Global Information Assurance Certification Paper

150 Questions from Course Materials
Practicum for the NT Security Track

Contents:

Submitted for GIAC approval this 15th day of August 2000.

Contact info:

Sean Mays
UVA Alderman Library
Newcomb Road
Charlottesville, VA 22903

90 Questions for Track 5.1 / 5.2 / 5.3: Securing Windows NT: Step-by-step

1. What is the gathering of information that is potentially useful for further intrusion or attack?

a) Reconnaissance p. 14
b) Part scanning
c) Pinging
d) Intense research

2. Useful methods to obtain information about an organization include(s):
a) Organizational website
b) USENET postings
c) Internet search engines
d) All of the above p. 16

3. The InterNIC database does not contain:
a) Key personnel contact info
b) DNS server addresses
c) Military and governmental records p. 16-17

4. Which of the following tools can be used to discover and map out network topologies and services?
a) ping
b) tracert
c) Port Scanners
d) All of the above p. 17

5. Which of the following is not a MS-related port?
a) 135
b) 138
c) 139
d) 50 p. 17-18

6. Which of the following Netbios names indicates a RAS Server Service?
a) <Computer name>00
b) <Computer name>01
c) <Computer name>20
d) <Computer name>06 p. 21

7. Generic term to describe utilities that automatically dial phone numbers within a range of numbers to circumvent firewalls.

a) Wardialers p. 23
b) Social Engineering
c) SMNP Snooping
d) Share Scanning

8. What is the devious art of tricking users and administrators into revealing info which can be used to break into their networks via phone or email.
a) Firewalling
b) Hacking
c) Phreaking
d) Social Engineering p.23

9. What is the best defense against reconnaissance from the Internet?
a) Network Firewall p.25
b) RRAS
c) LAN

10. What are real time packet sniffers that can detect attacks and certain types of suspicious behavior on a network?
a) Proxy Servers
b) Automated Protocol Analyzers p. 27
c) Honey Pots
d) Wins Servers

11. Which of the following server(s) are specific to MS networks to provide netbios name to IP address mapping?
a) DNS servers
b) WINS servers p. 28
c) HTTP web servers
d) SMTP e-mail servers

12. Security measures for WINS servers include(s)
a) Intranet use only (local lan)
b) Blocking traffic to it from the Internet via firewall
c) Restrict replication with partners
d) All of the above p. 29

13. Measures to screen information available to the public include(s):
a) Periodic review of company website and index services
b) Restricting company directions for internal user
c) Education about social engineering
d) Education about the lack of privacy on the Internet
e) All of the above p. 30

14. Methods for concealing RAS servers include(s):
a) Unpublished phone numbers

b) Educating users about SE and instructing them not to reveal phone number
c) Using a non-standard phone number outside the range of numbers assigned to your organization.
d) All of the above p32-33

15. Which of the following is a packet-filtering software run only one's own machine protecting only the computer on which it is installed?
a) Proxy server
b) Personal firewall p.34
c) Personal web server
d) Web browser

16. What is the most common form of attack against Windows NT?
a) BSOD
b) DOS p. 37
c) Mac
d) Whopper

17. What are the characteristics of a DOS attack on a server?
a) >95% CPU utilization
b) BSODs
c) Services fails to slow
d) Account lock outs
e) All of the above p. 39

18. The best defense against DOS attacks besides implementing a firewall is to install the latest
a) Option pack
b) Service pack p. 41
c) Encryption pack
d) Version of TechNet

19. Which of the following is true about service packs for Windows NT?
a) SP's must be reinstalled after the configuration of the server changes. p. 42
b) SP's remain intact regardless of configuration changes
c) SP's are not needed to maintain security
d) SP's, who needs them

20. Only the essential feature necessary for a system fulfill its purpose should be left installed or enabled, therefore one might want to disable which of the following:

a) Services
b) Hardware
c) Devices
d) Protocols and protocol bindings
e) All of the above p. 43

