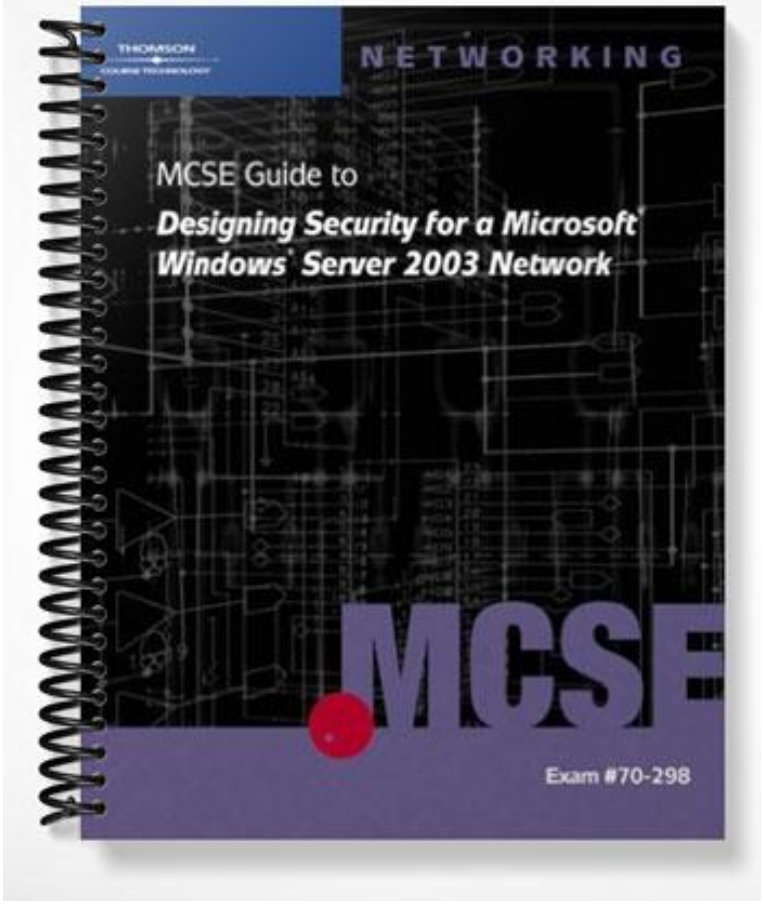
TEST BANK


THOMSON
COURSE TECHNOLOGY
NETWORKING
MCSE Guide to
Designing Security for a Microsoft Windows Server 2003 Network
MCSE
Exam #70-298

ch02

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

____ 1. The Security Configuration and Analysis snap-in can be used to configure local and remote computers.

____ 2. The three areas in local policies are Audit Policy, User Rights Assignment, and Security Options.

____ 3. Group policies are applied to three types of Active Directory objects: users, computers, and networks.

____ 4. The IIS role is one of the most vulnerable server roles due to its inherent exposure to the Internet.

____ 5. Group Policy provides the easiest way to apply security settings in an Active Directory domain.

Modified True/False
Indicate whether the statement is true or false. If false, change the identified word or phrase to make the statement true.

____ 6. In Windows Server 2003 security is set to the fewest possible permissions. _____

____ 7. The Secure template requires NTLM v5. _____

____ 8. Group policy is passed down from child to parent object within the domain. _____

____ 9. Desktop configurations, Internet Explorer settings, and security settings can all be configured using Group Policy. _____

____ 10. The most common threats to DCs are those that attempt to gain access to the security database on a DC. _____

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

____ 11. Which of the following is the baseline security template?
a. rootsec.inf
b. secure*.inf
c. Setup security.inf
d. DC security.inf

____ 12. If you want to apply the securews.inf security template to a client computer, you must ensure that all DCs that contain user accounts that might be accessed through the client computer are running _____ or later.
a. Windows NT 4.0 Service Pack 3
b. Windows NT 4.0 Service Pack 4
c. Windows 2000 Service Pack 3
d. Windows XP

____ 13. If a server is configured to use the hisec*.inf template, all clients must use _____ packet signing.
a. SMB
b. NTLM
c. LM
d. LDAP

____ 14. What is the recommended way to customize security templates?
a. Make changes directly to the predefined security template.
b. Use the Save As command to save a copy of a predefined template, then modify the copy.
c. Use the Copy command to create a copy of a predefined security template, then modify the copy.
d. Use the New command to create a blank security template, then add the settings.

