domain controllers and five Windows 2000 Server computers configured as file servers. The domain also includes 750 Windows 2000 Professional computers.

User account policies are set to their default values on the domain. The Account logon event policy is configured for failure auditing on the domain controllers and file servers. While reviewing the audit logs, you notice more than 100 Event ID 529 (failed logon event) and Event ID 681 (failed account logon event) entries in the Security log that contains the same three user accounts. The users who use these accounts work on Windows 2000 Professional client computers. These users report that they have no difficulty logging on to the network. You verify this statement by asking the users to log off and log on in your presence.

You need to reduce the chance that the attacks shown in the event log will succeed. What should you do?

- A. Run the syskey command and set it to Password Startup on all domain controllers.
- B. Run the syskey command and set it to Password Startup on all client computers in your domain.
- C. Set the Account lockout threshold policy to 3 and accept the suggested settings for the other account lockout values.

D. Set the Account lockout threshold policy to 0 and accept the suggested settings for other account lockout values.

Answer: C

Explanation:

The Account lockout threshold policy specifies the number of tries that a user (or intruder) gets to enter in an incorrect password before the account becomes locked out for the above specified time. A strong setting would be 3 attempts.

Incorrect Answers

A, B: Use the Windows 2000 System Key (SysKey) to protect EFS private keys. SysKey uses strong encryption techniques to increase the protection of users' protected stores, including users' private keys for EFS. (Ref: Windows 2000 Server Resource Kit).

However, this does not address the problem in this scenario.

D: An Account lockout threshold policy with a 0 setting would allow the password to be guessed at indefinitely

QUESTION 199:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

The finance department uses a Windows 2000 member server named Certkiller 1 to store confidential files. The files are in a folder named Budget, which is shared as Budget. All users in the finance department are members of a group named Finance.

The NTFS permissions on the Budget folder and the files in that folder allow access only to the Administrators group and the Finance group. The NTFS permissions are configured to allow full control. The share permissions are the default permissions.

You want to track which users attempt to gain access to files in the Budget folder on Certkiller 1. You configure auditing on the Budget folder and all files in that folder. In the auditing entries, you enable Failed access on each access type for the Everyone group. You test the auditing configuration by attempting to access the files in the Budget folder with a domain user account that does not have permissions to the file. You receive an "Access Denied" error message.

However, this failed attempt does not appear in the Security Event Log on Certkiller 1. How should you correct this problem?

- A. Configure the auditing entries to apply to the Administrators group and the Finance group, instead of the Everyone group.
- B. Configure the auditing entries to include both failed and successful access for all access types.
- C. Enable the Audit object access option for failed attempts in a new Group Policy object (GPO) that applies only to Certkiller 1.
- D. Grant the Certkiller 1 computer account the Generate security audits right.
- E. Add NTFS permission access control entries to the Budget folder and all files in the folder that specify Deny - Full Control permission for the Everyone group.

Answer: C

Explanation:

We must enable Audit object access. Determines whether to audit the event of a user accessing an object (for example, file, folder, registry key, printer, and so forth) which has its own system access control list (SACL) specified.

By default, this value is set to No auditing in the Default Domain Controller Group Policy object (GPO) and in the local policies of workstations and servers.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not to audit the event type at all. Success audits generate an audit entry when a user successfully accesses an object that has a SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified. You can select No auditing by defining the policy setting and unchecking Success and Failure.

Incorrect Answers

A: The auditing entries correctly applies to the Everyone group. There is no need to change this configuration,

B: We do not need to audit successful access.

D: The Generate security audits right lets users or processes create Security log entries. Software developers use this right to give their programs the ability to generate log entries for certain actions. Typically, software that requires this right will either grant it automatically during installation or instruct you to grant it to the software's service account.

E: There is no need to change the NTFS permission to enable auditing.

QUESTION 200:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains three member servers that run Windows 2000 Server. All three servers use Routing and Remote Access to accept dial-up connections from remote Certkiller employees. You will soon add four more dial-up servers to handle the demand for dial-up services.

The written security policy for Certkiller requires the start and end time of all dial up connections to be logged. The logs must be maintained for at least six months.

You need to configure the existing dial-up servers to comply with the written policy. You need to ensure that the configuration can support additional dial-up servers. You also want to minimize the amount of time you spend maintaining dial-up logs.