21. Although additional subsystems are provided for greater compatibility, which of the following could safely be removed from an NT box?
a) OS/2
b) Posix
c) Win 32
d) a and b p 44-45

22. What recommended registry value is needed to mitigate the damage of SYN floods post SP5?
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect
a) 0
b) 1
c) 2 p.54

23. The number of times NT can be installed on a single hard drive is
a) Twice
b) Once
c**) Limited only be the amount of free space on a drive p. 57**
d) None of the above

24. What is the only thing an emergency repair disk cannot be used for?
a) Repair essential registry hive
b) Repair and replace OS files needed to boot computer
c) Compare checksums of OS files
d) Inspect and replace boot sector
e) Boot the computer p. 57

25. What is the command line used to copy the current user account database to an ERD?
a) rdisk /s p.58-59
b) rdisk
c) rdisk /erd
d) erd /s

26. What is the most effective tool for analyzing DOS attacks?
a) Performance monitor
b) Protocol analyzer / packet sniffer p. 63
c) Log files
d) Crashdump file

27. What types of information can be obtained by a hacker using "Null sessions?"

a) Username with description
b) User's last login date and time
c) Current password and account lockout policies
d) List of running services and device drives
e) All of these and more p. 72-73

28. Which of the following accounts may be renamed, but not deleted?
a) Administrator
b) Guest
c) Everyone
d) a and b p. 73

29. Where is a backup copy of the user accounts SAM database kept?
a) %system root\repair p. 75
b) %system root\repair\System32\repair
c) %system root\repair\SAM
d) %system root\repair\system32\SAM

30. When can the Security Configuration Editor not be used?
a) To define a template of security configuration settings.
b) To compare a local machine's setting against a template.
c) To configure a local machine's setting to match a template.
d) To configure machines remotely over the network. p. 76

31. Which of the following statements is not true of "null" sessions?
a) Username and password are each a null character
b) Members of Everyone and Network groups
c) Security access token has a SID of S-1-5-7
d) Members of the Authenticated Users group p. 80

32. What is the value name and value data used to prevent null sessions?
a) RestrictAnonymous 0
b) RestrictAnonymous 1 p. 85
c) NullSession 0
d) NullSession 1

33. Which of the following steps should be implemented to protect the administrator account from being hacked?
a) Rename the administrator account
b) Enable administrator account lockout with pasprop
c) Use two accounts for administrators
d) Use extended ASCII characters in the password
e) Remove administrator log on over network right
f) All of the above p.87-89

34. Which of the following statements is not true for the guest account?
a) This account is enabled on the workstation and disabled on the server.

b) Cannot be deleted, but can be renamed
c) Guest is a member of the Authenticated Users group
d) All unknown users will be transparently logged in as guests p. 90-91

35. What is the preferred order to assigning accounts to service apps?
a) System, local, global p. 98-99
b) Local, global, system
c) Global, local, system
d) System, global, local

36. What is the name of the native DLL file that forces complex passwords post SP 3?
a) Passfilt p. 101
b) Filtpass
c) Secpass
d) Quakenbush

37. What is the name of a post SP3 utility that can strongly encrypt passwords in the SAM?
a) syskey p.109
b) systemkey
c) syssam
d) samsec

38. Which of the following operating systems does not support NTLM v.2 authentication?
a) Windows 95/98 p. 112
b) NT 4 with SP4
c) Windows 2000
d) Windows 95/98 with Directory Services Client

39. List the authentication methods NT uses from weakest to strongest in terms of security.
a) LM, NTLM v.1, NTLM v.2 p. 113-114
b) NTLM v 2, NTLM v 1, LM
c) NTLM v1, NTLM v2, LM

40. Authentication and session security are set in a registry value named _____ on both NT and W9x clients.
a) NTLMCompatibilityLevel
b) LMCompatibilityLevel p. 116
c) SecCompatibilityLevel
d) LM2CompatibilityLevel

