Global Information Assurance Certification Paper

Practical Assignment

Securing NT Step-by-Step

Contents:

Submitted by: Don Ferrara

Part 1

Securing Windows NT Step by Step

1. The gathering of information, which is potentially used for further intrusion or attack, is known as?

   a. Scanning
   b. Reconnaissance (NT pg 14)
   c. Pinging
   d. Intelligence gathering

2. Once a hacker obtains the IP addresses of a DNS server, what utility can they use to obtain hostnames and IP addresses for systems in the domain?

   a. nbtstat
   b. tracert
   c. nslookup (NT pg 17)
   d. ping

3. Using the nbstat utility the following output is obtained:

EDRMSTRG1001CNT	<00>	unique
EDRMSTRG1001CNT	<20>	unique
EDRMSTRG	<00>	group
EDRMSTRG	<1C>	group
EDRMSTRG	<1B>	unique

4. From this information what can the hacker determine?

   a. EDRMSTRG1001CNT is the domain name
   b. EDRMSTRG is the domain name (NT pg 21)
   c. EDRMSTRG1001CNT is an Exchange server
   d. EDRMSTRG is an IIS server

5. Which of the following is an example of a wardialer used to find telephone numbers connected to a modem?

   a. ToneLoc (NT pg 23)
   b. DialDetect
   c. PhoneSearch
   d. All of the above

6. What is the single best defense against Internet reconnaissance?

   a. Using strong passwords
   b. Running through a proxy server
   c. Deploy a firewall (NT pg 25)
   d. Install RRAS on the server

7. Which of the following is true of an automated protocol analyzer?

   a. are able to send administrative alerts
   b. are also called "Intrusion Detection Systems"
   c. are able to block the attacker's IP address
   d. all of the above (NT pg 27)

8. The database of a remote WINS server can be downloaded using?

   a. winslst
   b. winsrepl
   c. winsdmp (NT pg 29)
   d. lstwins

9. Which of the following is a typical personal firewall, used to protect a home computer?

   a. ZoneAlarm
   b. BlackIce
   c. Tiny Personal Firewall
   d. All of the above (NT pg 34-35)

10. What is the most common form of attack against Windows NT?

    a. Virus
    b. DoS (NT pg 37)
    c. Trojan Horse
    d. Ping of Death

11. Which of the following is an example of a DoS attack?

    a. Ping of Death
    b. Syn Flood
    c. WinNuke
    d. All of the above (NT pg 40)

12. A Syn Flood consists of:

    a. an extremely large ICMP packet, which is fragmented in transit, but when the target starts to reassemble the packet, it's large size overflows the buffer
    b. a steam of TCP handshake packets that each request a new TCP session to begin, using a non-existant host (NT pg 40)
    c. consists of out of band data which causes a crash or 100% CPU usage
    d. fragmented packets whose completing packets never arrive

13. What is the main difference between the North American and Export versions of service packs?
    a. Different languages
    b. Different folder structure
    c. North American has stronger encryption (NT pg 41)
    d. There is no significant difference

14. Which of the following can be disabled on most systems?

    a. Server Service
    b. Workstation Service
    c. Simple TCP/IP Service (NT pg 44)
    d. Net Logon Service

15. What command allows you to manually determine if your system is being Syn-Flooded?

a. **netstat –a –n | find /I "syn" (NT pg 53)**
b. nbtstat –a –n | find /I "syn"
c. nslookup –a –n | find /I "syn"
d. netuse –a –n | find /I "syn"

16. What must the registry value be set at, to reduce the number of SYN-ACK retries?

HKEY_LOCAL_MACHINE
\system\CurrentControlSet\Services\Tcpip\ParametersSynAttackProtect:

a. 0
b. 1
c. **2 (NT pg 54)**
e. delete any entry found here

17. Which of the following disks should an administrator create?

(1) Emergency Repair Disk
(2) MS-DOS Boot Disk
(3) Emergency NT Boot Disk
(4) Setup Disks

a. (1) and (3)
b. (1) and (4)
c. (1) , (2) and (3)
d. (1), (2), (3) and (4) (NT pg 58)

18. To use the ERD the first step is:

a. press "R" and insert the ERD
b. boot using the setup disks (NT pg 59)
c. boot using the ERD
d. restart the machine and select "repair"

