ch02

True/False
Indicate whether the statement is true or false.

____ 1. Microsoft recommends creating separate forests rather than domains to keep your environment secure from rogue administrators and various other threats.

____ 2. The servers may experience some impact on performance because of the High Security settings.

____ 3. The Domain Controller template requires a baseline group policy, making it similar in concept to a member server baseline policy.

____ 4. Applying the High Security-Bastion Host.inf security template makes remote management of the bastion host easier.

____ 5. Security settings can be used with administrative templates in Group Policy to restrict the settings users can change.

Multiple Choice
Identify the choice that best completes the statement or answers the question.

____ 6. A(n) ____ is the management boundary of Active Directory.
a. forest
b. domain
c. organizational unit
d. user directory

____ 7. ____ are Active Directory containers where users, groups, computers, and other organizational units can be placed.
a. Forests
b. Domains
c. Organizational units
d. User directories

____ 8. Security templates are what kind of files?
a. Text files
b. Zip files
c. pdf files
d. tar files

____ 9. The High Security environment is the highest lockdown level. The High Security settings are designed to work in an Active Directory domain with member servers and domain controllers running ____.
a. Windows 98 SE
b. Windows NT 4.0
c. Windows Server 2003
d. All of the above

____ 10. The recommended security template for bastion hosts is ____.
a. Legacy Client
b. Enterprise Client
c. High Security
d. Medium Security

____ 11. What is the first step in securing an environment?
a. Formulate the Active Directory design plan
b. Look at server roles
c. Create a security template for the various types of servers
d. Establish a baseline member server

____ 12. ____ are performed by the domain controller.
a. Web services
b. NLA services
c. Directory searches
d. Print services

____ 13. ____ is a network infrastructure service.
a. WebDAV
b. DHCP
c. ASP.NET
d. GPO

____ 14. ____ should be put into place for securing DHCP.
a. Disabling the DFS service
b. Enabling the SMB packet digital signing
c. Watching for an unusual number of lease requests from clients
d. Disabling the FRS service

____ 15. ____ can be prevented by enabling the SMB packet digital signing.
a. File transfers
b. The print process
c. Viewing the print queue
d. Access to Internet

____ 16. A(n) ____ is a publicly accessible computer located on the perimeter network.
a. bastion host
b. file server
c. IAS server
d. domain controller

____ 17. When a member server baseline policy is established, all unneeded services and executable files are disabled or removed. In order to add Web server functionality to an IIS server, the ____ must be enabled.
a. HTTP SSL service
b. TCP/IP NetBIOS Helper service
c. Remote Registry service
d. All of the above

____ 18. The ____ turns off unnecessary features to better protect the server from attackers. It provides templates for IIS-dependent Microsoft products such as Microsoft Exchange 5.5 and 2000.
a. bastion host
b. IIS Lockdown tool
c. NAT-T
d. DHCP

____ 19. In the standard edition of Windows Server 2003, what is the maximum number of remote RADIUS server groups that IAS can have?
a. 2
b. 10
c. 50
d. Unlimited

____ 20. Connection Manager can be used to customize a self-installing service in order to reduce support. It would most likely be used with ____.
a. desktop computers
b. E-mail computers
c. mobile or laptop computers
d. kiosks

____ 21. ____ should be tightly configured and have no direct connections to internal networks.
a. Kiosks and e-mail computers
b. Palmtops
c. Desktops
d. Mobile or laptops

____ 22. A(n) ____ allows access to sites that are not included in other zones.
a. Internet zone
b. local intranet zone
c. Trusted zone
d. Restricted zone

____ 23. The local intranet zone ____.
a. is allowed to perform only minimal, safe operations
b. consists of sites corresponding to business partners
c. consists of sites with a firewall or those specified to bypass the proxy server
d. consists of sites that are not included in other zones

____ 24. Group Policy administrative templates define how the policy settings appear. The .adm files are administrative templates. What information does an .adm file contain?
a. Registry location that corresponds to the setting
b. An explanation of what the setting does
c. The versions of Windows that is supported by the setting
d. All of the above

____ 25. ____ store directory data for Active Directory and manage communication between users and domains.
a. File servers
b. Domain controllers
c. IIS servers
d. Bastion hosts

____ 26. ____ contains policy settings to configure Windows Update. It is loaded by default in Windows 2000 Service Pack 3 (SP3), XP Service Pack 1 (SP1), and Server 2003.

a. Wuau.adm
b. System.adm
c. Wmplayer.adm
d. Conf.adm

Completion

Complete each statement.