41. What is the service, which handles pass-through authentication and account synchronization on NT?
a) netloger

b) netlogin p. 118
c) loginnow
d) server

42. A 1996 FBI report on computer crime estimated, that legitimate users perpetrate 75% of security breaches. List the severity of these threats from most likely to less likely.
a) full time employees, part-time and contract, hackers p. 131
b) part-time employees, full time, contract, hackers
c) contract employees, part-time employees, hackers, full time
d) hackers, full time employees, part-time, contract

43. Which of the following statements is not true of local groups?
a) Contain global groups from local and trusted domains
b) Have rights and permissions assigned to them
c) Are "trapped" on the machines where they are created
d) Can contain other local groups p. 135

44. Which of the following statements is incorrect about NTFS?
a) NTFS permissions are enforced over the network.
b) NTFS permissions are enforced against local console users.
c) NTFS supports detailed auditing
d) NTFS supports dual-booting to other operating systems p. 136

45. What is the effective permission to an individual belonging to all three groups?

	NTFS Permissions	Share Permissions
Sales	Change	No Access
Admins	Changes	FC
Manage	Read	Change

a) No Access p. 138-139
b) Change
c) FC
d) Read

46. The default NTFS and share permissions for the group Everyone is
a) No Access
b) Change
c) Full Control p. 140
d) Read

47. The Change permission is the same as Full Control except that:
I It does not include the Take Ownership permission.
II It does not include the Change Permission.

III It includes the Take Ownership Permission.
IV It includes the Change Permission.

a) I & II p. 140
b) II & III
c) III & IV
d) I & IV
e) I & III

48. By default, the backup operators and restore operators groups have which of the following rights:
I B/U files and directories
II Restore files and directories
III Bypass traverse checking

a) I & II
b) II & III
c) I & III
d) I, II, & III pp. 146-147

49. What is the term that describes the hidden shares NT creates with full control permissions at the root of all volumes (C$, D$, etc.)?
a) Administrative shares p. 150
b) IPC shares
c) Hidden shares
d) Dollar shares

50. Remote access to the registry is determined by ACL permissions set on which key in the registry key:
a) regevir
b) winreg pp. 152-154
c) remreg
d) regedit

51. When RestrictNullSessAccess is set to 1, which of the following statements is false?
a) Null session users cannot access any shares
b) Null session users can access any folder/printer shared to the Everyone pp. 155-156
c) Null session shares mush be set manually within the registry
d) Null session users can access only shares found in the registry key which have share permissions for the Everyone group

52. Which of the following options if the most secure call back option for RAS?
a) No Call Back

b) Set by caller
c) Preset to a predefined number (user's home, remote office) p. 162

53. What is the value needed to prevent downgrading of MS chap as set within UseLMPassword value on client and servers?
a) 0 p. 163
b) 1
c) 2
d) 3

54. SMB sessions can be hijacked or replayed with modification because the ___ is by default, always sent over the network in clear text.
a) UID P. 166
b) SID
c) SMBID
d) CIFS

55. What is the common name for a server or resource designed to ensnare intruders, log their intruders and alert administrators?
a) Sugar pot
b) Sugar daddy
c) Honey pot p. 181
d) NT server

56. In a high security environment, a server can be made to shut down rather than to operate without auditing by which of the following registry keys?
a) Crash on Audit/Fail = 0
b) Crash on Audit/Fail =1 p. 190
c) Crash on Audit/Fail = 2
d) None of the above

57. What should one implement to examine audit log entries in real-time for suspicious or threatening activities?
a**) host-based intrusion detection system p. 195**
b) event viewer
c) unix syslog
d) dumpel

58. A ____ is a set of files, which patches or replaces critical OS files in order to allow undetected complete control of a system.
a) oskit
b) rootkit p. 174

c) patchkit
d) ntkit

59. What is a quick and harmless measure if you suspect your system has been tampered with?
a) Wipe your drives and reinstall the OS again
b) Compare your files against the tape backup
c) Reapply the latest service patch from cd-rom p. 197