____ 15. What is the order of precedence for application of group policies?

a. domain, local computer, OU
b. domain, OU, local computer
c. local computer, OU, domain
d. OU, domain, local computer

____ 16. The _____ Policies in the predefined security templates allows the administrator to modify settings related to system services such as startup, shutdown, indexing, license logging, and many more.
a. System Services
b. Event Log
c. Restricted Groups
d. Local

____ 17. Which of the following groups of nodes is listed under each GPO in the Active Directory Users and Computers console?
a. Software Settings, Hardware Settings, and Local Settings
b. Software Settings, Windows Settings, and Administrative Templates
c. Security Templates and Administrative Templates
d. Windows Settings, Security Settings, and Registry Settings

____ 18. Which MMC snap-in would you use to compare the current security configuration on a computer with another configuration?
a. Active Directory Users and Computers
b. Security Configuration and Analysis
c. Resultant Set of Policy
d. Security Extensions to Group Policy

____ 19. Which switch to the secedit command is used to create a snapshot of the current configuration values that can later be used to undo changes?
a. export
b. snap
c. generaterollback
d. generateundo

____ 20. The ____.exe is used to refresh Group Policy settings, including security settings.
a. gpupdate
b. gprefresh
c. refreshgp
d. gp

____ 21. Which server role typically authenticates domain logons and maintains the security policy as well as the master database for the domain?
a. Terminal server
b. Remote access/VPN server
c. Domain controller
d. DHCP Server

____ 22. Which version of the IP security protocol should be installed on POP3 servers?
a. 3
b. 6
c. 9
d. 11

____ 23. A _____ attack occurs when someone captures DNS zone data in order to reverse engineer your DNS structure.
a. denial-of-service
b. data modification
c. redirection
d. footprinting

____ 24. Securing file, print, and member servers is simplified in Windows Server 2003 because _____ is no longer installed by default on these computers.
a. DNS
b. IIS
c. WINS
d. DHCP

____ 25. A server with the _____ role typically runs the Indexing Service and Remote Storage.
a. IIS
b. Application server
c. File server
d. Print server

____ 26. Which security templates should be applied to servers with infrastructure services roles?
a. Setup security.inf (default), secure*.inf, hisec*.inf, compat*.inf
b. Setup security.inf (default), secure*.inf, compat*.inf
c. Setup security.inf (default)
d. Setup security.inf (default), secure*.inf, hisec*.inf

Yes/No
Indicate whether you agree with the statement.

____ 27. Should NTFS be used to secure the data storage for a streaming media server?

____ 28. In Windows Server 2003, are modifications to security templates usually made to tighten default security settings?

____ 29. Does Microsoft recommend applying security templates to sites, domains, and OUs?

____ 30. Is there a security template that allows end users to have appropriate permissions to run noncertified applications and still not grant the full permissions granted to Power Users?

____ 31. Should an administrator modify the predefined templates provided in Windows Server 2003?

Completion
Complete each statement.

32. The _____ security template is used for setting very high security between computers for network communications.

33. In Terminal Server, the _____ security setting is used when legacy applications accessed through Terminal Server require access to the Registry.

34. Settings for passwords, account lockout, and Kerberos are defined in _____ policies.

35. When securing an IIS server, one security measure you can take specific to IIS servers is to place content on a dedicated _____.

36. DHCP servers manage a set of DHCP addresses, called a(n) _____, and assigns addresses to computers in a dynamic fashion.

Matching

Match each item with a statement below.

a. Security Extensions to Group Policy
b. DC
c. secedit.exe
d. RSoP
e. setup security.inf
f. Hfnetchk.exe
g. firewall
h. secure*.inf
i. DNS

____ 37. software and hardware interface that prevents unauthorized access to internal networks from external locations by means of filtering and routing
____ 38. command-line tool used to analyze, configure, and export system security settings
____ 39. service that provides the means for computers, users, and applications to resolve names to IP addresses
____ 40. default security template
____ 41. server that controls activities on the domain
____ 42. used to define security configurations for various users, groups, or computers within a GPO
____ 43. allows you to see the results of the policies applied to a particular computer
____ 44. secure security template
____ 45. command-line tool that analyzes Windows computers and reports any missing security updates

Short Answer

46. If a strong password policy is set, what are the criteria that user passwords must meet?
47. Describe the function of the Restricted Groups node of the security templates.
48. Describe the use of the analyze switch to secedit.
49. List at least six of the server roles identified by Microsoft Windows Server 2003.
50. What are some of the steps you can take to secure an IIS server?