19. How do you encrypt the SAM database?

a. use SYSKEY.exe (NT pg 60)
b. use DES.exe
c. use RSA.exe
d. use AES.exe

20. Where is the backup copy of the SAM kept?

a. %system root\system32\repair
b. % system root\repair\SAM
c. % system root\repair (NT pg 60)
d. on the ERD

21. What utility saves all information in RAM to the local drive, then to a .dmp file on the next reboot after a BSOD attack?

a. MEMORY.dmp
b. RAM.dmp
c. CRASH.dmp
d. BSOD.dmp

22. What built in accounts cannot be deleted from NT?

(1) Administrator
(2) Guest
(3) Backup
(4) Everyone

a. (1) and (2) (NT pg 73)
b. (2) and (4)
c. (1) and (3)
d. (3)

23. Which of the following statements is false?

a. The "Guest" account can be locked out due to bad logon attempts
b. The "Backup" account can be locked out due to bad logon attempts
c. **The "Administrator" account can be locked out due to bad logon attempts (NT pg 73)**
d. All of the above

24. The Microsoft Security Configuration Editor is not used to:

a. define a template of security configuration settings
b. compare the local machine's settings against a template
c. configure the local machine's settings to match a template
d. configure a remote machine's settings to match a template (NT pg 76)

25. How do you establish a null user session on the server EDRMSTRG1001CNT?

a. Net use \\edrmstrg1001cnt\ipc$ ""/user:"" (NT pg 81)
b. Net view \\edrmstrg1001cnt\ipc$ ""/user:administrator
c. Net map \\10.0.0.1\ipc$ ""/user: ""
d. Net use \\10.0.0.1\ipc$ ""/user:backup

26. What utility from the NT Resource Kit will list all usernames on a remote computer irrespective of dial-in-permissions (including permissios)?

a. RSAUSERS.exe
b. USERS.exe
c. ADDUSERS.exe (NT pg 83)
d. REMOTEUSR.exe

27. What "SomarSoft" utility allows you to extract a list of usernames, password policy, assigned user rights, running services, share permissions and NTFS permissions.

a. DumpSec (NT pg 84)
b. DumpNT
c. ACLDump
d. DumpPol

28. Which ASCII character, in particular does L0phtCrack have difficulty breaking?

a. Alt-0-2-3
b. Alt-0-1-3 (NT pg 87)
c. Alt-0-2-3
d. Alt-0-3-3

29. What utility will enable you to lockout the Administrator account for over-the-network authentication?

a. ADMINLOCK.exe
b. ADMINPROP.exe
c. PASSLOCK.exe
d. PASSPROP.exe (NT PG 88)

30. Which of the following statements is not true?

a. Administrators should log on to the "administrator" account
b. Administrators should have two accounts, one for normal work and one for administration of the LAN
c. The "administrator account should never be renamed (NT pg 89)
d. The "log on over network" right should, if possible, be removed from administrator accounts

31. Which of the following statements is true?

a. The "Guest" account can be deleted but cannot be renamed
b. The "Guest" account is disabled by default on Workstation
c. The "Guest" account is enabled by default on Server
d. The "Guest" account allows automatic logon when the password is blank (NT pg 90)

32. NT observes the following order of preference for all processes:

a. System, Global, Local
b. Local, System, Global
c. System, Local, Global (NT pg 98)
d. Global, Local, System

33. PASSFILT.DLL, found in SP3 or later provides an optional password filter that can require coplex passwords. It requires that the password be at least 6 characters long, not contain any part of the user's full name and contain _____ of the following categories of characters: uppercase letters, lowercase letters, numbers, non-alphanumeric symbols?

a. 1
b. 2
c. 3 (NT pg 101)
d. 4

34. With a null user session an attacker can use the Pedestal Software utility NTUSER to list what ?

a. account and password policies (NT pg 104)
b. user's rights
c. user's IP address
d. All of the above

35. In a medium security network, password uniqueness should be set to?

a. Between 5 and 6
b. Between 7 and 9
c. Between 8 and 13 (NT pg 105)
d. Between 14 and 16

36. Which operating system does not support NTLM v.2 authentication?

a. NT 4 (SP4)
b. Windows 95/98 (NT pg 112)
c. Windows 2000
d. Windows 95/98 with Directory Services Client from Win2000