60. What should be developed long before an intrusion is discovered in order to save time, prevent harm, reduce chaos, and perhaps avoid legal troubles?
a) Incident response plan * p. 200-201
b) Risk analysis
c) Contact list
d) Publicity policy

61. What tools are available to make registry changes to hundred of computers and enforce those changes for users from computer to computer?
a) System policy
b) Group policy
c) Security policy
d) a and b p. 206
e) b and c

62. Which of the following operating systems cannot use system policies?
a) Windows NT
b) Windows 9x
c) Windows 2000
d) Windows 3.1/ WFWG p.207

63. System policy files are created with System Policy Editor (poledit.exe)
What are the respective names of the files created for NT and Windows 9x?
a) config.pol - config.pol
b) ntconfig.pol - config.pol p. 210
c) config.pol - ntconfig.pol
d) ntsec.pol - sec.pol

64. Which folder do computer systems look in to obtain system policies?
a) netlogin (%systemroot%\system32\repl\imports\scripts)
b) netlogin (%systemroot%\system32\repl\exports\scripts)
c) netlogon (%systemroot%\system32\repl\imports scripts) p. 210
d) netlogon (%systemroot%\system32\repl\exports\scripts)

65. A _____ implemented under a system policy will not deter the unscrupulous, but it may assist in the legal prosecution of unauthorized users.
a) Banner
b) Logon banner p. 215

c) Dial-in banner
d) Automatic banner

66. What is the name of a recent tool MS has introduced which can define registry values like system policies, but adds the capability to set permissions for drives and the registry itself?
a) Security editor
b) Regedit
c) Security configuration editor p. 216
d) Regini

67. Which feature circumvents the bulk of user-level-security by permitting a computer to boot straight into its desktop and is especially dangerous because it stores username and password in the registry as clear text.
a) Open sesame
b) Secure logon
c) Logon auto
d) Automatic logon p. 218

68. Which of the following can prevent users from logging in with cached credentials even if their account has been deleted or disabled?
a) CachedLogonsCount = 10
b) CachedLogonsCount = 0 p. 221
c) NoCachedLogons = 0
d) NoCachedLogons = 1

69. What is a better way to secure a user's desktop while they are away and minimize user inconvenience of logging off and losing open files and applications?
a) Ctrl - Alt - Delete Enter to lock workstation p. 222
b) Ctrl - Esc to lock workstation
c) Ctrl - Alt - Esc to lock workstation

70. What is another alternative that has the same effect as locking the workstation?
a) Screen savers
b) Screen savers with passwords p. 223
c) LifeSavers
d) Corporate background logos

71. Which of the following measures could weaken password security?
a) Don't share your password
b) Don't have your password near your workstation

c) Don't use password which is identical to any prominent, fixed word in you immediate vicinity

d) Write down your password and keep it on a post-it near your monitor p. 224

72. What can be used to monitor workstation configuration, search for installed device drives for modems or other undersized hardware, search for files of undersized programs and verify that security options are still in effect?
a) Virus scanner
b) Enterprise management system (EMS) p. 228
c) Software licensing package (SLP)
d) Integrated security project (ISP)

73. Since new viruses are continually being discovered, the software must also be continually _____ to detect and eradicate them.
a) Backed-up
b) Updated p.231
c) Uninstalled
d) Reinstalled

74. What is the biggest (main) reason to secure printer drivers?
a) They run in kernel mode (thus having unlimited access to the OS and hard drives) p. 233
b) Users can delete and install them by default
c) Reduce chaos
d) Job security

75. How does one go about disabling the floppy drive in a computer system?
a) Remove the drive
b) Bios settings, disable the floppy
c) Bios settings, change boot order to begin with hard drive
d) Floplock.exe
e) Any or all the above p. 236

76. What is the registry value and value data to disable the creation of "8.3" names?
a) NTFSDisable8dot3NameCreation = 1 p.240
b) NTFSDisable8dot3NameCreation = 0
c) Disable8dot3NameCreation = 1
d) Disable8dot3NameCreation = 0