27. The _____ is the lowest lockdown level of security for baseline templates.
28. Computers running the Microsoft DHCP service offer dynamic configuration of _____ and related information to DHCP-enabled clients on your network.
29. To provide multiple layers of protection against attackers, URLScan has been integrated into the _____.
30. The _____ is used to override the user-based Group Policy with the computer-based Group Policy.
31. _____ enable administrators to configure the behavior and appearance of the desktop, including the operating system, components, and applications. They can be used with administrative templates in Group Policy to restrict the settings users can change.

Matching

Match each term with the correct statement below.

a. NNTP server
b. Domain
c. Bastion host
d. Internet zone
e. EFS
f. Organization unit
g. SMTP
h. WLAN
i. File server

____ 32. Allows portable computers to access network connections from any point where the organization has wireless access points
____ 33. Used to protect files
____ 34. Used for newsgroup postings
____ 35. A publicly accessible computer located on a perimeter network
____ 36. Administrative unit that groups together various capabilities for management convenience
____ 37. Provides services for applications that require protocols such as NetBIOS, SMB (Server Message Block), and CIFS (Common Internet File System)
____ 38. Allows access to sites that are not included in other zones. By default, it is set to the medium security level
____ 39. Active Directory containers where users, groups, computers, and other organizational units can be placed
____ 40. Used to store and forward electronic mail

Short Answer

41. List and explain briefly the elements that require careful planning for the organization's security structure.
42. Briefly describe the three categories in which the environment needs of an organization fall.
43. What are the various server roles on a network?
44. Explain the server role as a domain controller.

45. How can running a DHCP service cause issues for the network?
46. What are the changes that should be made to the baseline server template for servers that will run DHCP?
47. What are the various considerations for securing print servers?
48. What is a bastion host? List some of the most common uses for a bastion host.
49. What is zone security? List and explain briefly four zones that can be configured for security.
50. Explain the concept of software restriction policies. What are the various rules that act as valid exceptions to this default security level?

ch02
Answer Section

TRUE/FALSE

1. ANS: T PTS: 1 REF: 28
2. ANS: T PTS: 1 REF: 30
3. ANS: T PTS: 1 REF: 33
4. ANS: F PTS: 1 REF: 44
5. ANS: T PTS: 1 REF: 53

MULTIPLE CHOICE

6. ANS: B PTS: 1 REF: 28
7. ANS: C PTS: 1 REF: 28
8. ANS: A PTS: 1 REF: 29
9. ANS: C PTS: 1 REF: 30
10. ANS: C PTS: 1 REF: 31
11. ANS: A PTS: 1 REF: 31
12. ANS: C PTS: 1 REF: 32
13. ANS: B PTS: 1 REF: 38
14. ANS: C PTS: 1 REF: 39
15. ANS: C PTS: 1 REF: 41
16. ANS: A PTS: 1 REF: 43
17. ANS: A PTS: 1 REF: 46
18. ANS: B PTS: 1 REF: 47
19. ANS: A PTS: 1 REF: 49
20. ANS: C PTS: 1 REF: 51
21. ANS: A PTS: 1 REF: 52
22. ANS: A PTS: 1 REF: 53
23. ANS: C PTS: 1 REF: 53
24. ANS: D PTS: 1 REF: 55
25. ANS: B PTS: 1 REF: 32
26. ANS: A PTS: 1 REF: 56