37. Authentication and session security options for NTLM v.2 are set in a registry value named_____ on NT and Windows 9x

a. LMCompatibliltyLevel (NT pg 116)
b. SecurityCompatibilityLevel
c. NTLMCompatibilityLevel
d. NTLM2CompatibilityLevel

38. Pass-through authentication and synchronization of the user accounts database occur over the:

a. Authentication channel
b. Logon channel
c. NetLogon channel (NT pg 118)
d. NetLogin channel

39. Which of the following is not a valid registry value for the encryption and integrity-checking of the NetLogon channel?

a. SignSecureChannel
b. RequireSignOrSeal
c. SealSecureChannel
d. AuthenticateSecureChannel (NT pg 120)

40. What is Social Engineering?

a. The sharing of security concepts between IT Sec professionals
b. The attempt to trick a user into revealing information to overcome network security (NT pg 122)
c. The policies put in place when trusting a domain from another company
d. The assistance given a user by the IT Sec personnel in the company

41. Reverse Social Engineering can be accomplished by:

a. a hacker getting friendly with a company employee to obtain security information
b. a hacker finding out what software a company is using and contacting them to provide free uNT pgrades (NT pg 125)
c. a hacker attempting to break passwords on the network
d. a hacker initiating a DoS attack to deny access to needed data and resources

42. According to a 1996 FBI report on computer crime, what was the estimated percentage attributed to legitimate internal users?

a. 35%
b. 50%
c. 75% (NT pg 131)
d. 85%

43. In NT which of the following statements is false?

a. Local groups can contain global users and local groups (NT pg 135)
b. Local groups can contain global groups
c. Local groups can contain global users
d. Local groups can contain global users and global groups

44. Which of the following benefits does the NTFS file system provide?

a. inheritable file and folder permissions
b. detailed auditing of the exercise of permissions to folders or files
c. permissions are enforced against local console users
d. All of the above (NT pg 136)

45. If a user belonged to the Training, Managers and Contractor groups what would the user's cumulative permissions be for the following:

NTFS Permissions	Share Permissions
Training – Change	Training – Read
Managers – Change	Managers – Full Control
Contractor – Read	Contractor – Change

a. Full Control
b. Change (NT pg 138)
c. No Access
d. Read

46. When talking about permissions, which of the following statements is false?

a. Full Control access overrides all others (NT pg 137)
b. No Access overrides all others
c. The effective permission is the most restrictive of the share and NTFS permissions
d. NTFS permissions are inheritable

47. What are the default NTFS and Share permissions?

a. Everyone – Change
b. Everyone – No Access
c. Everyone – Full Control (NT pg 140 –142)
d. Everyone – Read

48. The "Authenticated Users" group can only be seen:

a. in "User Manager for Domains" under Groups
b. in "User Manager for Domains" under the User's group membership
c. in "User Manager for Domains" under User rights (NT pg 142)
d. all of the above

49. What utility can be fount in the NT Resource Kit which will allow you to copy share permissions from one share to another?

a. CACLS.exe
b. SHARECPY.exe
c. SECADD.exe
d. PERMCOPY.exe (NT pg 144)

50. The SECADD.exe utility in the NT Resource Kit allows you to:

a. add new security parameters
b. change permissions on registry keys (NT pg 144)
c. create new security templates
d. all of the above

51. The CACLS.exe utility in the NT Resource Kit allows you to:

a. copy share permissions from one share to another
b. manage NTFS permissions on files (NT pg 144)
c. add new security parameters
d. create new security templates

52. What utility, which will allow you to manage shared folders and printers on remote systems, can be fount in the NT Resource Kit,?

a. RMTMANAGE.exe
b. RSHARE.exe
c. RMANAGE.exe
d. RMTSHARE.exe (NT pg 144)

53. In HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA, what does the value "Restrict Anonymous" achieve?

a. restricts anonymous users to specified folders
b. does not allow anonymous users to log on
c. prevents null session users from listing usernames and groups (NT pg 149)
d. prevents null session user sessions

54. What are the default share permissions on the root of the drive volumes on NT computers?

a. Everyone – Read
b. Administrator – Full Control (NT pg 150)
c. Everyone – Full Control
d. Creator Owner – Full Control

55. What utility can be used to change permissions on registry keys?

a. REGEDIT.exe
b. EDITREG.exe
c. REGEDIT32.exe (NT pg 153)
d. (a) and (c)