77. Which statement about the power users group is incorrect?
a) They can modify the membership of any group they create
b) They can modify the member of power users, users and guest group
c) They can modify administrator or backup operators group p.258

78. Which group has the shutdown right on a default NT build that permits even guests to have the ability to shutdown a computer?

a) Power users
b) Users
c) Everyone **p. 257-258**
d) Administrator

79. In general, local accounts can only be used to log onto the computer where they were created and can only be assigned rights and permissions on the same computer. What is the exception to this statement?
a) The computer is a stand-alone workstation
b) The computer is a domain controller **p. 256**
c) The computer is an application server

80. Before undertaking any actions suggested in this course, one must
a) Obtain professional psychiatric care
b) Obtain professional legal counsel **p. 264**
c) Obtain professional employment elsewhere

81. Successful prosecution of company employees depends upon:
a) Employee education and information of appropriate use policies.
b) Forewarning of monitoring activities and information gathering.
c) Employee awareness of the penalties for inappropriate use.
d) All of the above **p. 265-266**

82. Which of the following groups is not a built-in account on a domain controller?
a) Server operators
b) Print operators
c) Account operators
d) Power users **p.257**

83. What is the term for when a target user or administrator initiates the call to the hacker and asks for assistance from the hacker?
a) Social engineering
b) Reverse social engineering **p. 124**
c) Sabotage
d) Chaos

84. Which of the following is not a physical security threat to NT?
a) Using null sessions to gather information **p. 246**
b) Booting from an alternate operating system
c) Unauthorized access to server consoles
d) Theft of backup tapes or Emergency Repair Disks

85. Which of the following programs can be used to detect modified binaries or rootkits under Windows NT?
a) Centrax
b) EventAdmin

c) Dumpel
d) Intact pp. 197-199

86. The recommended "best practice" for a secure configuration of Windows NT is to place user accounts in _____ but assign rights to _____.
a) Local Groups, Global Groups
b) Global Groups, Local Groups pp. 134-135
c) Local Groups, Domain Users
d) Global Groups, Domain Users

87. The effective permission to a resource is the most _____ of the share and NTFS permissions.
a) Restrictive p. 138
b) Powerful
c) Permissive
d) Expansive

88. Which of the following best describes the purpose of setting SealSecureChannel to 1?
I Netlogon channel packets will be digitally signed.
II Netlogon channel packets will be encrypted.
III Both signature and encryption will be negotiated.
IV No packets will be signed or encrypted.

a) I only
b) II only
c) III only
d) IV only
d) I & II pp. 120-121

89. Which of the following ASCII characters does L0phtCrack have difficulty with?
a) ALT-0-1-3 (carriage return) p. 87
b) ALT-0-2-7 (escape)
c) ALT-0-3-2 (space)
d) ALT-0-0-7 (bell)

90. Which of the following is not a system policy template?
a) Winnt.adm
b) Common.adm
c) Shell.adm
d) Windows.map p. 211

30 Questions for Track 5.4: Internet Information Server

1. Which of the following filename extensions is not unique to IIS?
A) .ASP

B) .HTR
C) .IDC
D) .HTM p. 12

2. The most common threat to IIS is:
A) DOS p. 19
B) BSOD
C) Security
D) Script Codes

3. Which of the following mechanisms does not control access to IIS?
A) IIS permissions
B) NTFS permissions
C) Share permissions p. 22
D) IP Filtering

4. HTTP is a ____ protocol in that a web server does not remember who you are when you make another request.
A) Clueless
B) Session less
C) Stateless p. 30
D) Useless

5. Which of the following tools would not be used for security scanning and penetration testing of IIS?
A) Nessus
B) CyberCop
C) Internet Scanner
D) Dsniff p.32

6. Packet filters should only permit access to IIS servers using the default ports of
I 80 II 443 III 135 IV 139
A) I & II pp. 43-44
B) II & III
C) III & IV
D) I & IV