What should you do?

A. Enable auditing on each dial-up server.

Configure the Security log on each dial-up server to be 20 MB in size and to never overwrite events.

Save each Security log to an archived location every day.

B. Use the Eventcomb utility to collect the security events from each dial-up server every day.

Export the Security log from each dial-up server to a file every day.
C. Install Internet Authentication Service (IAS) on a new Windows 2000 Server computer.
Configure each dial-up server to use IAS for authentication and accounting.
Configure IAS to log authentication and accounting.
Use Task Scheduler to archive the IAS log files every day.
D. Move the dial-up servers to a new organizational unit (OU).
Create a Group Policy object (GPO) and link the GPO to the new OU.
Configure the GPO to enable auditing for logon and logoff events.

Answer: C

Explanation:

We should centralize the authentication with an IAS server. Only a single log need to be maintained and checked. Furthermore, it is very easy to install and configure further RRAS servers to use the IAS server.

Incorrect Answers

A: The questions stated : "minimize the amount if time you spend maintaining dial-up logs". Manually saving a log file every day takes to much time.

B: This is the next best solution.

D: The questions stated : " The logs must be maintained for at least six months". Default eventlog settings will not allow six months of logging.

QUESTION 201:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains a Windows 2000 Server computers and Windows 2000 Professional client computers.

Certkiller uses a Windows 2000 member server named Certkiller 1 as a file server. You configure Certkiller 1 to log all events of users making a network connection to Certkiller 1. You regularly check the event log entries on Certkiller 1 remotely from another computer in the domain.

On morning, you notice that the Security event log on Certkiller 1 does not contain any new log events for users making a network connection for the last two days. You verify that users have connected to Certkiller 1 during the last two days. You also verify that the Audit logon events policy for successful events is enabled for Certkiller 1.

You want to ensure that Certkiller 1 resumes logging the network connection events.

What should you do?

- A. Increase the maximum size of the security log for Certkiller 1.
- B. Enable the Audit object access policy for Certkiller 1.
- C. Grant Certkiller 1 the Generate security auditsright.
- D. On Certkiller 1, change the CrashOnAuditFail registry value to 1.

Answer: A

Explanation:

The security log is full. We could

1. Set the Event Log Wrapping for "Overwrite Events as Needed." (not listed)
2. Decrease the amount of information being audited.
3. Increase the log file size and use a combination of the previous options listed above.
4. Disable auditing (not an option here since we must audit this event).

Incorrect Answers

B: Auditing worked successfully. We do not need to reconfigure the Audit policy.

C: Auditing worked successfully. We do not need to grant Certkiller 1 further rights.

D: Changing the CrashOnAuditFail registry value to 1 would make Certkiller 1 crash when the security logs fills up. It improves security, but would not meet the requirements of this scenario.

QUESTION 202:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers.

Several of the Windows 2000 Server computers are deployed as file servers. Those file servers contain home folders for users on the network. Only users have permissions to access the files in their home folder.

You have delegated administration of the file servers to five assistant administrators. The assistant administrators are members of the local Administrators group on each of the file servers and do not have administrative privileges on the domain.

The written security policy for Certkiller specifies that administrators are not allowed to read the content of the files in user's home folders. You want to track whether the assistant administrators comply with the written policy.

You configure the Eventcomb utility to collect the security events for exercising a user right on the file servers and scan for the use of the "Take ownership of files and other objects" user right and the "Backup files and directories user" right.

You want to ensure that when these events occur, they are logged in the event logs on the file servers.

What should you do? (Each correct answer presents part of the solution. Choose two)

- A. Enable the Audit privilege use policy for the file servers.
- B. Enable the Audit system events policy for the file servers.
- C. Enable the Audit the access of global system objects security option for the file servers.
- D. Enable the Audit use of Backup and Restore privilege security option for the file servers.
- E. Grant the file server computer accounts the Generate security audits right.
- F. Grant the file server computer accounts the Profile system performance right.

Answer: A, D

Explanation:

A: Privileges indicate rights assigned to Administrators or other power users. Tracks all user rights except Bypass Traverse Checking, Debug Programs, Create a Token Object, Replace Process Level Token, Generate Security Audits, Back Up Files and Directories, and Restore Files and Directories.