56. When the RestrictNullSessAccess value is set to "1"_____.

a. Null Session users cannot access or see any Null Session shares
b. Null Session users can access any folder or printer shared to the "Everyone" group
c. Null Session users cannot access any shares
d. Null Session users cannot access but can see Null Session shares (NT pg 155)

57. What authentication protocol is used by dial-in clients and RAS servers?

a. DES
b. RSA
c. CHAP (NT pg 162)
d. DSA

58. What is the name of the Remote Access Service uNT pgrade provided by Microsoft?

a. Routing and Remote Access Service (RRAS) (NT pg 164)
b. Remote Access Plus (RAP)
c. RAS Callback
d. Remote Access Service v.2 (RAS2)

59. What is the main flaw in Microsoft Network Monitor?

a. Cannot capture some packet types
b. Has weak password encryption (NT pg 165)
c. Will not work with firewalls on the system
d. Does not have password protection

60. Server Message Block (SMB) protocol is susceptible to attack because what is transmitted in cleartext?

a. The SID
b. The password
c. The CHAP
d. The UID (NT pg 166)

61. A rootkit is:

a. A security template for the root directory
b. A utility for listing permissions applied to the root directory
c. A set of files that patch or replace critical OS files to allow undetected, complete control of the system (NT pg 174)
d. (a) and (b)

62. When Windows NT auditing is enabled in the User Manager\Policies menu\Audit option on a PDC:

a. The policy applies to all servers in the domain
b. The policy applies to all domain controllers (NT pg 177)
c. The policy applies to all computers in the domain
d. The policy applies only to the computer it was installed on

63. What utility can be used to write custom events for auditing?

a. EVENTLOG.exe
b. EVENTWTR.exe
c. LOGEVENT.exe (NT pg 180)
d. AUDITWTR.exe

64. What is the purpose of a Honey Pot server?

a. to alert administrators to intrusion
b. audit intruders actions
c. to draw intruders attention from the real server and ensnare them (NT pg 181)
d. all of the above

65. Which of the following is a valid Event Log?

a. Startup
b. Application (NT pg 185)
c. User
d. Admin

66. Which of the following is not a log file wrapping option?

a. Overwrite Events as Needed
b. Overwrite Events Older than __ Days
c. Do Not Overwrite Events (Clear Log Manually)
d. Auto Save Events (Clear Log Automatically) (NT pg 187)

67. Which of the following is a command-line utility found in the NT Resource Kit?

a. DUMPEVT.exe
b. EVNTSLOG.exe
c. DUMPEL.exe (NT pg 193)
d. NTSLOG.exe

68. An automated protocol analyzer and an automated event log analyzer are the two primary components of which of the following products?

a. CyberSafe Centrax (page 196)
b. BindView NOSadmin
c. Aelita EventAdmin
d. All of the above

69. Which utility is used to create system policies?

a. SYSPOL.exe
b. POLEDIT.exe (NT PG 210)
c. POLCFG.exe
d. CONFIGSYS.exe

70. What is the name of the share in which system policy files can be found?

a. EXPORT
b. IMPORT
c. NETLOGON (NT PG 210)
d. SYSPOLICY

71. The System Policy settings are found in either NTCONFIG.pol (for NT) or CONFIG.pol (Win9x) in a special folder shared as NetLogOn on the domain controller. Where can this NetLogOn share be found?

a. %systemroot%\system32\config
b. %systemroot%\system\repl\import\scripts
c. %systemroot%\system32\repl\import\scripts (NT pg 210)
d. %systemroot%\system\config

72. Which of the following statements is true?

a. Disabling the registry editing tools will prevent all users from using POLEDIT.exe
b. Disabling the registry editing tools will prevent all but Local Administrators from using POLEDIT.exe
c. Disabling the registry editing tools will prevent all but Local and Global Administrators from using POLEDIT.exe
d. Disabling the registry editing tools will not prevent users from using POLEDIT.exe (NT pg 215)

73. _____ is a utility found in the NT Resource Kit which will allow you to apply registry changes to computers over the network.