7. The main advantage to moving the root folder of an IIS server to another server is:
A) A box becomes generic and can be easily replaceD) P.47
B) Fault tolerance via DFS
C) Improved performance
D) Improved security

8. Which of the following computer systems is the least favorable for hosting IIS?
A) Domain Controller pp. 50-51
B) Stand-alone server
C) Member server

D) NT workstation with Personal Web Services

9. On a stand-alone IIS server, which of the services below could not be disabled?
A) Computer Browser
B) NetLogon
C) Spooler
D) WWW Publishing Service pp.53-54

10. Anonymous users authenticate via a special user account to IIS. What is the default name of this account?
A) IUSR_computername pp.62-63
B) IIS_computername
C) Anon_computername
D) IWAM_computername

11. When a folder or file has all authentication options enabled, what is the order in which these authentications take precedence?
A) Certificate, Anonymous, Integrated Windows, Basic, Digest pp.79-80
B) Integrated Windows, Basic, Digest, Anonymous, Certificate
C) Anonymous, Digest, Basic, Integrated Windows, Certificate
D) Basic, Anonymous, Digest, Certificate, Integrated Windows

12. Which of the following statements is false for Integrated Windows authentication?
A) It uses NTLM and Kerberos in parallel.
B) Only supported in versions 2 or later of IE.
C) It can be utilized through a proxy server. p. 80
D) It is often transparent to users.

13. Which of the following statements about DS mappings is false?
A) Once enabled other certificate authentications will not function
B) Feature is only available to machines part of a Windows 2000 domain
C) Is also known as "UPS" mapping. P. 95
D) It cannot be applied for some sites and not others on the same IIS box.

14. Which of the following authentication methods will always defeat anonymous authentications?
A) Certificate p. 80
B) Integrated Windows
C) Basic
D) Digest

15. Which of the following execute permissions does not exist?
A) None
B) Scripts Only
C) Scripts & Executables

D) Executables Only pp. 108-110

16. The help desk receives a call from a user stating they can no longer access a active server page they were working on just yesterday and are now receiving an error message. After identifying them as working for your company (no SE going on here), you realize you changed execute permissions on this folder this morning to _____.

A) None p. 110
B) Scripts Only
C) Scripts & Executables
D) Executables Only

17. What is the deadliest combination of IIS permissions to have on a folder?

I Write II Execute III Read IV Script Source Access

A) I & II p. 111
B) II & III
C) III & IV
D) I & IV

18. This tool is a miniature registry editor made especially for configuring IIS.

A) iissync
B) metaedit p. 162
C) regedt32
D) regsrv32

19. Which of the following systems and/or applications do not support WebDAV?

A) Windows 2000
B) IE 5
C) Office 2000 products
D) Windows 95 p. 126

20. Which of the following processes permit IIS to run applications separately from it?

A) Inetinfo.exe
B) DLLHost.exe p. 144
C) Lsass.exe
D) Msdtc.exe

21. What is the default user account that web applications utilize to run isolated or "out-of-process"?

A) IUSR_computername
B) IIS_computername
C) IWAM_computername p. 147
D) AP_computername

22. To unregister OLE and COM components, which application and syntax would you use below?

A) regsvr32 filename /u p. 152
B) unregvr32 filename /u

C) regsvr32 filename
D) regedt32 filename

23. To prevent hostile ASP scripts from using relative directory addressing to access other files in the directory structure above it, one should

I Enable parent paths.
II Disable parent paths.
III Place the IIS root folder on a different partition than the %systemroot%.
IV Place the IIS root folder on the same partition as the %systemroot%.

