Trish is the systems administrator for a growing company. The company has recently merged with a competitor, requiring the upgrade of all of the competitor’s servers, running Microsoft Windows 2000 Advanced Server, to the corporate standard, Microsoft Windows Server 2003, Enterprise Edition. Trish is uncertain what security settings were configured on the servers prior to the upgrade, and she would like to see how the current settings deviate from the defaults.

What tools can Trish use to accomplish this? (Choose all that apply.)

1. The Gpresult command
2. The Security Templates snap-in
3. The Netsh command
4. The IP Security Monitor
5. The Secedit command  <Correct>
6. The Security Configuration and Analysis snap-in  <Correct>

Explanation:
Both the Security Configuration and Analysis snap-in and the Secedit command allow the comparison of the current security setting against a predefined template, as well as the application of the templates settings.

The Security Templates snap-in is used to view and modify the security configurations used by the Security Configuration and Analysis snap-in and the Secedit command.

The Gpresult command is used to view the cumulative group policy setting currently in effect, but it cannot compare the results to a preconfigured template.

The Netsh command does not include any group policy functions.

The IP Security Monitor does not include and group policy functions.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Implement secure network administration procedures. - Implement security baseline settings and audit security settings by using security templates.

References:
How to
TechNet, Microsoft
Analyze System Security in Windows 2000
Link: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B313203>
You are the network administrator for your company's Active Directory network. The servers in your organization are running Microsoft Windows Server 2003. The client computers are running Microsoft Windows XP Professional and Microsoft Windows 2000 Professional. You have implemented an IPSec policy for all of the computers in the domain. You are having problems connecting to one of your servers from any client computer.

In the exhibit below, click on the area that you would use to obtain detailed information about the IPSec Policy, including the numbers of authentications and negotiations.

**Explanation:**
The Main Mode, Statistics node of the IPSec Monitor will allow you to obtain detailed information about the IPSec Policy, including the numbers of authentications and negotiations.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Troubleshoot network protocol security. [59] Tools might include the IPSec Monitor MMC snap-in, Event Viewer, and Network Monitor.

**References:**
Monitor IPSec Activity
TechNet, Microsoft
Link:
You are the administrator for a network that supports 7,500 client computers. The network design calls for IPSec to be used on all network connections across public communication media.

You have been given a compiled listing of statistics as follows: Active Acquire, Active Receive, Acquire Heap Size, Total Acquire, Key Additions, Total Get SPI, Bad SPI Packets, Pending Key Operations.

You need to use quick mode statistics only for analysis purposes. Which statistics from the compiled listing can you use? (Choose all that apply.)

1. Bad SPI Packets  <Correct>
2. Pending Key Operations  <Correct>
3. Total Get SPI
4. Active Receive
5. Total Acquire
6. Acquire Heap Size
7. Active Acquire
8. Key Additions  <Correct>

Explanation:
From the compiled listing, only the Key Additions, Bad SPI Packets, and Pending Key Operations statistics can be used in quick mode.

The Key Additions statistic can also be used in main mode.

The Active Acquire, Active Receive, Acquire Heap Size, Total Acquire, and Total Get SPI statistics can only be used in main mode.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

References:
Viewing IPSec statistics and details about active IPSec policies
Windows Server 2003 Help, Microsoft
Lucy is the administrator for a small network consisting of three servers running Microsoft Windows Server 2003, Standard Edition, and 60 computers running Microsoft Windows XP Professional. She has recently received permission to increase the level of local security on the computers to reduce the amount of deskside support. She is writing a script using the Secedit command. She has configured a template named “xpsecure.inf” and placed it in the database located on a network share.

Which of the following commands should she include in her script to test syntax of the security template before applying it?

1. Secedit /analyze
2. Secedit /validate <Correct>
3. Secedit /configure
4. Secedit /import

Explanation:
The Secedit /validate command is used to verify the syntax of the template prior to application.

The Secedit /configure command is used to apply the settings in the specified template to the computer the command is run on.

The Secedit /analyze command is used to compare the computer the command is run on to a predefined template, not to apply the settings.

The Secedit /import command is used to place the template into a database so the template can be compared or configured. This step has already been performed.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Implement secure network administration procedures. - Implement security baseline settings and audit security settings by using security templates.

References:
How to
TechNet, Microsoft
Apply Predefined Security Templates in Windows 2000
Link: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B309689>
Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Question Number (ID): 5 (ebcMSP_MngNWI-024)

You are the network administrator for your company's Active Directory network. The servers in your organization are running Microsoft Windows Server 2003. The client computers are running Microsoft Windows XP Professional and Microsoft Windows 2000 Professional. You have implemented an IPSec policy on your network to ensure that data is secured during transmission.

Which of the following tools can be used to display IPSec Policy information on the Windows Server 2003 computers in your network?

From the list on the right, select the tools that allow you to view IPSec information. Place your selections in the list on the left by clicking the items in the list on the right and clicking the arrow button. You may not need to use all of the items from the list on the right.

Explanation:
The netsh ipsec static and dynamic show commands can be used to view details about IPSec policies.

The RSoP (Resultant Set of Policy) utility can be used to view the effective IPSec policy settings for a specific computer.

The netdiag utility was a Windows 2000 tool that could be used to view IPSec policy information. In Windows Server 2003, the netdiag /test:ipsec switch has been removed. The netdiag utility can be used to obtain basic networking information, but not IPSec-specific information. Netdiag /v/l can return basic networking information, such as IP and routing configuration.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

References:
Monitor IPSec Activity
TechNet, Microsoft

Troubleshooting Tools
TechNet, Microsoft
Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Question Number (ID) :  6  (wmpMSP_MngNW-068)

You are the administrator for a network that supports 5,500 client computers. The network design calls for IPSec to be used on all network connections across public communication media.

Which command-line tool can you use to configure IPSec on computers running Microsoft Windows Server 2003?

1. ipsecmon
2. netdiag
3. ipseccmd
4. netsh  <Correct>

Explanation :
For computers running Windows Server 2003, you can use the netsh command-line tool to run scripts for IPSec policy creation, display IPSec policy details, and make changes to IPSec configuration. The command begins with netsh ipsec and is followed by a variety of options.

The netdiag tool is available to install on computers running Windows Server 2003. However, the IPSec-related functionality of netdiag no longer is available on Windows Server 2003. It has been replaced by the netsh IPSec commands.

The ipseccmd command-line tool is used on computers running Windows XP to script IPSec policy creation, display IPSec policy details, and display IPSec configuration details.

Ipsecmon is a command-line tool that is used to monitor IPSec on a computer running Windows 2000. It is entered from a Windows 2000 command prompt.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

References :
Microsoft security administration tools
TechNet, Microsoft

Using Netdiag.exe to display IPSec information and to test and view network configuration
TechNet, Microsoft

Using Netsh to change the IPSec configuration on computers running the Windows .NET Server 2003 family
TechNet, Microsoft

Using Ipseccmd.exe to manage and monitor IPSec on computers running Windows XP
TechNet, Microsoft
You are the network administrator for your company's Active Directory network. The servers in your organization are running Microsoft Windows Server 2003. The client computers are running Microsoft Windows XP Professional and Microsoft Windows 2000 Professional. You are responsible for the security settings of all the servers. Each server must have the security settings configured identically. You decide to customize a predefined security template that will then be applied to the servers.