a. REGINI.exe
b. RREGCHG.exe (NT pg 217)
c. REGEDIT.exe
d. UPDTREG.exe

74. Which of the following utilities from the NT Resource Kit allows a user to bypass the windows network logon prompt?

a. TRUEPASS.exe
b. AUTOPSWD.exe
c. AUTOLOG.exe (NT pg 218)
d. AUTOSEC.exe

75. By default NT caches the credentials of the last ____ logged on users.

a. 5
b. 1
c. 15
d. 10 (NT pg 221)

76. To prevent users from logging on with cached credentials, even though their account has been disabled, set the registry value _____ = _____ under HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon.

a. CachedLogonsCount = 0 (NT pg 221)
b. CachedLogons = 1
c. CachedLogonsCount =1
d. CachedLogons = 0

77. Which of the following denotes a bad password practice?

a. Creating a password consisting of upper and lower case letters and numbers
b. Creating a password consisting of letters, numbers and ASCII characters
c. Creating a password consisting of a common word (NT pg 224)
d. Creating a password consisting of 8 or more characters

78. Which of the following statements are true in regard to the Schedule Service?

a. AT.exe is a scheduling utility
b. By default only Administrators and Power Users can submit jobs to the schedule service
c. WINAT.exe is a scheduling utility
e. All of the above (NT pg 234 –235)

79. What is the default authentication package in NT 4?

a. MSV1_0.dll (NT pg 237)
b. Kerberos
c. FPNWCLNT.dll
d. RSA

80. In order to disable the automatic creation of 8.3 file name standard what value must be created in the registry?

a. LFNDisable8dot3 = 1
b. NtfsDidable8dot3NameCreation = 1 (NT pg 240)
c. LFNDisable8dot3 = 0
d. NtfsDidable8dot3NameCreation = 0

81. Which of the following statements in regard to Backup auditing are true?

a. Auditing Tape Backups can be accomplished by auditing "Use of User Rights"
b. Backups cannot be audited
c. Auditing Tape Backups can be accomplished by auditing "Use of User Rights" and modifying the registry to add a value named FullPrivilegeAuditing (NT pg 252)
d. Auditing Tape Backups can be accomplished by auditing Backup operators

82. Which of the following are not built in abilities for Server Operators on a Domain Controller?

a. Create and Manage user accounts (NT pg 257)
b. Create common groups
c. Manage folder shares
d. Lock the server

83. Which of the following are not built in abilities for Account Operators on a Domain Controller?

a. Add workstation to domain
b. Create and manage user accounts
c. Assign user rights (NT pg 257)
d. Create and manage global groups

84. Which of the following are not built in abilities for Power Users on a Non-Domain Controller?

a. Create and manage user accounts
b. Create common groups
c. Manage folder shares
d. Assign user rights (NT pg 258)

85. Which of the following is a built in ability for the Everyone group on a Non-Domain Controller?

a. Create and manage local groups
b. Lock the computer (NT pg 258)
c. Manage auditing of system events
d. Manage printer shares

86. Successful prosecution of malicious company employees may depend on?

a. proof that the employee was informed of the penalties involved for inappropriate use
b. proof that the employee was informed that certain actions are prohibited
c. proof that the employee was informed of monitoring activities and information gathering
d. all of the above (NT pg 265-266)

87. Which of the following is not a security-related system policy?

a. common.adm
b. NT.adm (NT pg 280 – 292)
c. winnt.adm
d. windows.adm

88. Which of the following sequences should be used in the boot priority order for Windows 9x?

a. floppy, hard drive, cd-rom
b. hard drive, floppy, cd-rom
c. cd-rom, hard drive, floppy
d. hard drive, cd-rom, floppy (NT pg 295)

89. Which of the following is not a Principle of Firewall Design?

a. Least Restrictive Privilege (NT pg 300 – 303)
b. Fault Tolerance
c. Deny All Except
d. Isolate the Unsecure

90. When combining Firewall components it is not advisable to:

a. combine a bastion host with the interior LAN-attached router (NT pg 305)
b. combine the exterior Internet-attached router with the interior LAN-attached router into one computer
c. have multiple firewalls connecting a LAN to the Internet
d. have multiple Internet-attached routers on the exterior side of the DMZ

Part 2

Internet Information Server

1. Which of the following could be used to determine NewtBios names on a remote system?

   a. nbtstat –r 10.0.0.1
   b. nbtstat –a 10.0.0.1 (IIS pg 13)
   c. nbtstat –v 10.0.0.1
   d. nbtstat –n 10.0.0.1