A) I & III
B) II & IV
C) I & IV
D) II & III p 154

24. In order to make certain items invisible to queries of the Index Server, you need to modify this file.

A) \%systemroot%\system32\noise.dat p.171
B) \%systemroot%\system32\query.dat
C) \%systemroot%\system32\inetsrv\noise.dat
D) \%systemroot%\system32\inetsrv\query.dat

25. Which one of the following IIS optional components is especially dangerous?

A) Remote Data Service p. 56
B) NNTP Service
C) SMTP Service
D) Transaction Queue Service

26. A Microsoft applet which enables developers and security administrators test application and authentication issues.

A) What-If p. 98
B) Iissync
C) metaedit
D) regsrv32

27. Content sources for an IIS site can be

A) A directory located on the IIS computer
B) A share located on another computer
C) A redirection to another URL
D) All the above. P. 46-47

28. Which of the following users may need Script Source Access permissions?

p. 112 **A) Developers and webmasters who control the files on the server**
B) IUSR_computername
C) IWAM_computername

D) No user needs this permission.

29. Which of the following words is not an HTTP verb sent from the client to the server?
A) Get
B) Post
C) Delete
D) Put
E. Place p. 150

30. IIS 5 supports Internet Printing by mapping a virtual directory named /printers to __ .
A) %systemroot%\web\printers p. 58
B) %systemroot%\system32\spool\printers
C) %systemroot%\system32\spool
D) %systemroot%\web\spool

30 questions on Track 5.5: Active Directory for W2K in a Nutshell

1. What is the core security service in Windows 2000 that provides a directory service infrastructure upon which virtually all other security and management features depend?

a) ADS **p. 7**
b) NDS
c) NIS
d) CIFS

2. What feature of Windows 2000 when leveraged with active directory makes it possible to automatically reconfigure the permissions, registry values, account policies, group memberships, desktops and other features of your network's machines?

a) System Policy
b) Group Policy **p. 7**
c) System Configuration Editor
d) Regedit

3. What is the name of the folder that contains scripts, policies, and the Netlogon share under Windows 2000?

a) NTDSvol
b) Volsys
c) Sysvol **p. 22-23**
d) Dcvol

4. What is the name of the file and its location that is the Active Directory database?

a) %systemroot%\NTDS\ntds.dit **p. 21**
b) %systemroot%\NTDS\ads.dit
c) %systemroot%\ntds.dit
d) %systemroot%\ads.dit

5. What is the name of the tool used to directly modify the Active Directory database?

a) ADSI Edit **pp. 24-25**
b) dcpromo
c) acldiag
d) ntdsutil

6. Which of the following steps are required to use the Schema Manager snap-in to modify the schema?

I Regsvr32.exe schmmgmt.dll
II Regsvr32.exe schemmgmt.dll

III Must check box within AD Schema Manager snap-in to permit modification
IV Must disable check box within AD Schema Manager snap-in to permit modification

a) I & III pp 27-28
b) I & IV
c) II & III
d) II & IV
e) No steps are required.

7. What is the term to describe a set of well-connected machines on an IP subnet?
a) Domain
b) Forest
c) Tree
d) Site p. 31

8. What is the primary difference between a site and a domain?
a) There is no difference.
b) A site is a physical concept, whereas as a domain is a logical concept. p.31
c) A site is a logical concept, whereas as a domain is a physical concept.
d) A site is a contiguous structure, whereas a domain can be non-contiguous.

9. What service under Windows 2000 automatically manages the replication within a site?
a) Replication Manager service
b) Knowledge Consistency Checker p. 32
c) Netlogon Service
d) Active Directory Service

10. Which of the following statements are correct for SMTP intersite replication?
I It is generally used for slower unreliable links between sites.
II You must have Certificate Services installed on a DC to use it.
III SMTP data is encrypted.
IV SMTP transports follow schedule settings.

a) I, II, III pp. 32-33
b) I, III, IV
c) II, III, IV
d) I, II, III, IV

11. Which of the following is not a FSMO master role?
a) PDC Emulator Master
b) RID Master
c) Infrastructure Master

d) Schema Master
e) Domain Naming Master
f) WINS Master p. 37

12. A ____ is the "blueprint" for the Active Directory database.
a) Schema p. 40
b) FSMO
c) Master
d) LDAP

13. Which of the following is an example of a UPN?
a) Jason@fossen.net p. 47
b) cn=Admistrator,ou=Austin,dc=fossen,dc=net
c) cn=Administrator, ou=Austin
d) cn=Godzilla,ou=Domain Controllers,dc=fossen,dc=net