Tracks all user rights except Bypass Traverse Checking, Debug Programs, Create a Token Object, Replace Process Level Token, Generate Security Audits, Back Up Files and Directories, and Restore Files and Directories.

Note: The Audit use of all user rights including Backup and Restore setting under Security Options will audit those user rights excluded here.

D: When you set this option, the exercise of Backup and Restore will be logged.

Incorrect Answers

B: System events includes a user restarted or shut down the computer, or an event occurred that affects Windows 2000 security or the security log

C: Global system objects include internal objects. Auditing these objects are interesting for driver and system-level programmers, but not useful in this scenario.

E: The LocalSystem account already has the Generate Security Audits right.

F: The Profile system performance determines which users can use performance monitoring tools to monitor the performance of system processes.

QUESTION 203:

You are the administrator of Certkiller 's Web server named Certkiller 1. Certkiller 1 runs Windows 2000 Server and Internet Information Services (IIS). Certkiller 1 provides services to Internet users and is connected directly to the Internet.

During the afternoon, Certkiller 1 stops responding to request from Internet users. You restart the server, and it appears to work normally. Three hours later, the server again stops responding to requests from Internet users. You run the netstat.exe command and discover thousands of TCP connections in half-open state.

The Web services running on Certkiller 1 will function correctly only if Certkiller 1 is connected directly to the Internet. You need to make Certkiller 1 more resistant to this type of attack.

What should you do?

- A. Configure an IIS bandwidth throttle of 512 Kbps.
- B. Increase the amount of memory installed in Certkiller 1.
- C. Configure Certkiller 1 to accept connections only on port 80.
- D. Modify the server's registry to decrease the SYN_ACK timeout.

Answer: D

Explanation:

Decreasing the SYN_ACK timeout would improve the situation. TCP connections would be active for a smaller amount of time.

Note: TCP Spoofed Connection Request (SYN): Uses the first two steps of the three-way handshake. The scanning system sends a packet with the reset (RST) flag for the last step instead of a status acknowledge (ACK) thereby not establishing a complete connection.

TCP connect scan. Less likely to be detected or filtered by security devices since connection is never established. Somewhat slower than a TCP connect scan
Time-out tolerance. To protect the Web site and other extranet resources from a denial of service attack, the firewall should support time-outs for disconnected sessions. This feature prevents SYN flooding attacks against the network.

Reference:

Microsoft Security Operations Guide for Windows 2000 Server, p.21

QUESTION 204:

You are the administrator of Certkiller 's Web server. This server runs Windows 2000 Advanced Server and Internet Information Services (IIS). The server contains static Web pages and is connected directly to the Internet.

During the week, the server stops responding 15 times, and users cannot access its Web pages. Each time the problem occurs, you restart the server and restore it to service. You examine the IIS log files and discover that the server has been the target of a denial-of-service (DoS) attack.

You need to make your Web site more resistant to DoS attacks against IIS.

What should you do?

- A. Modify the server's registry to increase the SYN_ACK timeout.
- B. Configure IP port filtering on the server so that only ports 80 and 443 are accepted by the server's network adapter.
- C. Configure the server's recover options so that the server automatically restarts after encountering a STOP error.
- D. Install an additional Web server that is running Windows 2000.
Configure the new server to host the same Web pages as the original server.
Configure Network Load Balancing (NLB) between the two Web servers.

Answer: A

Explanation:

TCP Spoofed Connection Request (SYN): Uses the first two steps of the three-way handshake.

The scanning system sends a packet with the reset (RST) flag for the last step instead of a status acknowledge

(ACK) thereby not establishing a complete connection. TCP connect scan. Less likely to be detected or filtered by security devices since connection is never established.

Somewhat slower than a TCP connect scan.