Which of the following utilities can be used to apply the security template to the servers?

From the list on the right, select the utilities that can be used to apply the security template to the servers. Place your selections in the list on the left by clicking the items in the list on the right and clicking the arrow button. You may not need to use all of the items from the list on the right.

**Explanation:**
In this scenario, you are responsible for configuring identical security settings across multiple server computers. The best way to do this is to customize a predefined security policy and then propagate the policy to each of the servers. The predefined policy can be imported into a group policy, which in turn can then be linked to the OU that contains the servers. The Secedit command line utility can be used to apply a security template to a computer. The Security Configuration and Analysis snap-in can be used to import and apply a security template to each server. The Local Security Policy on each server can also be configured to import and apply a predefined security template.

The Security Template snap-in can be used to configure or create a customized security policy as well as export the policy. It cannot be used to apply the security settings.

Gpupdate replaces the Secedit /refreshpolicy option to force the security policy to refresh itself, looking for changes.

The Certificate Authority snap-in is used to configure certificate services to be used to encrypt data and authenticate users. It has no bearing on this problem.

The NETSH command line utility is used to view and configure various network settings, but it cannot be used to apply a security template to a computer.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Implement secure network administration procedures. - Implement security baseline settings and audit security settings by using security templates.

**References:**
Security Templates Overview
TechNet, Microsoft

Predefined Security Templates
TechNet, Microsoft
Trish is the administrator for a medium-sized network. Lately, there have been some concerns about security patches and other updates not being applied consistently.

What is the simplest way that Trish can improve the consistency of updates and patches?

1. Send an email to all users instructing them to use the automatic updates feature on their computers once per week.

2. Schedule the task manager on each user's computer to run a script that points to downloaded updates.

3. Install and configure Software Update Services. <Correct>

4. Have the administrators run the automatic updates feature on each user's computer every week.

Explanation:
Installing and configuring Software Update Services will allow Trish to both mandate and control the applying of patches and updates.

Scheduling the task manager on each user's computer to run a script that points to downloaded updates could be configured to work, but it would not be the simplest method of improving consistency.

Having the administrators run the automatic updates feature on each user's computer every week would not be the simplest method of improving consistency.

Sending an email to all users instructing them to use the automatic updates feature on their computers once per week would not be practical. There would be no way to verify that the proper updates had been applied.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Install and configure software update infrastructure. - Install and configure software update services.

References:
Software Update Services Overview White Paper
TechNet, Microsoft
Link: http://www.microsoft.com/windows2000/docs/SUSOverview.doc>
You are a security administrator for a large corporate network. Your network has an IPSec-enabled server running Microsoft Windows Server 2003. IP Security Monitor displays the error message: The IPSec server is unavailable or incompatible with the IPSec monitor.

What is the most likely cause of the problem?

2. The IPSec service has been stopped.
3. The IP Security Monitor is attempting to monitor IPSec on a computer running Microsoft Windows XP.
4. The IP Security Monitor is attempting to monitor IPSec on a computer running Microsoft Windows 2000 Server. <Correct>

Explanation:
If you try to use the IP Security Monitor snap-in console to monitor IPSec on a computer running Windows 2000, you will receive the error: The IPSec server is unavailable or incompatible with the IPSec monitor.

The IP Security Monitor snap-in console is designed to monitor IPSec on computers running Windows Server 2003, so you would not receive any errors.

The IP Security Monitor snap-in console can also be used to monitor IPSec on computers running Windows XP, so you would not receive any errors running it.

If the IPSec service is stopped, you will not receive any data, but you would not receive the error message.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

References:
Troubleshooting
TechNet, Microsoft
Internet Protocol Security (IPSec)
You are a security administrator for a large corporate network. During an audit of traffic flows, you are concerned that some computers are unable to communicate with IPSec-secure computers on the network. You determine it is because the secure computers are configured to require client computers to initiate communications, and the computers that cannot communicate are not configured to initiate secure communications.

Most client computers are located a considerable distance from the server.

What should you do to correct the problem?

1. Allow unsecured communication requests to be processed by the secure server.   <Correct>
2. Reconfigure the client computers that cannot communicate so they can initiate secure communications.
3. Restart the IPSec service.
4. Reinstall client computers to make them IPSec-enabled

Explanation:
If you allow unsecured communication requests to be processed by the secure server, the client computers will be able to connect to the server.

Since the client computers are a considerable distance from the server, it might be difficult to reconfigure all of them so they can initiate secure communications.

Reinstalling client computers to make them IPSec-enabled is not a practical option, because the client computers are at a remote location.

Restarting the IPSec service will not correct the problem without changing the configuration.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

References:
Troubleshooting
TechNet, Microsoft
Internet Protocol Security (IPSec)
You want to install the Software Updates Services (SUS) software to run automatic updates to client computers on your network. Which configurations are valid? (Choose all that apply.)

1. Install SUS Service Pack 1 on computers running Microsoft Windows Server 2003.  <Correct>
4. Install SUS Service Pack 1 on computers running Microsoft Windows 2000 Server with Service Pack 2 or later.  <Correct>
5. Install SUS on computers running Microsoft Windows 2000 Server with Service Pack 2 or later.

**Explanation:**
The latest version of Software Update Services (SUS) includes Service Pack 1. You must use this version when installing the SUS software on computers running Windows Server 2003.

You must also use SUS Service Pack 1 when installing the SUS software on computers running Windows 2000 Server. The computers must be running Windows 2000 Server with Service Pack 2 or later.

The computers must not be running Windows 2000 Server with Service Pack 1 or earlier.

SUS Service Pack 2 does not exist and cannot be installed on computers running Windows 2000 Server. Therefore, it also cannot be installed on computers running Windows Server 2003.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Install and configure software update infrastructure. - Configuring software updates on legacy operating systems.

**References:**
Software Update Services Overview White Paper
TechNet, Microsoft
Chapter:  Server-Side Software Update Services  Pages: 16 - 23
Kyle is the administrator for a small network. He has 10 computers running Microsoft Windows Millennium Edition, which he would like to configure with the automatic updates client.

Which service will Kyle be replacing when he installs the automatic updates client?

1. The workstation service

2. The application management service

3. The critical updates service  <Correct>

4. The Directory Services Client

Explanation:
The automatic updates client replaces the critical updates service on Windows Millennium Edition.

The directory service client is not affected by the automatic updates client installation.

The workstation service, which manages connections to other computers, is not replaced by the automatic updates client.

The application management service manages software publishing in Windows XP and 2000, and is not available in Windows Millennium Edition.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Install and configure software update infrastructure. - Configuring software updates on legacy operating systems.

References:
Description of Automatic Updates in Windows Millennium Edition (Me)
TechNet, Microsoft
You are the network administrator for your company's Active Directory network. The servers in your organization are running Microsoft Windows Server 2003. The client computers are running Microsoft Windows XP Professional and Microsoft Windows 2000 Professional. Your company has 15,000 users. To ensure that all of the client computers have the latest updates and security patches, you are planning to install Software Update Services on one of your Windows Server 2003 computers.

From the list on the right, select the minimum hardware requirements that are necessary to install Software Update Services. Place your selections in the list on the left by clicking the items in the list on the right and clicking the arrow button. You may not need to use all of the items from the list on the right.

