Global Information Assurance Certification Paper

Charles John

Option 3

Windows NT Security Step-by-Step

1. Once a hacker obtains the IP addresses of an organization's DNS servers, what command could the hacker use to obtain hostnames and IP addresses of systems in the organization's domain?

   A. tracert
   B. nbtstat
   C. hostname
   D. nslookup

   Correct answer is D. Windows NT page 17.

2. A hacker uses the NBTSTAT command to obtain the following output

   GODZILLA <20> unique
   GODZILLA <00> unique
   MONSTERISLAND <00> group
   MONSTERISLAND <1C> group
   MONSTERISLAND <1B> unique

   From the above what can the hacker determine?

   A. MONSTERISLAND is the Domain Name and GODZILLA is the Domain Master Browser.
   B. GODZILLA is the Domain Name
   C. GODZILLA is an IIS Server
   D. GODZILLA is an Exchange Server

   Correct answer is A. Windows NT page 20 and 21.

3. A wardialer is:

   A. A denial of service attack that attempts to flood a server causing buffer overflows,
   B. A utility that attempts to discover those phone numbers in a given range connected to modems.
   C. A boot sector virus that records a user's keystrokes in a file that can be accessed by the hacker.
   D. A program written to specifically bypass a Checkpoint Firewall.

   Correct answer is B. Windows NT page 23.

4. The single best defense against Internet reconnaissance is:

   A. A password filter that forces all users to maintain an 8 character password that employs alpha-numeric case-sensitive characters, special characters, and ALT keystrokes.

   B. Installation of RRAS on all NT servers

   C. Deployment of a firewall

   D. An IIS server running the proxy service.

   Correct answer is C. Windows NT page 25.

5. Automated protocol analyzers

   A. Are also called Intrusion Detection Systems
   B. Can send administrative alerts
   C. Can launch custom programs
   D. All of the above.

   Correct answer is D. Windows NT page 27.

6. A DMZ should not contain which of the following servers:

   A. DNS Servers
   B. SMTP e-mail servers
   C. HTTP web servers
   D. WINS Servers

   Correct answer is D. Windows NT page 29.

7. The database of a remote WINS server can be downloaded with a Windows NT Resource Kit utility called

   A. WINSBACK.EXE
   B. WINSDMP.EXE
   C. WINSLOAD.EXE
   D. WINSRECV.EXE

   Correct answer is B. Windows NT page 29.

8. Which of the following products would typically be used as a personal firewall to protect a user's home computer?

   A. Checkpoint Firewall-1
   B. ZoneAlarm
   C. Cisco PIX
   D. Axent Raptor Firewall

   Correct answer is B. Windows NT page 34.

9. A SYN flood is

   A. A stream of TCP handshake packets that each request a new TCP session to begin. The source is a non-existent host.
   B. TCP packets with source routing information
   C. An attempt to upload a virus program in fragments so that it can't be identified.
   D. A stream of TCP packets with low-level kernel commands embedded

   Correct answer is A. Windows NT page 40.

10. On most systems all but which can typically be disabled?

    A. Simple TCP/IP Services
    B. OS/2 Subsystem
    C. Server Service
    D. POSIX Subsystem

    Correct answer C. Windows NT page 44 and 45.

11. What command can be used to install Service packs and hotfixes and provides switches that can be used to write batch files for hands-free installations?

    A. HOTFIX.EXE
    B.SRVPACK.EXE
    C. INSTPACK.EXE
    D. UPGRADE.EXE

    Correct answer is D. Windows NT page 47.

12. Performance Monitor can be used to monitor up to ____ remote computers over the network from a central management station.

    A. 10
    B. 20
    C. 25
    D. 50

    Correct answer is C. Windows NT page 52.

13. Performance Monitor can be configured to run as an unattended service on the central management station by using which of the following 2 utilities?

    A. perfview.exe, pmanage.exe
    B. datalog.exe, monitor.exe
    C. perfview.exe, perfset.exe
    D. pmon.exe, pcontrol.exe

    Correct answer is B. Windows NT page 52.