2. HTTP and FTP transmit data _____.

   a. encrypted with DES
   b. encrypted with Base64
   c. encrypted with RSA
   d. in clear text (IIS pg 29)

3. When using Basic authentication to password protect a file, passwords are encoded using:

   a. **Basic64 (IIS pg 29**)
   b. DES
   c. Nothing
   d. RSA

4. _____ is a "Stateless" protocol which does not remember who you are when you make another request.

   a. TCP/IP
   b. HTTP (IIS pg 31)
   c. NetBEUI
   d. IPX/SPX

5. Which of the following is an example of a scanning and penetration testing tool?

   a. STAT
   b. NESSUS
   c. CyberCop
   d. All of the above (IIS pg 33)

6. When configuring HTTP- only filtering on NT 4.0, which of the following is true?

   a. permit only IP protocol number 6 for TCP (IIS pg 37)
   b. permit only UDP ports
   c. permit only IP protocol number 1 for TCP
   d. permit only IP protocol number 5 for TCP

7. Which ports should be permitted when configuring HTTP-only filtering on NT 4.0?

(1) TCP 80
(2) TCP 135
(3) UDP 139
(4) TCP443

a. 1 and 2
b. 1 and 3
c. 1 and 4 (IIS pg 37)
d. 2 and 3

8. Which of the following is Microsoft's firewall, NAT and proxy server product all rolled into one?

a. FireSafe
b. MSProxyPlus
c. **ISA (IIS pg 40)**
d. RRAS

9. Which of the following are possible components of a firewall?

a. static packet-filtering routers
b. dual-homed hosts
c. switches
d. all of the above (IIS pg 40)

10. Packet-filtering routers and bastion hosts can be configured to double check the hardware addresses of the packets against their source IP address using _____.

a. pkck –n
b. ckpk –n
c. arp –s (IIS pg 43)
d. filtck –s

11. IIS should not be installed on a domain controller. An exception to this rule is:

a. within a small company
b. for use as a honeypot server (IIS pg 51)
c. if it is inside the DMZ
d. all of the above

12. Which of the following services are required on an IIS server used as a web server only?

a. Simple TCP/IP services
b. DHCP client
c. Messanger
d. Windows NTLM Security Support Provider (IIS pg 54)

13. If the Workstation on an IIS server is disabled, which of the following is true?

a. it will cause no significant problems
b. it will cause error messages
c. User Manager for Domains will not work
d. All of the above (IIS pg 55)

14. To determine, manually, if your system is being SYN-flodded execute _____.

a. netstat –a –n |find /i "syn" (IIS pg 62)
b. nbtstat –a –n |find /i "syn"
c. nbtstat –n |find /i "syn"
d. netstat – a |find /i "syn"

15. Which of the following are not authentication methods?

a. negotiate
b. basic realm
c. NTLM
d. SSL (IIS pg 68 – 69)

16. When anonymous users log on, they authenticate using which of the following accounts?

a. ANYM_computername
b. IUSR_computername (IIS pg 71)
c. GUEST_computername
d. IWAM_computername

17. What is the most widely used authentication medhod?

a. SSL
b. DES
c. Basic (IIS pg 75)
d. NTLM

18. In IIS 5.0, the Integrated Windows authentication is also known as _____.

a. Kerberos
b. Negotiate (IIS pg 81)
c. NTLM
d. Basic64

19. Which of the following orders of precedence for selecting the authentication method used is correct?

a. certificate, integrated windows, digest (IIS pg 89)
b. certificate, integrated windows, anonymous
c. basic, integrated windows, certificate
d. anonymous, basic, certificate

20. The "What If Tool" is used to _____.

a. determine access rights to ASPs
b. determine access rights to web pages
c. test application/authentication scenarios (IIS pg 92)
d. determine what other servers are accessible through the IIS server

21. Which of the following is not an IIS folder permission?

a. None (IIS pg 118)
b. Read
c. Directory Browsing
d. Write

22. When NFTS and IIS permissions combine, the effective permission is _____.

a. the sum of the two
b. the NTFS permission
c. the most restrictive of the two (IIS pg 124)
d. the IIS permission