**Explanation:**
The minimum hardware configuration for a computer that will be running Software Update Services is:
* Pentium III 700 MHz Processor
* 512 MB RAM
* 6 GB of free hard disk space

This configuration is designed to support up to 15,000 clients with one SUS server.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Install and configure software update infrastructure. - Install and configure software update services.

**References:**
Patch Management using Microsoft Software Update Services
TechNet, Microsoft

Software Distribution Overview
TechNet, Microsoft

Software Update Services Deployment White Paper
TechNet, Microsoft
You are a systems administrator for an enterprise network. You have recently installed the Software Update Services (SUS) on a server running Microsoft Windows Server 2003, Enterprise Edition. Up to this point, the computers on the network had no consistent policy for updates.

Which feature of the Software Update Service will make sure that all necessary updates are applied in the proper order?

1. Chained installation <Correct>
2. Scheduled updates
3. Forced rebooting
4. Built-in security
5. Background updates

Explanation:
Chained installation applies the necessary updates in the proper order, with prerequisite updates installing first.

Background updates allows the updates to be applied without user initiation, but is not involved with the order in which the updates are applied.

The built-in security of SUS, where only administrators can modify the settings and digital signatures are used, does not affect the order in which the updates are applied.

Forced rebooting prompts the user to reboot if necessary, but does not control the order in which the updates are applied.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Install and configure software update infrastructure. - Install and configure automatic updates client.

References:
Software Update Services Overview White Paper
TechNet, Microsoft
Link: http://www.microsoft.com/windows2000/docs/SUSOverview.doc>
As an administrator for an organization, you are responsible for configuring the infrastructure to deploy critical and security updates to desktop and server clients. A systems engineer has already created a software update infrastructure plan. You are tasked with implementing this plan. You must test all client software updates prior to deploying them. You receive a new update and test it, but you decide not to install it because of concerns about how proprietary applications are affected.

Using the Approve Updates option, how can you prevent the update from being installed on the Automatic Updates clients?

1. Select the check box next to the update and click the Approve button.
2. Select the check box next to the update and click the Remove button.
3. Clear the check box next to the update and click the Approve button. <Correct>
4. Clear the check box next to the update and click the Remove button.

Explanation:
As the administrator, if you clear the check box next to the update and click the Approve button at the bottom of the page, the files will not be updated on the Automatic Updates clients. If that update has a dependency update that goes with it, you will receive a warning to that effect.

If you select the check box next to the update and click the Approve button at the bottom of the page, the updates will be available to any computer running the Automatic Updates client that is connected to the Software Update Services server. If that update has a dependency update that goes with it, the clients must also install that update.

If you clear the check box, there is no Remove button to click to disapprove the update.

If you select the check box, there is no Remove button to click to disapprove the update.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
- Install and configure software update infrastructure.
- Install and configure software update services.

References:
- Software Update Services Overview White Paper
- TechNet, Microsoft
- Server-Side Software Update Services
You are a security administrator for a large corporate network. After reviewing the audit logs with Event Viewer, you discover that computers are connecting, but that IPSec security association (SA) negotiation is failing. You are using certificate authentication on the network.

What could be the cause of the problem?

1. The Allow unsecured communication with non-IPSec-aware computers option is selected.
2. The Filter list is not configured properly.
3. Audit logging has not been configured.
4. The correct certificates are not installed on the IPSec peer computers. <Correct>

Explanation:
If the correct computer certificates are not installed on the IPSec peer computers, IPSec SA negotiation will fail if the computers are using certificate authentication. The solution is to install the certificates on the peer computers.

The filters not being configured properly would cause unsecured traffic, but not failed SA negotiations.

If the Allow unsecured communication with non-IPSec-aware computers option on the Security Methods tab of the filter action is selected, unsecured communications would be occurring on the network.

If audit logging had not been configured, you would not be able to view the logging information in Event Viewer.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

References:
Troubleshooting
TechNet, Microsoft
Internet Protocol Security (IPSec)
You are the administrator for a company. You log on to ComputerA running Microsoft Windows Server 2003 as a member of the Users group with no special administrative privileges. You enter the command \texttt{runas /user:Administrator@ComputerA} \texttt{mmc "C:\Windows\System32\compmgmt.msc"} to start an MMC snap-in with administrative privileges. The command does not work.

What could be the cause of the problem?

1. The Secondary Logon service is not running on ComputerA. \textit{<Correct>}
2. The DNS service is not running on ComputerA.
3. The DHCP service is not running on ComputerA.
4. You do not have permission to run the \texttt{runas} command.

\textbf{Explanation:}

The \texttt{runas} command uses the Secondary Logon service to allow you to run commands using another account's permissions. If the Secondary Logon service is stopped, the \texttt{runas} command may not work properly.

The \texttt{runas} command does not require any special permission to run. Any user should be able to run the command.

Whether the DNS service is or is not running on ComputerA has no effect on the proper functioning of the \texttt{runas} command.

Whether the DHCP service is or is not running on ComputerA has no effect on the proper functioning of the \texttt{runas} command.

\textbf{Objective:}

Implementing, Managing, and Maintaining Network Security

\textbf{Sub Objective(s):}

Implement secure network administration procedures. - Implement the principle of least privilege.

\textbf{References:}

Runas command
Windows Server 2003 Help, Microsoft
**Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure**

Question Number (ID): 18 (wmpMSP_MngNWl-070)

You are a security administrator for a large corporate network. During an audit of traffic flows, you are concerned by an increase in unsecured traffic occurring on the network. Using NETMON, you establish that the majority of this increase in unsecured traffic occurs to a single server on the network.

After reviewing the audit logs with Event Viewer, you discover that computers are connecting on the network, but traffic is not being secured by IPSec.

What could be the cause of the problem? (Choose all that apply.)

1. The correct certificates are not installed on the server.
2. The correct certificates are not installed on the IPSec peer computers.
3. The Filter list is not configured properly. **<Correct>**
4. The Allow unsecured communication with non-IPSec-aware computers option is not selected.
5. The Allow unsecured communication with non-IPSec-aware computers option is selected. **<Correct>**

**Explanation:**
If network traffic is not being made secure by IPSec, it is likely that an IPSec security association is not being established. This can happen if the filter list is not configured properly. It can also occur if you have enabled unsecured communication with non-IPSec-aware computers. This could be happening if the Allow unsecured communication with non-IPSec-aware computers option on the Security Methods tab of the filter action is selected.

If the Allow unsecured communication with non-IPSec-aware computers option on the Security Methods tab of the filter action is not selected, only IPSec communications should occur on the network.

It does not matter if the correct certificates are not installed on the server, unless the server uses certificate authentication.

It does not matter if the correct certificates are not installed on the IPSec peer computers, unless the IPSec peer computers use certificate authentication.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

**References:**
Troubleshooting
TechNet, Microsoft
Internet Protocol Security (IPSec)
You are the administrator for an organization. You want to set up secure network administration parameters based on a security configuration plan established by your organization. Your goal is to implement the principle of least privilege using secondary logon. You want to implement security best practices for your organization.

Which type of account should you use to log on to a computer running Microsoft Windows Server 2003?