14. Which commands could be used to determine if your system is being SYN flooded?

    A. nbtstat –n | find /I "syn"
    B. nslookup -a –n | find /I "syn"
    C. netstat –a –n | find /I "syn"
    D. netview –a | find /I "syn"

    Correct answer is C. Windows NT page 53.

15. Which of the following files is optional on a Windows NT boot disk, depending if the computer has a SCSI boot disk with the BIOS disabled?

    A. boot.ini
    B. ntldr
    C. ntdetect.com
    D. ntbootdd.sys

    Correct answer is D. Windows NT page 58.

16. Which of the following statements is FALSE?

    A. An Emergency Repair Disk (ERD) can be used to boot the computer.
    B. The command to create the ERD is RDISK
    C. RDISK does not copy the current user accounts database unless the /s switch is added to the end of the command line.
    D. When RDISK is used a set of recovery files is placed in the %systemroot%\repair folder.

    Correct answer is A. Windows NT page 58.

17. To create the Windows NT setup disks, which of the following commands can be used?

    A. winnt /b
    B. winnt /ox
    C. winnt /s
    D. winnt /d

    Correct answer is B. Windows NT page 59.

18. Which command can be used to encrypt the SAM database?

    A. IPSec.exe
    B. DES.EXE
    C. SYSKEY.EXE
    D. SAMCRYPT.EXE

    Correct answer C. Windows NT page 60.

19. To enable the creation of a MEMORY.DMP when a BSOD occurs, which of the following is FALSE

    A. A paging file must exist on the same partition as your operating system.
    B. The paging file must not be located on the same partition as your operating system.
    C. The paging file must be at least as big as the amount of physical RAM.
    D. The System applet in Control Panel allows you to enable the creation of a MEMORY.DMP file.

    Correct answer is B. Windows NT page 69.

20. A windows NT Resource Kit utility called _____ can be used to display detailed information about memory, threads, and Security Access Tokens of running processes.

    A. MEMORY.EXE
    B. WINMSD.EXE
    C. PVIEW.EXE
    D. PERFMON.EXE

    Correct answer is C. Windows NT page 66.

21. A BSOD may be the result of a hacker attempting to cover his actions. A crashdump file can be analyzed with either a command line utility called _____ or a GUI version of the debugger _____bundled with the Platform SDK.

    A. DEBUG.EXE, WINDBUG.EXE
    B. I386KD.EXE, WINDBG.EXE
    C. KERNEL.EXE, WINKRNL.EXE
    D. DBKRNL.EXE, WINKRNL.EXE

    Correct answer is B. Windows NT page 68.

22. Windows NT Server has two built-in user accounts Administrator and Guest. Which statement is FALSE regarding these accounts.

    A. The Administrator and Guest accounts can be renamed but not deleted.
    B. By default, the Administrator account can not be locked out due to excessive bad logon attempts.
    C. The Administrator account can not be renamed. The Guest account can be renamed.
    D. The Guest account on an NT server is disabled by default.

    Correct answer is C. The Administrator account can be renamed. Windows NT page 73.

23. A man-in-the-middle attack occurs when

    A. A hacker attempts to bypass the firewall by exploiting a known bug.
    B. A hacker captures NetLogon channel packets with the intent of modifying them.
    C. A hacker employs social engineering to obtain a password from a valid user.
    D. A hacker installs a replicating virus.

    Correct answer is B. Windows NT page 74.

24. Select the statement that is FALSE. NetLogon channel packets are used for:

A. Pass-thru authentication of users
B. The creation of trusts
C. Directory Replication
D. Domain Controller synchronization.

Correct answer is C. Windows NT page 74.

25. A backup copy of the SAM database can be found in the following path

A. %systemroot%\config
B. %systemroot%\backup
C. %systemroot%\repair
D. %systemroot%\samdb

Correct answer is C. Windows NT page 75.

26. All Security Configuration Editor (SCE) tasks can be performed from the command line using the _____ utility.

A. SCECONFIG.EXE
B. SECEDIT.EXE
C. SCONFIG.EXE
D. SEDITOR.EXE

Correct answer is B. Windows NT page 78.