23. What is the Microsoft tool used to help automate the configuration of IIS 5.0 on Windows 2000?

a. IISCONFIG.exe
b. IISLOCK.exe (IIS pg 133)
c. IISAUTOCFG.exe
d. IISCFGMGR.exe

24. What is the default account used to coordinate the activities of web applications running in separate process so they can access the same resources and communicate with each other?

a. IUSR_computername
b. Anonymous
c. IWAM_computername (IIS pg 145)
d. System

25. If not using Site Server, it is recommended, that you unregister the "File System object", which provides web applications with access to hard drives. The command to perform this action is _____.

a. regsvr 32 storage.dll/u
b. regsvr storage.dll/u
c. regsvr page.dll/u
d. regsvr32 scrrun.dll/u (IIS pg 150)

26. The IIS equivalent to the registry is the _____.

a. Metabase (IIS pg 156)
b. IIS Registry
c. Web Registry
d. Metadata

27. Which utility can be used to modify the metabase?

a. metaedit32.exe
b. metadata32.exe
c. metaedit.exe (IIS pg 156)
d. metadata.exe

28. Which of the following can a website operator not do?

a. enable logging
b. change virtual directory paths (IIS pg 164)
c. change IIS permissions
d. set content ratings

29. Which of the following are examples of information that can be logged for the HTTP service?

a. protocol version
b. cookie
c. client IP address
d. all of the above (IIS pg 171)

30. Where is the metabase located by default?

a. %systemroot%\system\MetaBase.bin
b. %systemroot%\system32\MetaBase.bin
c. %systemroot%\system32\Inetserv\MetaBase.bin (IIS pg 156)
d. %systemroot%\system\Inetserv\MetaBase.bin

Part 3

Active Directory

1. What is the primary means of securing servers and desktops, which depends on Active Directory?

   a. Active Directory
   b. DES
   c. NTLM
   d. Group Policy (AD pg 7)

2. What is the command run to promote a Windows 2000 server to become a Domain Controller?

   a. SETUP.exe
   b. PROMOexe
   c. DCPROMO.exe (AD pg 12)
   d. DCSETUP.exe

3. The Active Directory database and log files should _____.

   a. be placed in %systemroot%\NTDS\
   b. be placed in %systemroot%
   c. be placed on the same hard drive
   d. be placed on two separate hard drives (AD pg 14)

4. The System volume is a folder shared as _____.

   a. SYSTEM
   b. SYSVOL (AD pg 15)
   c. ADSYSVOL
   d. NTDS

5. What is the default location of the Active Directory database and log?

   a. %systemroot%\NTDS\ADS
   b. %systemroot%\NTDS (AD pg 15)
   c. %systemroot%\ADS
   d. %systemroot%

6. You cannot run in native mode if _____.

   a. you have NT 4.0 domain controllers
   b. you have NT 4.0 servers
   c. you have NT 4.0 clients
   d. all of the above (AD pg 16)

7. What is the default name of the Active Directory database file?

   a. ntds.mdb
   b. ads.dit
   c. ntds.dit (AD pg 21)
   d. ads.mdb

8. The Scripts subdirectory in the SYSVOL share is shared as _____.

a. SCRIPTING
b. NETLOGON (AD pg 22)
c. NETSCRIPTS
d. SYSSCRIPTS

9. Multi-master replications means that Active Directory changes made on _____.

a. a PDC are automatically replicated on all other PDCs in the domain
b. a BDC are automatically replicated on all other BDCs in the domain
c. a DC are automatically replicated to all other DCs in the domain (AD pg 23)
d. a DC are automatically replicated to all DCs on any Trusted Domain

10. The Active Directory, GUI, tool for displaying and managing replication topology is_____.

a. LDP.exe
b. REPLMGE.exe
c. MGEREPL.exe
d. REPLMON.exe (AD pg 24)

11. Which of the following is not an example of a command-line support tool?

a. NETDIAG.exe
b. SYSDIAG.exe (AD pg 25)
c. ACLDIAG.exe
d. IPSECPOL.exe

12. The Schema Manager snap-in cannot be installed until its DLL has been registered. How is this accomplished?

a. regsvr32.exe schmmgmt.dll (AD pg 27)
b. regedit 32.exe schmmgmt.dll
c. setup.exe schmmgmt.dll
d. regsvr.exe schmmgmt.dll