Time-out tolerance. To protect the Web site and other extranet resources from a denial of service attack, the firewall should support time-outs for disconnected sessions. This feature prevents SYN flooding attacks against the network. (MS Press - Designing Microsoft Windows 2000 Network Security Training Kit ebook, Chapter 14, Lesson 1)

Reference:

Microsoft Security Operations Guide for Windows 2000 Server, p.21

QUESTION 205:

You are the administrator of Certkiller 's Web server. This server runs Windows 2000 Server and Internet Information Services (IIS): IIS is installed with the default settings and included all optional components. The server is used only as a Web server. During the week, the server stops responding several times, and users cannot access its Web pages. You examine the server's IIS log files and discover that the SMTP and Network News Transfer Protocol (NNTP) services have received more than 300,000 connection requests and none were completed or properly closed. You suspect that the services have been targets of a denial-of-service (DoS) attack. You need to make the server more resistant to DoS attacks. What should you do?

- A. Uninstall the SMTP, NNTP, and FTP services.
- B. Modify the registry to increase the SYN_ACK timeout.
- C. Configure a bandwidth throttle of 1.024 Kbps on the server's default Web site.
- D. Install URLScan on the server.

Answer: D

Explanation:

Urlscan is a powerful security tool that works in conjunction with the IIS Lockdown Tool to give IIS Web site administrators the ability to turn off unneeded features and restrict the kind of HTTP requests that the server will process. By blocking specific HTTP requests, the Urlscan security tool prevents potentially harmful requests from reaching the server and causing damage. Urlscan screens all incoming requests to the server and filters them based on rules set by the administrator. This secures the server by ensuring that only valid requests are processed. Urlscan is effective in protecting Web servers because most malicious attacks share a common characteristic - they involve the use of a request that's unusual in some way. For instance, the request might be extremely long, request an unusual action, be encoded using an alternate character set, or include character sequences that are rarely seen in legitimate requests. By filtering out all unusual requests, Urlscan prevents them from reaching the server and potentially causing damage.

Note: Denial of Service (DoS) attacks involve tying up the resources of a system sufficiently to prevent it from performing its normal function. The following defensive steps will help you prevent these types of attacks:

1. Keep systems updated with the latest security patches.
2. Block Large ping packets at the router and firewall, stopping them from reaching the perimeter network.
3. Apply anti-spoof filters on the router; that is, block any incoming packet that has a source address equal to an address on the internal network.
4. Filters the ICMP messages on the firewall and router (although this could affect some management tools).
5. Develop a defense plan with your internetservice provider (ISP) that enables a rapid response to an attack that targets the bandwidth between your ISP and

your perimeter network.

6. Disable the response to directed broadcasts.
7. Apply proper router and firewall filtering.
8. Use an IDS system to check for unusual traffic and generate an alert if it detects any. Configure IDS to generate an alert if it detects ICMP_ECHOREPLY without associated ICMP_ECHO packets. (Microsoft Security Operations Guide for Windows 2000 Server p.24)

Reference:

- Q309394: HOW TO: Use URLScan with FrontPage 2000
- Q309508: IIS Lockdown and URLscan Configurations in Exchange Environment
- Q309677: XADM: Known Issues and Fine Tuning When You Use the IIS Lockdown Wizard in an Exchange 2000 Environment
- Q311595: XCCC: How to Install and Configure Microsoft Security Tool Kit On a Microsoft Mobile Information Server
- Q312376: HOW TO: Configure URLScan to Allow Requests with a Null Extension in IIS
- Q313131: HOW TO: Use URLScan with Exchange Outlook Web Access in Exchange Server 5.5
- Q311862: How to Use The IIS Lockdown Tool with Small Business Server
- Q311350: HOW TO: Create a Custom Server Type for Use with the IIS Lockdown Wizard

Incorrect Answers

A: It is not necessary to uninstall these services.

B: Increasing the SYN_ACK timeout would not improve the situation. Decreasing, not increasing, this value helps for SYN-ACK attacks, but are not so effective for DoS attacks.

Note: TCP Spoofed Connection Request (SYN): Uses the first two steps of the three-way handshake. The scanning system sends a packet with the reset (RST) flag for the last step instead of a status acknowledge (ACK) thereby not establishing a complete connection. TCP connect scan. Less likely to be detected or filtered by security devices since connection is never established. Somewhat slower than a TCP connect scan. (Reference: Microsoft Security Operations Guide for Windows 2000 Server, p.21)

Time-out tolerance. To protect the Web site and other extranet resources from a denial of service attack, the firewall should support time-outs for disconnected sessions. This feature prevents SYN flooding attacks against the network. (MS Press - Designing Microsoft Windows 2000 Network Security Training Kit ebook, Chapter 14, Lesson 1)

C: Bandwidth configuration would not make the server more resistant to DoS attacks.