ch02
Answer Section

TRUE/FALSE

1. ANS: F PTS: 1 REF: 51
2. ANS: T PTS: 1 REF: 69
3. ANS: F PTS: 1 REF: 96
4. ANS: T PTS: 1 REF: 112
5. ANS: T PTS: 1 REF: 133

MODIFIED TRUE/FALSE

6. ANS: T PTS: 1 REF: 53
7. ANS: F, v2

   PTS: 1 REF: 59
8. ANS: F, parent to child

   PTS: 1 REF: 70
9. ANS: T PTS: 1 REF: 76
10. ANS: T PTS: 1 REF: 107

MULTIPLE CHOICE

11. ANS: C PTS: 1 REF: 52
12. ANS: B PTS: 1 REF: 58
13. ANS: A PTS: 1 REF: 61
14. ANS: B PTS: 1 REF: 67
15. ANS: D PTS: 1 REF: 70
16. ANS: A PTS: 1 REF: 72
17. ANS: B PTS: 1 REF: 81
18. ANS: B PTS: 1 REF: 86
19. ANS: C PTS: 1 REF: 93
20. ANS: A PTS: 1 REF: 95
21. ANS: C PTS: 1 REF: 107
22. ANS: B PTS: 1 REF: 117
23. ANS: D PTS: 1 REF: 121
24. ANS: B PTS: 1 REF: 123
25. ANS: C PTS: 1 REF: 129
26. ANS: D PTS: 1 REF: 131

YES/NO

27. ANS: Y PTS: 1 REF: 128

28. ANS: N PTS: 1 REF: 129
29. ANS: Y PTS: 1 REF: 136
30. ANS: Y PTS: 1 REF: 57
31. ANS: N PTS: 1 REF: 66

COMPLETION

32. ANS: hisec*.inf

    PTS: 1 REF: 59
33. ANS: relaxed

    PTS: 1 REF: 63
34. ANS: Account

    PTS: 1 REF: 67
35. ANS: volume

    PTS: 1 REF: 114
36. ANS: scope

    PTS: 1 REF: 120

MATCHING

37. ANS: G PTS: 1 REF: 117
38. ANS: C PTS: 1 REF: 51
39. ANS: I PTS: 1 REF: 120
40. ANS: E PTS: 1 REF: 53
41. ANS: B PTS: 1 REF: 106
42. ANS: A PTS: 1 REF: 51
43. ANS: D PTS: 1 REF: 82
44. ANS: H PTS: 1 REF: 54
45. ANS: F PTS: 1 REF: 51

SHORT ANSWER

46. ANS:
    At least seven characters
    Does not contain username, real name, company name
    Does not contain complete dictionary word
    Is different from previous passwords
    Contains characters from four groups:
      Uppercase
      Lowercase
      Numerals
      Symbols

PTS: 1 REF: 68

47. ANS:
Restricted groups can be used to configure membership of sensitive groups, including the Administrator group. By using this feature, you can control who is and is not included in a group, and every time the policy is refreshed, group membership will be modified to include only the members specified in the Members list.

PTS: 1 REF: 72

48. ANS:
The analyze switch causes secedit to analyze security for whichever element is selected. This switch allows you to analyze current database settings against other settings (typically baseline settings) and store the results in a log file.You can view the results in the Security Configuration and Analysis snap-in.The result will show you the difference between the current settings and the baseline settings, allowing you to see and address any potential security holes.This can be very useful when troubleshooting or for analyzing a system whose exact settings might be unknown as compared to a standard security template.You can also use this switch to analyze the difference between a baseline template and a custom security template you create.

PTS: 1 REF: 90

49. ANS:
File server
Print server
Application server
Mail server
Terminal server
Remote Access/VPN server
Domain controller
DHCP server
DNS server
WINS server
Streaming Media server

PTS: 1 REF: 100

50. ANS:
Placing all IIS servers (if your firm is running more than one) into an IIS OU will help you manage GPOs related to securing and managing IIS servers across the organization. Remember to only install the necessary IIS components, including Web Service Extensions, that you'll use. Another security measure you can take specific to IIS servers is to place content on a dedicated volume. You can also apply IPSec filters to block or permit specific IP traffic and secure sensitive IP traffic.

PTS: 1 REF: 114