COMPLETION

27. ANS: Legacy Client

    PTS: 1 REF: 29
28. ANS: IP addresses

    PTS: 1 REF: 38
29. ANS: IIS Lockdown Wizard

PTS: 1 REF: 47

30. ANS: Loopback policy

PTS: 1 REF: 52

31. ANS: Security settings

PTS: 1 REF: 53

MATCHING

32. ANS: H PTS: 1 REF: 52
33. ANS: E PTS: 1 REF: 51 | 61
34. ANS: A PTS: 1 REF: 44 | 61
35. ANS: C PTS: 1 REF: 43 | 60
36. ANS: B PTS: 1 REF: 28 | 60
37. ANS: I PTS: 1 REF: 40 | 61
38. ANS: D PTS: 1 REF: 53 | 61
39. ANS: F PTS: 1 REF: 28 | 61
40. ANS: G PTS: 1 REF: 44 | 62

SHORT ANSWER

41. ANS:
Careful planning of the following elements is needed:
    1. Domains: Domains are administrative units that group together various capabilities for management convenience.
    2. Forests: Forests are one or more Active Directory domains that share a schema and global catalog.
    3. Organizational units: Organizational units are Active Directory containers where users, groups, computers, and other organizational units can be placed.

PTS: 1 REF: 28

42. ANS:
    1. Legacy Client: It is the lowest lockdown level. The Legacy Client settings are designed to work with member servers and domain controllers running Windows Server 2003, and clients running Microsoft Windows 98,Windows NT 4.0, and later versions of Windows operating systems.
    2. Enterprise Client: It is designed to provide solid security for the organization. It allows use of more restrictive security templates for added security. The Enterprise Client settings are designed to work with only Windows Server 2003, Windows 2000 Professional, and Windows XP Professional computers.
    3. High Security environment: It is the highest lockdown level and it allows use of very restrictive security templates for added security. The High Security settings are designed to work with only Windows Server 2003, Windows 2000, Windows XP, and later.

PTS: 1 REF: 29-30

43. ANS:
    1. Domain controller
    2. Member server
    3. Infrastructure server

4. File server
5. Print server
6. Bastion host
7. IIS server
8. IAS server

PTS: 1 REF: 32

44. ANS:
Domain controllers store directory data for Active Directory and manage the communication between users and domains. This includes functions such as user logon processes, authentication, and directory searches. Due to the services it provides, the domain controller server role is one of the most important roles to secure in any environment with computers running Microsoft Windows Server 2003 and running Active Directory services. Any loss or compromise of a domain controller in the environment could be devastating to clients, other servers, and other devices or applications that rely on the domain controller for authentication and services.
The Domain Controller template requires a baseline group policy, making it similar in concept to a member server baseline policy. However, the policy is linked to the Domain Controllers OU; therefore, it takes precedence over the Default Domain Controllers policy.

PTS: 1 REF: 32-33

45. ANS:
Computers running the Microsoft DHCP service offer dynamic configuration of IP addresses and related information to DHCP-enabled clients on the network. This can present issues on the network. Because DHCP is an unauthenticated protocol, a user can connect to the network without providing credentials. An unauthenticated user can then obtain a lease from any available DHCP server. Any option values that the DHCP server provides with the lease, such as WINS server or DNS server IP addresses, are available to the unauthenticated user. Malicious users with physical access to the DHCP-enabled network can initiate a denial of service attack by requesting numerous leases from the server, thereby depleting the number of leases that are available to other DHCP clients.

PTS: 1 REF: 38

46. ANS:
There are several changes that should be made to the baseline server template for servers that will run DHCP. They are:

- For a client to obtain an IP address configuration, the DHCP service must be running. Group Policy should be used to secure and set the service to grant access solely to server administrators.

- Event Viewer entries for the DHCP service are limited to startup and shutdown events; therefore,DHCP logging should be configured so that a more detailed log is available. Limit access to these logs to server administrators.