1. Power Users
2. Users <Correct>
3. Administrators
4. Domain Admins

Explanation:
Using the practice of least privilege, an administrator should log on to a computer with an account that has minimal privileges and then use the runas command with administrative credentials to perform higher-level tasks. By doing so, you avoid some of the security risks of Administrative logons such as Trojan Horse attacks.

If you log on as a power user, you may have more privileges than you need for a basic logon. For example, Power Users can often add or delete user accounts.

If you log on as a Domain Admin, you have full control of the domain, including administrative access to all computers in the domain. This is too much privilege to have with an account you use to log on. It allows a security risk.

If you log on under the Administrator account, you have administrative access to the local computer. This is too much privilege to have with an account you use to log on. It allows a security risk.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Implement secure network administration procedures. - Implement the principle of least privilege.

References:
Starting Programs and Tools in Administrative Context
TechNet, Microsoft
Secondary Logon (Run As)

Best Practices
Windows Server 2003 Help, Microsoft
Security
You are the administrator for an organization. You want to configure a computer running Microsoft Windows Server 2003 to automatically download critical and security updates as an Automatic Updates client and receive a notification when the updates are ready to be installed.

How does the local administrator know when an update is ready to install?

1. an e-mail message from the Windows Update server
2. a pop-up message on the Windows Update Web site
3. an entry in the event log
4. a message in the notification area  <Correct>

Explanation:
If you configure the Automatic Updates client to notify you when an update ready to be installed, the notification will appear as a balloon message in the lower-right corner of the desktop, also called the notification area.

You will not receive an e-mail message from the Windows Update server for this type of notification. However, you can configure a Software Update Services (SUS) server to send you an e-mail message when it is synchronizing with the Windows Update server.

When an update is ready to be installed, an entry is sent to the event log that makes note of the notification. This is not something that an administrator would check often enough and is not the most obvious form of notification.

An administrator would not receive a pop-up message from the Windows Update Web site. Even if such a notice were given, the administrator would have to be viewing the Windows Update Web site constantly to know when the updates were available.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Install and configure software update infrastructure. - Install and configure automatic updates client.

References:
Software Update Services Overview White Paper
TechNet, Microsoft
Chapter:  Client-Side Automatic Updates   Pages: 7 - 15

Software Update Services Overview White Paper
TechNet, Microsoft
Chapter:  Server-Side Software Update Services   Pages: 16 - 23
You are the network administrator for your company's Active Directory network. The servers in your organization are running Microsoft Windows Server 2003. The client computers are running Microsoft Windows XP Professional and Microsoft Windows 2000 Professional. You are responsible for the management and maintenance of security on the network. You plan on implementing the principle of least privilege.

From the list on the right, select the tasks that involve implementing the principle of least privilege. Place your selections in the list on the left by clicking the items in the list on the right and clicking the arrow button. You may not need to use all of the items from the list on the right.

**Explanation:**
The principle of least privilege is the security concept that a user should have the minimum permissions necessary to perform specific administrative tasks. This means that users should log on using normal non-administrative accounts to perform daily jobs and then use the runas utility to perform specific administrative tasks.

The principle of least privilege also involves delegating control over specific objects in Active Directory to allow users to perform specific tasks without needing to have membership in built-in groups. For example, you could delegate authority to a user so that the user could reset passwords for the user objects in Active Directory. This can also be accomplished by making that user a member of the Account Operators built-in group. As a member of the Account Operators, not only would the user be able to reset passwords, he or she would be able to create, delete, and manage all user accounts except for the Administrator account.

The principle of least privilege always begins with assigning the most restrictive permissions and then giving more if they are needed later on.

Logging on to perform normal job-related tasks using an administrator account goes against the principle of least privilege. You should log on using a regular account and then use the runas utility to perform administrative tasks.

The Windows Server 2003 built-in groups are designed for legacy support in mixed mode environments. You should delegate authority to perform specific tasks instead of adding users into the built-in groups. Often, the built-in groups will give too many rights to the users.

By assigning the least restrictive permissions first, you are going against the principle of least privilege. You should give the users the minimum permissions to perform a task. If they need a different level of permissions, they will let you know.

All authenticated users already have the Read and Apply Group Policy permissions assigned to the container objects in Active Directory. If you gave the users the permission to write to Active Directory, they would be able to make changes to attributes of objects in Active Directory.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
- Implement secure network administration procedures.
- Implement the principle of least privilege.

**References:**
Best Practices for Security
TechNet, Microsoft

**Link:**
docs/entserver/sag_seconceptsBP.asp
You are the network administrator for your company’s Active Directory network. The servers in your organization are running Microsoft Windows Server 2003. The client computers are running Microsoft Windows 2000 Professional. You are responsible for maintaining the client computers. You want to ensure that the client computers automatically download Windows Updates. To reduce the amount of Internet traffic that would be generated by this process, you have installed Software Update Services. The Active Directory OU structure is departmental. Each departmental OU has a computer OU that contains the client computers. The following exhibit shows a diagram of the Active Directory environment.

You must configure the client computers to use Software Update Services. Your implementation must be efficient.

Select from the list on the left the steps that are necessary to provide a solution. Place the steps in the list on the left in the order in which they should be performed. Place your selections in the list on the left by clicking the items in the list on the right and clicking the arrow button. You can also use the Up and Down buttons to rearrange items in the list on the left. You may not need to use all of the items from the list on the right.

**Explanation:**
To allow the Windows 2000 Professional computers to use Software Update Services, you must install wuau22.msi on them. This is the automatic update client software. To install the client software, the Windows 2000 Professional computers must have Service Pack 3 installed.

Instead of visiting each client computer to install wuau22.msi, it would be easier to push the software with a Group Policy. To push wuau22.msi, you should create a GPO on one OU and then link it to the other OUs that contain the other client computers.

Once the software is installed, it must be configured. Again, you could visit each client computer to configure the settings, but it would be much easier to use a Group Policy to configure the settings. You should create the GPO on one of the OUs that contains the client computers and then link it to the other OUs that also include client computers.

Since this software deployment and configuration should only affect the client computers, there is no reason to deploy GPOs at the domain level.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Install and configure software update infrastructure. - Install and configure automatic updates client.

**References:**
Windows Update
TechNet, Microsoft

Software Distribution Overview
TechNet, Microsoft

Software Update Services Deployment White Paper
TechNet, Microsoft
You are a security administrator for a large corporate network. Certificates are installed on all IPSec peers and the server, but the server does not use certificate authentication. Default Active Directory IPSec policies are implemented. All peer computers and the server on the network are IPSec-enabled and IPSec-compatible.

After reviewing the audit logs with Event Viewer, you discover that IPSec security association (SA) negotiation is failing.

What could be the cause of the problem? (Choose two.)

1. Certificates are not installed on the IPSec peer computers or the server.
2. One or both of the IPSec peer computers are not part of an Active Directory domain. <Correct>
3. One or both of the IPSec peer computers are running Microsoft Windows XP Home Edition. <Correct>
4. The Filter list is not configured properly.

**Explanation:**

If the default Active Directory IPSec policy is applied, and one or both of the IPSec-aware peer computers are not part of an Active Directory domain, IPSec SA negotiation will fail.

A computer running Windows XP Home Edition cannot be a member of an Active Directory domain; therefore this would cause IPSec SA negotiation to fail.