14. Which of the following best describes trusts under Windows 2000?
a) one-way, non-transitive
b) one-way, transitive
c) two-way, non-transitive
d) two-way, transitive p. 49

15. Which of the following groups cannot be created while Windows 2000 is running in mixed mode?
a) Universal distribution group
b) Universal security group p. 57
c) Global security group
d) Global distribution group

16. Which of the following is not true of Universal groups?
a) Can contain users and global groups from any domain in the forest.
b) Can contain local groups. p. 56
c) Can be used to assign rights and permissions.
d) Can be used to create distribution lists in either mixed or native modes.

17. Which of the following statements is not true of Windows 2000 running in native mode?
a) Local security groups can contain other local security groups
b) Global security can groups can contain other global security groups
c) Universal security groups cannot be created p. 58
d) Universal security groups can contain any other types of groups, except for local groups.

18. What account option must be enabled for CHAP authentication, Digest authentication, and Services for Macintosh UAM authentication to work?
a) Smart card is required for interactive login

b) Account is trusted for delegation
c) Store password using reversible encryption pp. 61-62
d) Use DES Encryption types for this account

19. Which of the following Dial-in options are unavailable to an administrator who is running in mixed mode?
a) Verify Caller-ID
b) Assign a static IP address
c) Control Access through Remote Access Policy p. 63
d) Apply static routes

20. What is the term used to describe the situation when a container or object does not inherit from its parent container?
a) bastard
b) orphan p. 65
c) outsider
d) non-conformist

21. What is the utility that can change the permissions on AD objects and containers?
a) DSACLS pp. 68 - 71
b) ENUMPROP
c) ACLDIAG
d) SDCHECK

22. What TCP port does SMB without netbios operate on?
a) 139
b) 135
c) 443
d) 445 p. 18

23. Which of the following utilities can used to determine what information can be gathered from LDAP with null user credentials?
a) RUNAS
b) LDP pp. 75-76
c) INTACT
d) DSACLS

24. Where are password policies for the domain set in Windows 2000?
a) User Manager for Domains
b) AD User Manager
c) Group Policy p. 60
d) Security Configuration Editor

25. Which of the following statements is not true of GPOs and GPO links?
I They are separate objects unto themselves.
II They continue to exist even if they are not linked to any containers.
III They are dependent upon the containers to which they are linked.

a) I
b) II
c) III pp. 86-88
d) I, II, & III

26. What order do GPOs and NT System Policies get applied?
I Domain GPOs
II Local GPOs
III Organizational Unit GPOS
IV NT 4 System Policy
V Site GPOs

a) I, II, III, IV, V
b) I, IV, V, II, II
c) III, V, IV, I, II
d) IV, II, V, I, III p. 89

27. In what order do multiple GPOs get applied if they are on the same container?
a) From the top of the list to the bottom of the list as found in the property sheet.
b) From the bottom of the list to the top of the list as found in the property sheet. P. 89-90
c) Randomly from the list in the property sheet.
d) One cannot have multiple GPOs on the same container.

28. Which of the following statements is not true for GPO scripts?
a) They can be run synchronously.
b) They can be run asynchronously.
c) They always run last. pp. 101-102
d) They can be run at computer startup/shutdown and user log on/log off.

29. What is the extension and location for GPO security templates?
a) .inf %systemroot%\Security\Templates p. 105
b) .adm %systemroot%\Security\Templates
c) .inf %systemroot%\SYSVOL\Scripts
d) .adm %systemroot%\SYSVOL\Scripts

30. Which of the following is not controlled by a GPO administrative template?
a) IE policies
b) User's desktops
c) User's Start menu
d) Password Policies p. 108-110