Exam : **070-214**

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

Version : DEMO

1. You are the network administrator for your company. Your network consists of a Windows 2000 Active Directorydomain. 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 /fixcommand 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 onthe 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 theswitch that prevents a restart. Run the netdiag /v /fix command on the intranet Web server. Restart the intranet Webserver.

D. Run the qfecheck.exe command on the intranet Web server. Apply the hotfixes to your intranet Web server with theswitch that prevents a restart. Run the qfecheck.exe command on the intranet Web server. Restart the intranet Web server.
Answer: B

2. You are the network administrator for your company. 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 ServerA, and the other server is configured as an intranet Web server. In addition, thenetwork contains 50 Windows XP Professional client computers. All but five of the client computers receive scheduled automatic updates. The five client computers that are not updatedautomatically are on an isolated LAN segment that is not connected to the Internet. The client computers on the isolatedLAN have access to ServerA 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 ServerA.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 ServerA.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. Sharethis 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 on the intranet Web server. Run the Windows Update service on the client computers on the isolated LAN.
Answer: B

3. You are the network administrator for your company. Your network consists of a Windows 2000 Active Directory domain. Your company 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 ServerC, 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 ServerC. Your company 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 Client1. You install and configure all the custom applications and the latest service pack on Client1. 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 Client1. Save that
Answer file as Risetup.sif and associate it with the CD-based RIS image on ServerC. 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 ServerC. Slipstream the latest service pack to that folder. Create a new RIS image from that folder. Run the riprep command on Client1 to create a new image on ServerC. 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

4. You are the network administrator for your company. The network consists of a Windows 2000 Active Directory domain. The domain contains 100 Windows 2000 Server computers, 5,000 Windows 2000 Professional computers, and1,000 Windows XP Professional computers. The computer accounts for all servers are located in an organizational unit (OU) named Servers. The computer accountsfor 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 aMicrosoft Windows Installer package. You need to ensure that all Windows 2000 Professional computers receive the service pack. The service pack must not bedeployed 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 tothe WinXP OU.

B. Create a child OU named Win2000 under the Desktops OU. Move all Windows 2000 Professional computer accountsto the Win2000 OU.

C. Create a Group Policy object (GPO) named W2KSP. In the user configuration section of W2KSP, publish the servicepack 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: BDG

5. You are the network administrator for your company. 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 SecurityAnalyzer (MBSA) to verify the status of hotfixes and security-related settings of computers in the domain. You haveinstalled 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

6. You are the administrator of a regional office LAN on your company network. The network consists of a Windows 2000 Active Directory domain. All computers on your company's network are using either Windows 2000 Professional or Windows 2000 Server. Your company 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: CD

7. You are the network administrator for your company. 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 2000Server computer is configured as a file server. The network also contains 1,500 Windows 2000 Professional clientcomputers. You use a Group Policy object (GPO) named SPDeploy to deploy a new service pack. SPDeploy is linked to the ClientsOU. 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 computerhas 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 Group 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 that 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

8. You are the network administrator for your company. The network consists of a Windows 2000 Active Directory domain. 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 ServerA, several error messages appear that report checksum differences in third-party device driver files. However, the versions of the device driver files on ServerA are the same. You suspect that a malicious administrator has replaced some of the device driver files on ServerA. 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

9. You are the network administrator for your company. The network consists of a Windows 2000 Active Directory domain. Your company 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

10. You are a network administrator for a branch office of your company. 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

11. You are the administrator of a Windows 2000 Server computer named ServerA. ServerA is a file server used by all company employees.One morning, users report that more than 500 files are missing from ServerA. You examine the audit log on ServerA anddiscover that the files were deleted by a former employee named Bruno, who was recently fired. Many deleted files arenew and are not contained on any backup tapes. Your legal department instructs you to preserve the evidence of Bruno's access to ServerA. You need to ensure that asmany deleted files as possible can be restored by using a disk sector editor. You also need to allow employees to accessthe remaining files. What should you do?