The filters not being configured properly would cause unsecured traffic, but not failed SA negotiations.

It does not matter whether or not certificates are installed on the IPSec peer computers or the server, because the server does not use certificate authentication.

**Objective:**

Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**

Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

**References:**

Troubleshooting
TechNet, Microsoft
Internet Protocol Security (IPSec)
Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Question Number (ID) :  24  (wmpMSP_MngNWI-067)

You are the administrator for a network that supports 7,500 client computers. The network design calls for IPSec to be used on all network connections across public communication media. The network uses Kerberos version 5 for authentication.

You want to monitor the issuing of Kerberos tickets for authentication using a command-line tool for computers running Microsoft Windows Server 2003. Which tool can you use?

1. netdiag /test:ipsec
2. kerbtray
3. IPSecmon
4. klist <Correct>

**Explanation:**
Kerberos List (klist) is a command-line tool that allows you to view and delete current Kerberos tickets.

Kerbtray is a GUI tool that displays Kerberos ticket information.

IPSecmon is a command-line tool that is used to monitor IPSec on a computer running Microsoft Windows 2000.

Netdiag /test:ipsec is no longer available for computers running Windows Server 2003. It has been replaced by the command netsh ipsec static show or netsh ipsec dynamic show. It displays information about IPSec policies, but not about Kerberos.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

**References :**
Microsoft security administration tools
TechNet, Microsoft

Monitor IPSec activity
Windows Server 2003 Help, Microsoft

Using Netdiag.exe to display IPSec information and to test and view network configuration
TechNet, Microsoft
You are the administrator for a medium-sized network consisting of servers running Microsoft Windows NT and Microsoft Windows Server 2003. You are planning to upgrade the domain controllers running Windows NT 4.0 to Windows Server 2003, Standard Edition. You are writing a script to apply a security template to the servers immediately after the upgrade.

Which template would be appropriate to use?

1. Rootsec
2. Setup security
3. DC security  <Correct>
4. Securews

**Explanation:**
It would be appropriate to use the DC security template in this case. This template applies the default settings that are used when the Active Directory is installed on a non-upgraded server.

The securews template should be used to restrict a user's access to a workstation computer (hence the "ws" at the end of the name).

The rootsec template is used to apply restricted file system permissions to the system directory.

The setup security template is used to apply the default security setting from a non-upgraded installation. Since these servers are domain controllers, higher security should be applied.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Implement secure network administration procedures. - Implement security baseline settings and audit security settings by using security templates.

**References:**
How to
TechNet, Microsoft
Apply Predefined Security Templates in Windows 2000
Link: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B309689>
Jeff is the systems security administrator for a large hospital. Changes in regulations have prompted him to increase security on his 45 servers running Microsoft Windows Server 2003. He has configured a security policy template with the desired settings and would like to apply it to his servers.

What is the simplest and quickest method of applying these settings to the local security policy of each of the 45 servers?

1. Through the Security Configuration and Analysis snap-in
2. Through the Security Templates snap-in
3. Writing a script that uses the Secedit command  <Correct>
4. Writing a script that uses the Gpresult command

Explanation:
Writing a script that uses the Secedit command would allow the application of the desired settings to be scheduled and applied to all servers, instead of manually applying the changes to each server individually.

Using the Security Configuration and Analysis snap-in would, in fact, apply the desired settings. However, Jeff would have to connect to each of the servers and apply the template to each. Other solutions would be quicker.

The Security Templates snap-in is used to view and modify the security configurations used by the Security Configuration and Analysis snap-in and the Secedit command.

The Gpresult command is used to view the cumulative group policy setting currently in effect, but it cannot compare the results to a preconfigured template.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Implement secure network administration procedures. - Implement security baseline settings and audit security settings by using security templates.

References:
How to
TechNet, Microsoft
Apply Predefined Security Templates in Windows 2000
Link: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B309689>
You are the administrator for an organization. You want to set up secure network administration parameters based on a security configuration plan established by your organization. You want to establish an account lockout policy and security options across a domain. You want to apply a template using a best practices philosophy.

Which task should you perform to maintain the best practices philosophy?

1. Edit and make changes to the Setup security.inf template.
2. Edit and make changes to the Compatible (Compatws.inf) security template.
3. Import the Setup security.inf template to a Group Policy Object (GPO).
4. Customize a predefined template and save the changes under a different file name. Import the custom template to a GPO. <Correct>

Explanation:
Since you want to apply an account lockout policy and security options across a domain, you need to import a security template to a GPO. You should start with a predefined security template, then make appropriate changes and save them to a different file name. If you save the changes under the original file name, your changes become part of the predefined security template. This may not be desirable. It is best to keep the predefined security template settings intact and create a new custom template with a different file name.

If you only import the Setup security.inf template to a GPO, you will not have your desired changes incorporated. You should also not apply this particular security template to a GPO. This is because it contains a large amount of data and degrades performance because of periodic refreshes of Group Policy throughout the domain.

If you edit and make changes to the Setup security.inf template, and save those changes to the same file, you will alter the default security settings, which may not be desirable. You should save changes under a different file name. Also, your changes are not applied across the domain unless they are imported to a GPO.

If you edit and make changes to the Comptws.inf template, and save those changes to the same file, you will alter the Compatws.inf security settings, which may not be desirable. You should save changes under a different file name. Also, your changes are not applied across the domain unless they are imported to a GPO. The Compatws.inf template should not be applied to domain controllers.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Implement secure network administration procedures. - Implement security baseline settings and audit security settings by using security templates.

References:
Best Practices for Security Templates
Windows Server 2003 Help, Microsoft

Predefined Security Templates
Windows Server 2003 Help, Microsoft
You are a security administrator for a large corporate network. During an audit of traffic flow on the network, you are concerned that some computers are unable to communicate with the IPSec-secure server running Microsoft Windows Server 2003. You determine that the secure server is not using the locally configured IPSec policy.

What could be the cause of the problem? (Choose all that apply.)

1. The IPSec service has stopped. <Correct>
2. The correct certificates are not installed on the server.
3. The server is receiving its policy from Active Directory. <Correct>
4. The server is not a member of an Active Directory domain.

Explanation:
If the IPSec service has stopped, this would cause the secure server not to use the locally configured IPSec policy. You will need to start the IPSec service.

If the secure server is a member of an Active Directory domain, it will receive its IPSec policy from the Active Directory database and not from the locally configured IPSec policy.

If the secure server were not a member of an Active Directory domain, it would use the locally configured IPSec policy.

Since the scenario does not mention the use of certificate authentication, the cause of the problem is not likely to be related to the installation of certificates on the server.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

References:
Troubleshooting
TechNet, Microsoft
Internet Protocol Security (IPSec)
Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Question Number (ID): 29 (jaaMSP_MngNWI-074)


On which of the following operating systems can Joan configure automatic updates? (Select all that apply.)

1. Windows Millennium Edition <Correct>
2. Windows 98
4. Windows 95
5. Windows XP Professional <Correct>
6. Windows 2000 Professional <Correct>
7. Windows NT Workstation 4.0

Explanation:

The automatic updates client is not available for the Windows NT Workstation 4.0 operating system.

The automatic updates client is not available for the Windows 98 operating system.