QUESTION 206:

You are the network administrator for Certkiller . The network consists of a native mode Windows 2000 Active Directory domain. All client computers run Windows 2000 Professional or Windows NT Workstation 4.0. All Windows NT Workstation 4.0 client computers have the Microsoft Directory Services client installed. The written security policy for Certkiller requires all communications between computers in the network to be encrypted where possible.

You install Certificate Services on a Windows 2000 Server computer and configure the server to act as an enterprise root Certification Authority (CA) for the domain. You configure the CA to issue IPSec certificates. You configure the Default Domain Policy Group Policy object (GPO) to issue IPSec certificates to all member computers automatically.

You create two new organizational units (OUs) in the domain: Desktops and Servers. The Desktops OU contains the computer accounts for all client computers. The Servers OU contains the computer accounts for all server computers. In each OU, you create and configure a GPO to apply IPSec policies to the computers as shown in the following table.

OU	GPO name	IPSec policy assigned
Domain controllers	Security-DC	Secure Server (Require Security)
Servers	Security-SRV	Secure Server (Require Security)
Desktops	Security-DTop	Client (Respond only)

You also configure the IPSec policies to use only IPSec certificates issued by the root CA for authentication.

Users with computers running Windows NT Workstation 4.0 report that they cannot access resources located on any network server. However, these users access resources located on other client computers. Users with computers running Windows 2000 Professional do not report similar problems.

You need to ensure that all client computers can access server-based resources.

What should you do?

- A. Configure all IPSec policies in all OUs to use Kerberos as the authentication protocol.
- B. Configure the Secure Server (Require Security) IPSec policy to use a preshared key for key exchange.
- C. Assign the Server (Request Security) IPSec policy in the Security-DC GPO and the Security-SRV GPO.
- D. Use the Web-based Certificate Enrollment tool to request and install computer certificates on the Windows NT Workstation 4.0 computers.

Answer: C

Explanation:

Server (Request Security) - This policy is for computers that require secure communications. These computers will accept unsecured traffic, but they will always attempt to secure subsequent communications by requesting security from the sending computer. If the sending computer does not respond positively, all communications are sent without using IPSec. In our scenario the windows 2000 workstations will be using IPsec and our Windows NT4 machines will not use IPsec but NTLMv2 for instance.

Incorrect Answers

A: Since we have Windows NT4 clients in our network, we are not able to use the Kerberos authentication protocol. We have Directory Services client installed on the Windows NT4 machines but the maximum security we can have is NTLMv2 authentication protocol.

B: Secure Server (Require Security) - This policy will require computers to use IPsec and secure their communications. Computers assigned to this policy will always reject unsecured communications, and outgoing traffic will always be secured. Since our Windows NT4 machine can NOT use IPsec we can not use this setting.

D: There is no such thing as Web-based Certificate Enrollment tool. Only a Certificate Enrollment ActiveX Control that can be used on the windows NT4 workstations. however this will be alot of work.

QUESTION 207:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain include three Windows 2000 Advanced Server computers configured as domain controllers and Windows 2000 Professional client computers. The network also include Windows 98 client computers.

The three domain controllers are the only computers on the network that are running Windows 2000 Advanced Server. All Windows 2000 computers are configured to use all available authentication methods. All domain computer accounts are located in an organizational unit (OU) named Clients.

You must ensure that all Windows 98 client computers implement only the most secure authentication method available to them.

What should you do? (Each correct answer presents part of the solution. Choose two)

- A. Install the Microsoft Directory Services Client on the Windows 98 client computers.
- B. Install the Windows 98 Dial-up Networking Security Upgrade on the Windows 98 client computers.
- C. Create a new Group Policy object (GPO) and link it to the Clients OU. Set the LAN Manager Authentication Level policy to Send NTLMv2 response only/refuse LM.
- D. Create a new Group Policy object (GPO) and link it to the Clients OU. Set the LAN Manager Authentication Level policy to Send NTLMv2 response only.
- E. On each Windows 98 client computer, create an LSA registry subkey subordinate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control. Create an LMCompatibilityLevel value and set the value to 3.