13. What is the main protocol used to query and edit Active Directory?

a. HTTP
b. LDAP (AD pg 28)
c. SMNP
d. None of the above

14. The default port used by LDAP servers to listen is _____.

a. TCP 445
b. UDP 3269
c. **TCP 389 (AD pg 28**)
d. TCP 88

15. To use a SMTP transport, you must have _____ on some DC and install _____ on the DC with the transport.

a. IIS-SMTP, Certificate Services
b. **Certificate Services, IIS-SMTP (AD pg 33)**
c. TCP/IP, Certificate Services
d. Certificate Services, TCP/IP

16. The Global Catalog is _____.

a. a list of all objects in the Active Directory database
b. a compilation of all Certificates in the Active Directory database
c. **a small subset of the Active Directory database (AD pg 35)**
d. a list of all universal groups contained in the Active Directory dababase

17. Which of the following is not a FSMO master role?

a. PDC Emulator Master
b. GPO Master (AD pg 37)
c. Schema Master
d. Domain Naming Master

18. Which of the following is not a major section in the Active Directory database?

a. Domain Naming Context
b. Configuration Naming Context
c. Schema Naming Context
d. Group Naming (AD pg 43)

19. _____ is an example of a UPN.

a. cn=Administrator,cn=Users.dc=fossen,dc=net
b. cn=jennifer.ou=Austin.ou=sales,dc=fossen,dc=net
c. cn=godzilla,ou=Domain Controllers,dc=fossen,dc=net
d. jason@fossen.net (AD pg 47)

20. A _____ is two or more domains in a hierarchical domain structure where one domain serves as a DNS root domain for the others.

a. forest
b. tree (AD pg 50)
c. two-way trust
d. none of the above.

21. Which of the following groups can only exist in mixed mode environments?

a. Global Security Groups
b. Local Security Groups
c. Universal Security Groups (AD pg 56)
d. Universal Groups

22. Which of the following is a command-line utility for managing Active Directory permissions?

a. DSACL.exe (AD pg 68)
b. ADACL.exe
c. ACL.exe
d. ACLPERM.exe

23. Which of the following utilities allow you to test Active Directory permissions under the security context of a different user, while logged on as an Administrator?

(1) TSTPERM.exe
(2) SU.exe
(3) RUNAS,exe
(4) ADPERM.exe

a. 1 and 2
b. 1 and 3
c. 1 and 4
d. 2 and 3 (AD pg 75)

24. Which of the following, relating to GPOs is False?

a. A GPO is an independent object, not a property of a site, domain or OU
b. A GPO continues to exist even if it is not linked to any containers
c. A GPO can only be linked to one OU (AD pg 86)
d. GPO links bind GPOs to containers

25. Which of the following would be an accurate example of the order GPOs and System Policies would be applied?

a. Local GPOs, NT 4.0 System Policy, Domain GPOs
b. NT 4.0, OU GPOs, Domain GPOs
c. Local GPOs, Site GPOs, OU GPOs (AD pg 89)
d. Site GPOs, OU GPOs, Domain GPOs

26. Which of the following statements is true?

a. A user or group can be made exempt from an existing GPO (AD pg 95)
b. A user must have at least Apply Group Policy permissions to have a GPO applied to their desktop
c. A user must have at least Read Group Policy permissions to have a GPO applied to their desktop
d. user must have at least Create All Child Objects permissions to have a GPO applied to their desktop

27. A Group Policy can be used to install, update, repair and remove applications. However, these applications must support the new Microsoft Installer Service by including a special installation script with the _____ extension.

a. .MIS
b. .WSH
c. .INS
d. .MSI (AD pg 98)

28. Where are the GPO templates stored?

a. %systemroot%\Templates
b. %systemroot%\Security\Templates (AD pg 105)
c. %systemroot%\SYSVol\Security\Templates
d. %systemroot%\SYSVol\Templates

29. The security Configuration and Analysis snap-in can be used to_____.

a. compare your current configuration against a template
b. configure the local machine to match a template
c. export/save the current configuration as a template
d. all of the above (AD pg 107)

30. The User Configuration > Administrative Templates are used to _____.

a. modify the HKEY_Local_Machine key of the user's registry
b. modify the HKEY_Current_Config key of the user's registry
c. modify the HKEY_Current_User key of the user's registry (AD pg 108)
d. modify the HKEY_Users key of the user's registry

Last Updated: September 19th, 2017

Upcoming Training

Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**