The automatic updates client is not available for the Windows 95 operating system.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Install and configure software update infrastructure. - Configuring software updates on legacy operating systems.

References:
Software Update Services Overview White Paper
TechNet, Microsoft
Link: http://www.microsoft.com/windows2000/docs/SUSOverview.doc>
You are the administrator for an organization. You want to set up secure network administration parameters based on a security configuration plan established by your organization. You log on to your local computer running Microsoft Windows Server 2003 with an account that has minimal administrative privileges. You perform numerous tasks and then discover that you need to perform some higher-level administrative tasks for which you do not have permissions under your logged-in account. You want to perform the higher-level tasks using security best practices.

What should you do?

1. Send an e-mail to another administrator who has higher-level privileges and ask him or her to perform the higher-level tasks.
2. Restart the computer and log on again under the Administrator account.
3. Log off and log on again under the Administrator account.
4. Perform the tasks using the runas command. <Correct>

**Explanation:**
The runas command in Windows Server 2003 allows a user to perform tasks with different permissions than the permissions associated with their current logged-on account. For example, if you want to run a command using the Administrator permissions, click the Start button, then click Run and enter runas /user:AdministratorAccountName@ComputerName <command>. The runas command can be used to log on under any account, not just the Administrator account.

Logging off and logging back on under the Administrator account allows you to perform higher-level administrative tasks, but this is not considered a best practice for security. The Administrator account credentials are more likely to be compromised by doing so.

Sending an e-mail to another administrator with higher-level privileges to ask him or her to perform higher-level tasks is not considered a best practice for security. The e-mail message could be intercepted by an unauthorized person, revealing information you might desire to keep private. Also, another administrator could not perform the tasks by any more efficient method than you can.

It is not necessary to restart the computer before logging on to the computer under another account.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Implement secure network administration procedures. - Implement the principle of least privilege.

**References:**
Best Practices
Windows Server 2003 Help, Microsoft
Security

Runas command
Windows Server 2003 Help, Microsoft
You are the administrator for a medium-sized organization. You want to set up secure network administration parameters. You want to configure a security template for use on multiple computers on the local network. You log on to a computer running Microsoft Windows Server 2003 to begin making changes.

Which tool should you use to create the new template?

1.  Secedit
2.  Security Configuration and Analysis snap-in <Correct>
3.  Local Security Policy
4.  Security Settings extension to Group Policy

Explanation:
The Security Configuration and Analysis tool is used to analyze or configure computer security with a security template. It is an MMC snap-in that you can launch by clicking the Start button and clicking Administrative Tools. You may need to add this tool to the MMC if it is not already there.

The Security Settings extension to Group Policy tool is used to edit individual security settings on a domain, site, or organizational unit in Active Directory.

The Local Security Policy tool is used to edit security settings on a local computer.

The secedit tool is a command-line tool that is used to automate security tasks.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Implement secure network administration procedures. - Implement security baseline settings and audit security settings by using security templates.

References:
Security Templates
TechNet, Microsoft
You want to configure a computer running Microsoft Windows Server 2003 to automatically download critical and security updates as an Automatic Updates client and install the updates according to a predetermined schedule. Active Directory is not installed.

What can you do to perform this task?

1. Configure the Group Policy Automatic Updates Properties configure automatic update setting to Enabled.

2. Set NoAutoUpdate to 0 in the registry key HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU.

3. Configure the Group Policy Automatic Updates Properties automatic update setting to Auto download, and schedule the install.

4. Set AUOptions to 4 in the registry key HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU. <Correct>

Explanation:
Since Active Directory is not installed, you will need to edit the registry keys to make changes to the Automatic Update settings. To configure the updates to be downloaded automatically and installed according to a predetermined schedule, you must change AUOptions to 4 in the registry key HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU.

The NoAutoUpdate is set to 0 by default in the registry key HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU. This setting enables Automatic Updates on the client.

Since Active Directory is not installed, you will not be able to use the Group Policy Automatic Updates Properties to configure the automatic updates clients.

If Active Directory were installed, you would set the Configure Automatic Update setting to Enabled and the Automatic Update setting to Auto download, and schedule the install.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Install and configure software update infrastructure. - Install and configure automatic updates client.

References:
Software Update Services Overview White Paper
TechNet, Microsoft
Chapter: Client-Side Automatic Updates Pages: 7 - 15
You are the administrator for a network that supports 4,000 client computers. The network design calls for IPSec to be used on all network connections across public communication media.

Using IPSec Monitor, how can you determine how many users have successfully logged on to your network through the secure IPSec authentication processes main mode since the IPSec process was last started?

1. View Active Security Associations under Quick Mode Statistics. <Correct>
2. View IKE Quick Mode statistics under Main Mode Statistics.
3. View IKE Main Mode statistics under Main Mode Statistics.
4. View the Active Acquire statistic under Main Mode Statistics.

Explanation:
The Quick Mode Active Security Associations statistic is the number of Quick Mode security associations. A security association is a connection between IPSec peer computers. This is the same as a successful logon.

The Main Mode Active Acquire statistic is the number of pending and queued requests to establish a Security Association (connection) between IPSec peers.

The Main Mode IKE Quick Mode statistic is the total number of successful Security Associations created during Quick Mode operation since the IPSec service was last started.

The Main Mode IKE Main Mode statistic is the total number of successful Security Associations during Main Mode operation since the IPSec service was last started.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

References:
Viewing IPSec statistics and details about active IPSec policies
Windows Server 2003 Help, Microsoft
You are the administrator for a network that supports 6,500 client computers. The network design calls for IPSec to be used on all network connections across public communication media.

You need to know which Main Mode statistics to use when you implement the design.

Match each statistic name with its Main Mode description by dragging the statistic name to the box to the left of the correct description.

**Explanation:**
- The Main Mode Active Acquire statistic is the number of pending requests to establish a security association. A security association is a completed IPSec connection and logon.
- The Main Mode Active Receive statistic is the number of IKE messages received that are queued for processing.
- The Main Mode Receive Heap Size statistic is the number of entries in the IKE receive buffers.
- The Main Mode Total Acquire statistic is the total number of requests received for IKE processing since the IPSec service was last started.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Monitor network protocol security. Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

**References:**
Viewing IPSec statistics and details about active IPSec policies
Windows Server 2003 Help, Microsoft
Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

You are the administrator for a medium-sized organization. You want to set up secure network administration parameters. Currently, the default security template parameters are configured on a computer running Microsoft Windows Server 2003 on the local network. You want to create a new security template that contains slight modifications to the password policies of the default parameters.

How can you accomplish this?

1. Open the MMC and add the Security Templates snap-in. Configure the necessary changes and save the file under a new file name.

2. Open the Security Templates folder from the MMC. Make modifications to the default file and save the file under the file named Setup security.inf.

3. Open the MMC and add the Security Configuration and Analysis snap-in. Make modifications to the default file and save the file under a new file name.

4. Open the Security Templates folder from the MMC. Make modifications to the default file and save the file under a new file name. <Correct>

Explanation:
To make changes to the default security template, click the Security Templates folder from the Microsoft Management Console (MMC). To run the MMC, click Start, then click Run and enter mmc. Since the default security template is loaded, to make changes you need to make modifications in the Details pane after clicking the Setup security template. Then you need to save the changes under a new file name.