- Use the 80/20 rule by splitting DHCP server scopes between servers so that 80% of the addresses are distributed by one DHCP server and 20% by another.

- Rename the Administrator and Guest accounts, change their passwords to be more complex, and use different names and passwords on each server. You may want to disable the Guest account instead of just renaming it, especially if there is no need to use the account.

- Enhance the level of security on servers by using IPSec filters to block unnecessary ports.

PTS: 1 REF: 39-40

47. ANS:

- Under Security Options the option Microsoft network server: Digitally sign communications (always) can be enabled. This setting determines whether packet signing is required by the SMB server component. SMB packet digital signing is used to prevent man-in-the-middle attacks. It is disabled by default but it can be enabled for servers in a High Security environment. Enabling this setting allows users to print, but not view, the print queue. Users attempting to view the print queue will receive an access denied message.

- Any unneeded services or executable files should be disabled or removed to eliminate a potential point of attack. The Print Spooler service must be enabled because it manages all local and network print queues and controls all print jobs. It is the center of the Windows printing subsystem and communicates with printer drivers and I/O components.

Secure well-known accounts on print servers by following the same procedures that are used for a file server.

- Never configure a service to run under the security context of a domain account unless absolutely necessary.

- Internet Protocol Security (IPSec) filters can provide an effective means for enhancing the level of security required for servers. Block ports by using IPSec filters.

PTS: 1 REF: 41-42

48. ANS:

A bastion host is a publicly accessible computer located on the perimeter network, also referred to as the DMZ (demilitarized zone), or screened subnet. Although in most situations the DMZ would have some type of firewall or filtering router on each interface into the DMZ, sometimes bastion hosts are unprotected by a firewall or filtering router, leaving them highly exposed to attacks. They must be secured as much as possible to maximize their availability and yet minimize the chance of their being compromised. Because they are so vulnerable, the design and configuration of bastion hosts must be carefully thought out to reduce the chances of an attack being successful. The most secure bastion host servers limit access to only highly trusted accounts and enable the fewest services possible necessary to fully perform their functions.

Some of the most common uses for bastion hosts include:

1. Web servers
2. Domain Name Systems (DNS) servers
3. File Transfer Protocol (FTP) servers
4. Network News Transfer Protocol (NNTP) servers

PTS: 1 REF: 43-44

49. ANS:

Zone security is a method that enables you to divide online Web content into groups or zones. Specific Web sites can then be assigned to each zone, depending on the degree to which the content of each site is trusted. The Web content can be anything from an HTML or graphics file to a Microsoft ActiveX control, Java applet, or executable file. Depending on the role of the computer, it may need more or less in the way of Internet security configuration. This will depend on the types of Web sites that you want to allow your users to access. You can configure the following four zones for security:

1. Internet zone: An Internet zone allows access to sites that are not included in other zones. You cannot add sites to this zone. By default, it is set to the medium security level.
2. Local intranet zone: A local intranet zone consists of sites with a firewall or those specified to bypass the proxy server. By default, it is set to the medium security level.

3. Trusted zone: A Trusted zone is intended for sites that can be trusted to never cause harm, such as those of business partners. By default, it is assigned the low security level.
4. Restricted: A Restricted zone is allowed to perform only minimal, safe operations because the content is questionable. By default, it is assigned the high security level.

PTS: 1 REF: 53-54

50. ANS:
Software restriction policies are used to maintain more granular control over who receives what software. Software restriction policies specify the software that is allowed to run. Some of the features include controlling which programs can run on a computer, permitting users to run only specific files on multiple-user computers, and preventing any files from running on a local computer, OU, site, or domain in case of a virus infection. Software restriction policies provide a policy-based method to enforce decisions about whether the software can run, thereby forcing users to follow the parameters that are set by administrators. Software restriction policies are not meant to replace antivirus software.
Following rules act as valid exceptions to this default security level:
1. Hash rules
2. Certificate rules
3. Path rules
4. Internet zone rules

PTS: 1 REF: 57-58