A. Remove ServerA from your network. Create an exact image of ServerA'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:A

12. You are the administrator of your company's Web server named ServerA. ServerA runs Windows 2000 Server andInternet Information Services (IIS). ServerA provides services to Internet users and is connected directly to the Internet. During the afternoon, ServerA stops responding to requests from Internet users. You restart the server, and it appears towork normally. Three hours later, the server again

stops responding to requests from Internet users. You run thenetstat.exe command and discover thousands of TCP connections in a half-open state. The Web services running on ServerA will function correctly only if ServerA is connected directly to the Internet. Youneed to make ServerA 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 ServerA.

C. Configure ServerA to accept connections only on port 80.

D. Modify the server's registry to decrease the SYN_ACK timeout.
Answer: D

13. You are the network administrator for your company. The network consists of a Windows 2000 Active Directory domain. The Web developers in your company 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 your company. A developer reports that his computer becomes infected with a virus every time he uses the computer at home. Your company'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

14. You are the network administrator for your company. 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

15. You are the network administrator for your company. The network consists of a Windows 2000 Active Directorydomain. 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 2000domain controllers. All users use their domain user account to log on to the network from Windows 2000 Professionalclient computers in the domain.In the Default Domain Controllers Policy Group Policy object (GPO), you enable the Audit logon events policy to logsuccessful 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 clientcomputers. You want to ensure that all logon and logoff events are recorded in the event logs on the 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

16. You are the network administrator for your company. The network consists of a Windows 2000 Active Directorydomain. The network also contains 1,500 Windows 2000 Professional client computers. The written security policy for your company requires that failed domain logon attempts be tracked. You enable failureauditing on the Audit logon events setting in the Domain Controller Security Policy. You then use the Terminal Services client to connect to ServerA 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. Youexamine the Security log on ServerA 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 for 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

17. You are the network administrator for your company. 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 folders 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 from 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: BE

18. You are the network administrator for your company. 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 company employees.

You will soon add four more dial-up servers to handle the demand for dial-up services. The written security policy for your company 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 spendmaintaining dial-up logs.What should you do?

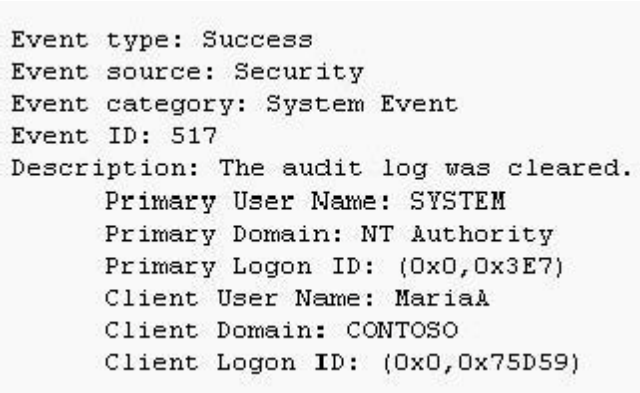
A. Enable auditing on each dial-up server. Configure the Security log on each dial-up server to be 20 MB in size and to never overwrite events. Save each Security log to an archived location every day.

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

19. You are the network administrator for your company. You manage three Windows 2000 Server computers. Two of these servers are configured as domain controllers, and the other is a member server named ServerA. ServerA's computer account is in 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 the company requires you to back up and clear the logs on ServerA monthly. To back up and clear the event logs, you log on as BrunoA@contoso.com. As you are archiving the Security log on ServerA, you notice that the log has fewer events than usual. The first entry in the audit log is shown in the exhibit.



You must ensure that company policy is enforced. What should you do first?

A. On ServerA, 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 MariaA from all groups that allow administrative access to ServerA.

D. Configure Audit Policy of the GPO linked to Secure to Audit privilege use for the administrators group.

E. Configure the System group for Read only permission to Systemroot\System32\Config folder on ServerA.
Answer: C

20. You are the network administrator for your company. The network consists of a Windows 2000 Active Directorydomain. The domain is configured to audit logon events. Maria is a user in the company sales department. On Monday, Maria 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
   Reason: Unknown user name or bad password
   User Name: MARIA                Domain: CONTOSO
   Logon Type: 3                   Logon Process: NETLOGON
   Authentication Package: NTLM    Workstation Name: CLIENT1
```

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 Client1.

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 Client1.
Answer: B