27. Which command can be used to establish a null user session with the server BRUTUS

A. net view \\BRUTUS\IPC$ "" /user:""
B. net use \\BRUTUS\IPC$ "" /user:""
C. net map \\BRUTUS\IPC$ "" /user:""
D. net use \\BRUTUS\IPC$ "" / user:Administrator

Correct answer is B. Windows NT page 81.

28. The Windows NT Resource Kit has a utility named _____ which can be used to list all users that have the dial-in permission.

    A. DINUSERS.EXE
    B. RASUSERS.EXE
    C. RASMON.EXE
    D. DIALIN.EXE

    Correct answer is B. Windows NT page 82.

29. The _____ utility from SomarSoft is both a GUI and a command line utility which can extract a list of usernames from a remote domain controller. Other settings such as password policy, assigned user rights, running services, share permissions, end NTFS permissions can be obtained.

    A. DumpSec
    B. Extract
    C. NTDump
    D. DACLS

    Correct answer is A. Windows NT page 85.

30. By default, the Windows NT Administrator account can not be locked out by bad logon attempts. What program could be used to lock out the Administrator account for over-the-network authentications?

    A. PASSLOCK.EXE
    B. ADMNLOCK.EXE
    C. PASSPROP.EXE
    D. ADMINPROP.EXE

    Correct answer is C. Windows NT page 88.

31. All processes on Windows NT run under the context of an account. Given the following account types: Local, Global, System
    What is the order of preference?

    A. Local, Global, System
    B. Global, Local, System
    C. System, Local, Global
    D. Local, System, Global

    Correct answer is C. Windows NT page 98.

32. Windows NT Service Pack 3 introduced an optional password filter that can require complex passwords that include: Uppercase Letters, Lowercase Letters, Numbers, and non-alphanumeric symbols. The name of this option is:

    A. SECURE.DLL
    B. PROTECT.DLL
    C. PASSCNTRL.DLL
    D. PASSFILT.DLL

    Correct answer is D. Windows NT page 101.

33. Which utility from Pedestal Software could you use to list account and password policies in force after you have established a null user session to IP address 204.86.29.10?

    A. netview –v 204.86.29.10 policy
    B. netuse –s 204.86.29.10 policy
    C. ntuser –s 204.86.29.10 policy
    D. ntview –v 204.86.29.10 policy

    Correct answer is C. Windows NT page 104.

34. Which statement is FALSE

    A. In Windows NT valid password lengths range from 0 to 14 characters.
    B. Windows NT can track up to 24 prior passwords of a user.
    C. By default, users are required to enter a minimum 6 character password the first time they log in.
    D. A user can be required to keep their password by setting the Minimum Password Age.

    Correct answer is C. Windows NT page 105.

35. Which of the following statements regarding SYSKEY is FALSE?

    A. The System Key can be hidden on the computer on which the utility is run.
    B. The System Key can be stored on a floppy disk.
    C. The System Key can be generated from a password up to 128 characters long.
    D. If the System Key password or floppy is lost, you can remove the password by running the UNCRYPT.EXE utility as long as you have the Administrator's password.

    The correct answer is D. Once SYSKEY is used it is not possible to disable the encryption. Windows NT page 110.

36. For a Windows 95/98 client to support NTLM2 authentication you must:

A. Do nothing for Windows 98, Install Windows 95 service pack 1 for NTLM2 authentication.
B. Install the Directory Services Client from the Windows 2000 CD-ROM. Then make the necessary registry change.
C. Do nothing. Windows 95/98 can not support NTLM2 authentication.
D. Only registry changes are required for Windows 95/98 NTLM2 authentication.

Correct answer is B. Windows NT pages 116 and 117.

37. The NetLogon channel is an

A. Inter-process communication that employs mailslots
B. Inter-process communication that employs a two-way SMB named pipe \\servername\pipe\netlogon for RPC communications.
C. Inter-process communication that employs Winsock and DCOM
D. Inter-process communication that employs NetDDE

Correct answer is B. Windows NT page 119.

38. Encryption and integrity checking of the NetLogon Channel is enabled in the registry. Which of the following is not a valid value that can be entered under the following key?

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

A. SignSecureChannel
B. SealSecureChannel
C. RequireSignOrSeal
D. EncryptSecureChannel

Correct answer is D. Windows NT page 120.