Answer: A, E

Explanation:

NTLM 2 is the most secure LAN Manager authentication level. NTLM2 support to Windows 95 and Windows 98 can be added by installing the Directory Services Client from the Windows 2000 CD-ROM. We also need to activate NTLM on the clients by reconfiguration of the Registry (see below). By enforcing use of NTLMv2 we would

ensure that the most secure authentication method is available.

Procedure to activate NTLM 2 on the client:

1. Start Registry Editor (Regedit.exe).

2. Locate and click the following key in the registry:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control

3. Create an LSA registry key in the registry key listed above.

4. On the Edit menu, click Add Value, and then add the following registry value:

Value Name: LMCompatibility

Data Type: REG_DWORD

Value: 3

Valid Range: 0,3

Description: This parameter specifies the mode of authentication and session security to be used for network logons. It does not affect interactive logons.

o Level 0- Send LM and NTLM response; never use NTLM 2 session security. Clients will use LM and NTML authentication, and never use NTML 2 session security; domain controllers accept LM, NTLM, and NTLM 2 authentication.

o Level 3 - Send NTLM 2 response only. Clients will use NTLM 2 authentication and use NTML 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication.

NOTE: To enable NTLM 2 for Windows 95 Clients, install Distributed File System (DFS) Client, WinSock 2.0 Update, and Microsoft DUN 1.3 for Windows 2000.

5. Quit Registry Editor.

Note: The LAN Manager authentication level determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers. The NTLM authentication package in Windows 2000 supports three methods of challenge/response authentication: LAN Manager (LM) which is least secure, NTLM version 1, NTLM version 2 which is the most secure.

By default, all three challenge/response mechanisms are enabled. You can disable authentication using weaker variants by setting the LAN Manager authentication level security option in local security policy for the computer.

Reference:

How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT, Microsoft Knowledge Base Article - Q239869

Incorrect Answers

B: The Dial-up Networking Security Upgrade is not required by Windows 98 clients.

C, D: We must reconfigure the Registry of the client computers. We cannot deploy the reconfiguration through GPOs.

QUESTION 208:

You are the administrator of a Windows 2000 Server computer named Certkiller 1. The server has two network adapters named Nic1 and Nic2 and is connected to two internal network segments. The IP addresses of the server are 10.1.5.2/24 on Nic1 and 10.1.6.2/24 on Nic2.

Both network segments contain Windows 2000 Professional client computers. All computers are members of the same Windows 2000 Active Directory domain. The Windows 2000 Professional client computers are configured with the Client (Respond Only) IPsec policy.

You want to ensure that all network traffic to and from Certkiller 1 and the segment connected to Nic2 is encrypted.

Users on other computers on that segment should not be able to read the information in the network packets.

You do not want to encrypt the network traffic on the segment connected to Nic1.

What should you do?

- A. On Certkiller 1, change the Advanced TCP/IP Settings of Nic2 to use the Secure Server (Require Security) IPsec policy.
- B. On Certkiller 1, change the Advanced TCP/IP Settings of Nic2 to enable TCP/IP filtering.
- C. On Certkiller 1, add input filters for any protocol to IP address 10.1.6.2, and add the output filters for any protocol from IP address 10.1.6.2.
- D. Configure the local policy on Certkiller 1 to assign an IPsec policy with a mirrored security rule for all network traffic to IP address 10.1.6.2