If you save the changes under the filename Setup security.inf, then the default security template file will be overwritten, and you will never be able to go back to the original default settings.

Since the default security template is already being used, you will not need to add the Security Templates snap-in to the MMC. You can make configuration changes to the default security template by clicking the File menu and then opening the appropriate .msc file from the Administrative Tools folder.

The Security Configuration and Analysis snap-in is used to apply a security template to a local policy. This means that it applies the template settings to the local computer.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Implement secure network administration procedures. - Implement security baseline settings and audit security settings by using security templates.

References:
To apply a security template to local policy
TechNet, Microsoft

Security Templates
TechNet, Microsoft

To add Security Templates to an MMC console
TechNet, Microsoft
**Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure**

**Question Number (ID) :** 36 (wmpMSP_MngNWI-050)

You are the administrator for an organization. You want to set up secure network administration parameters based on a security configuration plan established by your organization. You want to establish account lockout policy and security options across a domain. You log on to a computer running Microsoft Windows Server 2003 to begin making changes.

How can you accomplish your goal?

1. Configure a custom security template and apply it to a Group Policy Object (GPO).  <Correct>
2. Configure a custom security template and apply it to the local security policy.
3. Apply the Rootsec.inf template to the GPO.
4. Apply the Setup security.inf template across the domain.

**Explanation :**
To apply security parameters across a domain or organizational unit (OU), you need to configure a custom security template and import it into an existing Group Policy Object (GPO).

Configuring a customer security template and applying it to the local security policy will only change the settings for the local computer. It will have no effect on the other computers in the domain.

Applying the Setup security.inf template across the domain will implement the default security template across the domain, but will not provide changes to individual settings for account lockout and security options. To make changes to the default security template, you need to click the Security Templates folder from the Microsoft Management Console (MMC). Since the default security template is loaded, to make changes you need to make modifications in the Details pane after clicking the Setup security template. Then you need to save the changes under a new file name.

Applying the Rootsec.inf security template to the GPO will implement the predefined security template associated with root security. It applies permissions to the root folder of the system drive. If you implement this template, you will not have accomplished your intent, which is to implement changes to settings for account lockout and security options.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Implement secure network administration procedures. - Implement security baseline settings and audit security settings by using security templates.

**References :**
Security Templates
Introducing Microsoft Windows Server 2003, Microsoft Press
Chapter:  4  Pages: 65 - 66

Predefined Security Templates
Windows Server 2003 Help, Microsoft
You are the administrator for an organization. You want to configure a computer running Microsoft Windows Server 2003 to automatically download critical and security updates as an Automatic Updates client, and receive a notification when the updates are ready to be installed.

Which group of users has permission to perform this configuration? (Choose all that apply.)

1. Administrators <Correct>
2. Domain Users
3. Domain Guests
4. Users
5. Domain Admins <Correct>

Explanation:
Only a local administrator can configure an Automatic Updates client to receive updates. Therefore, since a local administrator is a member of the Administrators group, he or she has permission to perform the configuration. Since a member of the Domain Admins group can perform administrative functions locally, he or she also has permission to perform the configuration. The valid configuration settings are:

- Notify me before downloading any updates, and notify me again before installing them on my computer
- Download the updates automatically, and notify me when they are ready to be installed
- Automatically download the updates, and install them on the schedule that I specify

A member of the Users group does not have administrative permission and cannot configure an Automatic Updates client.

A member of the Domain Users group has permission to perform tasks that all other users in the domain can perform. A member of the Domain Users group does not have administrative permissions and cannot configure an Automatic Updates client.

A member of the Domain Guests group has the same permission as all guests in the domain. A member of the Domain Guests group does not have administrative permissions and cannot configure an Automatic Updates client.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
- Install and configure software update infrastructure.
  - Install and configure automatic updates client.

References:
Software Update Services Overview White Paper
TechNet, Microsoft
Chapter: Client-Side Automatic Updates Pages: 7 - 15

Default Groups
Windows Server 2003 Help, Microsoft
You are the administrator for a network that supports 3,500 client computers. The network design calls for IPSec to be used on all network connections across public communication media. You configure IPSec filters on a computer running Microsoft Windows Server 2003.

Which filters are exempt from being configured?

1. RSVP
2. IKE <Correct>
3. Broadcast
4. Kerberos
5. Multicast

**Explanation:**
For computers running Windows Server 2003, only IKE traffic is exempt from IPSec filtering. This means that you can configure filters for every kind of traffic except IKE.

For computers running Microsoft Windows 2000 Server, broadcast, multicast, IKE, Kerberos, and RSVP traffic are exempt from IPSec filtering.

For computers running Microsoft Windows XP, broadcast, multicast, IKE, Kerberos, and RSVP traffic are exempt from IPSec filtering.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

**References:**
Exempt all broadcast, multicast, IKE, Kerberos, and RSVP traffic from IPSec filtering
Windows Server 2003 Help, Microsoft
You are the administrator for a network that supports 4,000 client computers. The network design calls for IPSec to be used on all network connections across public communication media. Using IPSec Monitor, how can you determine how many users have attempted to log on to your network through the secure IPSec authentication processes main mode since the IPSec process was last started?

1. View the Total Acquire statistic under Main Mode Statistics. <Correct>

2. View the Offloaded Security Associations statistic under Quick Mode Statistics.

3. View the Acquire Heap Size statistic under Main Mode Statistics.

4. View the Active Security Associations statistic under Quick Mode Statistics.

Explanation:
The Main Mode Total Acquire statistic refers to the total number of requests to log on using IPSec using Internet Key Exchange (IKE) since the last time the IPSec service was started.

The Main Mode Acquire Heap Size statistic is the size of the heap that contains active acquires. Active acquires are the number of requests pending using Internet Key Exchange (IKE).

The Quick Mode Active Security Associations statistic is the number of Quick Mode security associations. A security association is a connection between IPSec peer computers.

The Quick Mode Offloaded Security Associations statistic is the number of Quick Mode security associations that have been offloaded to hardware to perform cryptographic functions.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Monitor network protocol security. [56] Tools might include the IPSec Monitor MMC snap-in and Kerberos support tools.

References:
Viewing IPSec statistics and details about active IPSec policies
Windows Server 2003 Help, Microsoft
Craig is the systems architect for an enterprise network. He is concerned about applying updates that he has not tested with the company's proprietary software, or are not necessary.

Which of the following features of the Software Update Service (SUS) would allow Craig to test and limit the updates available to the computers on the network?

1. Scheduled updates
2. Background installation
3. Active Directory integration
4. On-site SUS server <Correct>

Explanation:
Setting up an on-site SUS server would give Craig the ability to control which updates are available to the computers on the network, allowing only tested and necessary updates to be applied.

Background installation alone would not allow the available updates to be controlled.

Active Directory integration alone would not allow the necessary control of which updates are available on the network.

The scheduled updates option of SUS would not control which updates are being installed.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Install and configure software update infrastructure. - Install and configure software update services.

References:
Software Update Services Overview White Paper
TechNet, Microsoft
Link: http://www.microsoft.com/windows2000/docs/SUSOverview.doc>
You are the administrator for a company. You log on to ComputerB running Microsoft Windows Server 2003 as a member of the Power Users group. You need to perform administrative tasks for which you do not have permissions. You enter the command runas /user:joeb@ComputerB "cmd27.exe" to run a proprietary administrative application. The command does not work.