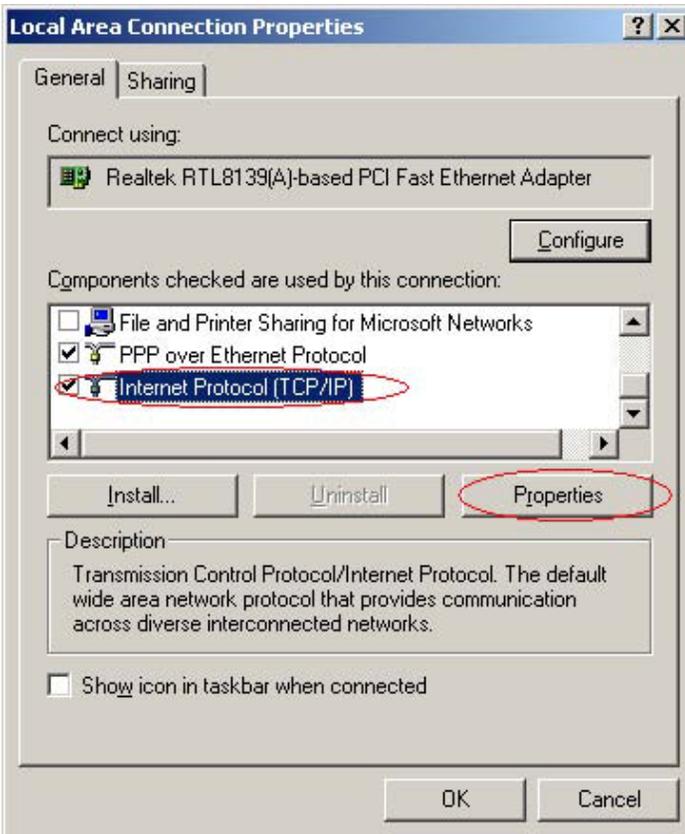
Answer: A

Explanation:

We change the IPsec security policy on NIC2 to Secure Server (Require Security). This will ensure that all traffic to and from the server on NIC2 is encrypted.

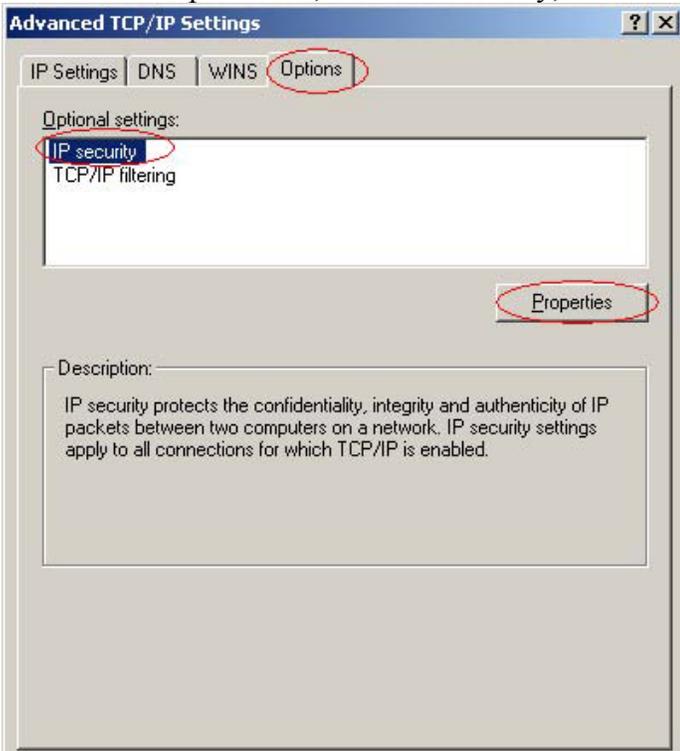
Procedure configure IP security policy for a network adapter:

1. Open Local Area Network (or similar) Properties for the Network adapter.
2. Select Internet Protocol (TCP/IP)
3. Click Properties.

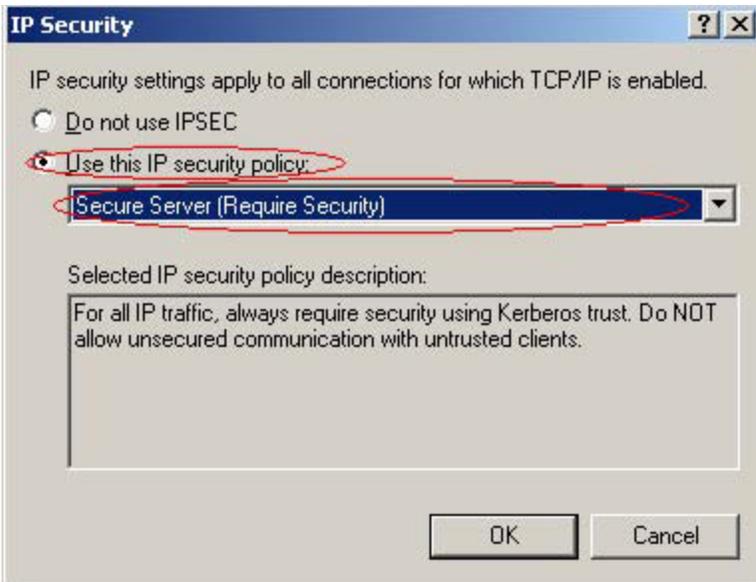


4. Click the Advanced button.

5. Select the Options tab, select IP Security, select Properties



6. Select Use this IP security policy and select Secure Server (Require Security).



Incorrect Answers

- B: TCP/IP filtering does not enable encryption.
 C: Input and output filters do not provide filtering.
 D: There is no such thing as mirrored security role.

QUESTION 209:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. All client computers run Windows 2000 Professional. Each department at Certkiller is in a separate organizational unit (OU) in the domain. Each departmental OU contains user, group, and computer accounts for that department. The human resources (HR) department has one Windows 2000 Server computer named Certkiller 1. The written security policy for the HR department requires all network communications with Certkiller 1 to be encrypted. Client computers in the HR department must also be able to communicate with servers in other departments.

The administrator for Certkiller 1 creates a Group Policy object (GPO) named HRLockdown and links the GPO to the HR OU. HRLockdown is configured with the No Override check box selected. The administrators configure and assign a new IPSec policy named HRSec in the HRLockdown GPO with the parameters shown in the following table.

Properties	Settings	Parameters (if required)
Tunnel setting	No IPSec tunnel specified	
Connection type	All connections	
Authentication	Kerberos	

IP filter list	All IP traffic	Source address: ANY Source Port: ANY Destination address: ANY Source port: ANY Destination address: ANY Destination port: ANY
Filter action	Require security	

The administrator reports that communications are secure within the department but that users in the department cannot access resources located on other network servers. You need to ensure that client computers in the HR department can communicate with other network servers, while maintaining the HR department's written policy. What should you do?

- A. Unassign the HRSec policy in the HRLockdown GPO.
Create child OU's named Servers and Clients in the HR OU.
Move the computer accounts for the client computers and for Certkiller 1 to the appropriate OUs.
Create a GPO and link it to the Clients OU.
Assign the Client (Respond Only) IPSec policy to that GPO.
Create a GPO and link it to the Servers OU.
Assign the Secure Server (Require Security) IPSec policy to that GPO.
- B. Unassign the HRSec policy in the HRLockdown GPO.
Create child OUs named Servers and Clients in the HR OU.
Move the computer accounts for the client computers and for Certkiller 1 to the appropriate OUs.
Create a GPO and link it to the Clients OU.
Assign the Client (Respond Only) IPSec policy to that GPO.
Create a GPO and link to the Servers OU.
Assign the Server (Request Security)IPSec policy to that GPO.
- C. Create a child OU named Clients in the HR OU and move the client computer accounts to the OU.
Create a GPO and link it to the Clients OU.
Assign the Client (Respond Only) IPSec policy to the GPO.
In the HRSec policy, specify the IP subnet address used by computers in the HR department as the source and destination addresses.
In the HRSec policy, set the filter action property to Request security.
- D. Create a child OU named Servers in the HR OU and move the computer account for Certkiller 1 to the OU.
Create a GPO and link it to the Servers OU.
Assign the Secure Server (Require Security) IPSec policy to the GPO.
In the HRSec policy, specify the IP subnet address used by computers in the HR department as the source and destination addresses.
In the HRSec policy, set the filter action property to Request security.

Answer: A

Explanation:

We cannot use the same IPSec policy for the server and for the clients. The Server must use the Secure Server (Require Security) IPSec policy to ensure that all communication to and from Certkiller 1 is encrypted. The clients only need to use the Client (Respond Only) IPSec policy. We separate the server and the client computers by using separate OUs.

Incorrect Answers

B: The GPO linked to the Servers OU must use the Secure Server (Require Security) IPSec policy to ensure that all communication to and from Certkiller 1 is encrypted.

C: The HRLockdown GPO will override the GPO linked to the Clients OU. The Secure Server (Require Security) policy will still be used on the client computers.

D: The HRLockdown GPO will override the GPO linked to the Servers OU. The Secure Server (Require Security) policy will not be used on Certkiller 1.