What could be the cause of the problem?

1. Members of the Power Users group do not have permission to run the runas command.
2. The joeb account does not have permission to run the runas command.
3. The Administrator account does not have permission to run cmd27.exe.
4. The joeb account does not have permission to run cmd27.exe. <Correct>

Explanation:
Since cmd27.exe is a proprietary administrative application, you will likely need to have Administrator account privileges to run it. The joeb account is not likely to have such privileges. It is likely to have minimal privileges, such as those provided to members of the Users group.

The runas command does not require any special permission to run. Members of the Power Users group should be able to run the command.

Since the runas command does not require special permissions, the joeb account should also be able to run it.

The Administrator account should have sufficient privileges to run this application. The Administrator account usually has the highest-level privileges of all user accounts.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Implement secure network administration procedures. - Implement the principle of least privilege.

References:
Runas command
Windows Server 2003 Help, Microsoft
You are the network administrator for your company's Active Directory network. The servers in your organization are running Microsoft Windows Server 2003. The client computers are almost all running Microsoft Windows XP Professional and Microsoft Windows 2000 Professional. You have a few Microsoft Windows 98 computers left on the network.

You have installed Software Update Services on one of your Windows Server 2003 computers. You have configured this server to download Windows Updates and make them available to all of the clients on the network.

From the list on the right, select the steps that are necessary to be able to configure the client computers to use Software Update Services. Place your selections in the list on the left by clicking the items in the list on the right and clicking the arrow button. You may not need to use all of the items from the list on the right.

Explanation:
In this scenario, you must provide Windows Updates for all of the client computers that run Windows XP Professional, Windows 2000 Professional, and Windows 98. The Windows XP client computers already have an automatic update property sheet that can be used to connect to the SUS server to retrieve updates. The only thing that you would have to do to them is install Service Pack 1. After SP1 is installed, a GPO can be used to configure the automatic update settings.

The Windows 2000 Professional computers need wuau22.msi installed. This is the client software for the Software Update Services. To install wuau22.msi, Service Pack 3 must be installed first. After SP3 is installed, you could use a GPO to deploy the client software.

The Windows 98 computers do not support the automatic update through SUS. You must manually perform the updates from Microsoft's Web site.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objectives:
Install and configure software update infrastructure. - Configuring software updates on legacy operating systems.

References:
Software Update Services
TechNet, Microsoft

Software Distribution Overview
TechNet, Microsoft

Software Update Services Deployment White Paper
TechNet, Microsoft
Brian is the administrator for a medium-sized network. He is concerned about unnecessary and potential conflicting updates being installed through Microsoft's Windows Update Web site.

What is the simplest method that Brian can receive and apply updates and patches to his users' computers only after he has tested them?

1. Send an e-mail to all users instructing them to use the automatic updates feature on their computers once per week.
2. Install and configure Software Update Services. **<Correct>**
3. Have the administrators run the automatic updates feature on each user's computer every week.
4. Schedule the task manager on each user's computer to run a script that points to downloaded updates.

**Explanation:**
Installing and configuring Software Update Services will allow Brian to both mandate and control the applying of patches and updates.

Scheduling the task manager on each user's computer to run a script that points to downloaded updates could be configured to work, but it would not be the simplest method of improving consistency.

Having the administrators run the automatic updates feature on each user's computer every week would not be the simplest method of improving consistency.

Sending an e-mail to all users instructing them to use the automatic updates feature on their computers once per week would not be practical. There would be no way to verify that the proper updates had been applied.

**Objective:**
Implementing, Managing, and Maintaining Network Security

**Sub Objective(s):**
Install and configure software update infrastructure. - Install and configure software update services.

**References:**
Software Update Services Overview White Paper
TechNet, Microsoft
Link: http://www.microsoft.com/windows2000/docs/SUSOverview.doc>
You are the administrator for your company's network. You have computers on the network running the following operating systems: Microsoft Windows Server 2003, Microsoft Windows 2000 Server Service Pack 2, Microsoft Windows 2000 Professional Service Pack 1, Microsoft Windows NT 4.0 Workstation Service Pack 4, and Microsoft Windows NT 4.0 Server Service Pack 5.

Which task do you need to perform before you can use Automatic Updates with Software Update Services (SUS) for these computers?

1. Install Service Pack 6 on the computers running Windows NT 4.0 Workstation Service Pack 4.

Explanation:
The Windows Server 2003 operating system natively supports SUS and does not require any additional service packs to be installed prior to installing SUS.

Windows 2000 Server Service Pack 3 does not require any updates to be able to use SUS.

Windows 2000 Server Service Pack 2 does require an update prior to using SUS.

Windows 2000 Professional Service Pack 2 does require an update prior to using SUS.

Windows NT 4.0 Workstation is not supported by SUS.

Windows NT 4.0 Server is not supported by SUS.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Install and configure software update infrastructure. - Configuring software updates on legacy operating systems.

References:
Software Update Services Overview White Paper
TechNet, Microsoft
Chapter: Client-Side Automatic Updates Pages: 7 - 15
As an administrator for an organization, you are responsible for configuring the infrastructure to deploy critical and security updates to desktop and server clients. A systems engineer has already created a software update infrastructure plan. You are tasked with implementing this plan. You must ensure that all client software updates are deployed. The plan calls for maximum administrative control over the downloading, testing, and monitoring of software updates from the Windows Update server.

Which group of tasks should you choose?

1. Configure the update files to be hosted on the Windows Update server. Configure the selection and approval of content prior to publishing to Automatic Updates clients. Configure the monitoring of the Software Updates Services server and logs.

2. Configure the update files to be hosted locally on your server running Software Update Services. Configure the synchronization of approved content to additional servers. Configure the monitoring of the Software Updates Services server and logs. <Correct>

3. Configure the update files to be hosted locally on your server running Software Update Services. Configure the selection and approval of content prior to publishing to Automatic Updates clients. Configure the monitoring of the Software Updates Services server and logs.

4. Configure the update files to be hosted on the Windows Update server. Configure the synchronization of approved content to additional servers.

Explanation:
To achieve maximum administrative control over the process of downloading and installing updates from the Windows Update server, you should download the updates to a local server first. Then you should use the local server to host updates to Automatic Updates clients.

Using the Windows Update server to host update files will give you less control over the process.

To achieve even more control and efficient distribution of updates, you can use additional servers to host the updates by synchronizing content with the local server that first downloaded the updates.

You should evaluate and approve the updated files prior to distributing them to other servers on the network. This will give you a greater confidence in the updates, causing minimal impact to the operation of your network and the applications running on it.

To track the downloading and success or failure of updates, you should configure monitoring of the Software Updates services servers and logs. You can access the data collected in the logs by using a Web server configured with Internet Information Services (IIS) 6.0 with Internet Explorer 5.5 or later.

Objective:
Implementing, Managing, and Maintaining Network Security

Sub Objective(s):
Install and configure software update infrastructure. - Install and configure software update services.

References:
Software Update Services Overview White Paper
TechNet, Microsoft
Server-Side Software Update Services

Software Update Services
Windows Server 2003 Help, Microsoft
Chapter: 4 Pages: 68 - 70