39. What is Social Engineering?

A. An attempt by a hacker to trick a user into providing a user account and password by exploiting the user's desire to provide assistance.
B. Training provided to users by management regarding computer system policies.
C. Computer policies employed when an Extranet is created between two companies.
D. Computer policies put in place when a Virtual Private Network (VPN) is implemented.

Correct answer is A. Windows NT page 122.

40. Using Reverse Social Engineering:

A. A hacker calls the help desk pretending to be a new employee and requests assistance.
B. A hacker determines what applications an organization uses and calls to offer assistance, to provide free upgrades and patches.
C. A hacker prevents an organization from accessing resources by initiating DOS attacks.
D. A hacker attempts to discover user accounts and passwords of users determined to be offsite.

Correct answer is B. Windows NT page 124 and 125.

41. In Windows NT, a local group can not contain:

A. Global groups from the same domain
B. Global groups from trusted domains.
C. User accounts from trusted domains
D. Other local groups.

Correct answer is D. Windows NT page 135.

42. Which of the following statements is FALSE?

A. A global group cannot contain other global groups.
B. A global group cannot contain user accounts from another domain.
C. A global group cannot contain local groups.
D. Any server, including member servers can contain global groups.

Correct answer is D. In Windows NT global groups exist on domain controllers. Windows NT page 135.

43. Which of the following statements is FALSE?

A. Windows NT share permissions apply over the network, while NTFS permissions apply only for local logon.
B. Windows NT share permissions apply over the network, while NTFS permissions apply both over the network and for local logon.
C. Windows NTFS permissions are not available on FAT partitions.
D. Only NTFS partitions can be audited. FAT partitions cannot be audited.

Correct answer is A. NTFS permissions apply both over the network and locally. Windows NT page 136.

44. Identify the FALSE statement.

A. NTFS is a transaction based file system for fault system.
B. NTFS is more efficient than FAT on volumes larger than 400 MB
C. NTFS supports detailed auditing.
D. NTFS partitions do not support native compression. A third-party tool must be used,

Correct answer is D. Windows NT page 136.

45. Identify the FALSE statement.

A. The No Access NTFS permission overrides any other permission granted.
B. The Full Control NTFS permission overrides the No Access permission.
C. Share permissions do not apply to console users.
D. When determining effective rights over the network both share and NTFS permissions must be considered,

Correct answer is B. Windows NT page 137.

46. Bob is a member of two groups SALES and OPERATIONS.
His Share level and NTFS permissions to the folder OPS are as follows:

	SALES	OPERATIONS
Share	READ	FULL CONTROL
NTFS	LIST	CHANGE

Bob is accessing the share from across the network. What are Bob's effective permissions?

A. READ
B. CHANGE
C. FULL CONTROL
D. LIST

Correct answer is B CHANGE. Bob's share level permissions are least restrictive and cumulative which is FULL Control. Bob's NTFS permissions are least restrictive and cumulative which is CHANGE. Between the Share Level and NTFS permissions the most restrictive is applied. This is CHANGE.
Windows NT page 137.

47. The Windows NT default share permission is:

A. The Everyone Group No Access. Permissions must be specifically assigned.
B. The Everyone Group Full Control
C. The Everyone Group Read
D. The Everyone Group Change

Correct answer is B. Windows NT page 142.

48. When Service Pack 3 or greater is applied to Windows NT a new dynamic group that can be seen when assigning rights and permissions is:

A. Valid Users
B. Authenticated Users
C. Global Users
D. Encrypted Users

Correct answer is B. Windows NT page 142.

49. The Windows NT Resource kit has a utility called _____ which copies share permissions from one share to another.

E. SHRCOPY.EXE
F. PERMCOPY.EXE
G. SHARECPY.EXE
H. COPYSHR.EXE

Correct answer is B. Windows NT page 144.

50. Which of the following groups includes null session users?

i. Authenticated Users
ii. Guests
iii. Everyone
iv. Domain Users

Correct answer is C. Windows NT page 143.

51. Windows NT includes a command utility called _____ that can be used to manage NTFS permissions on files.

A. PERMIT.EXE
B. RIGHTS.EXE
C. CACLS.EXE
D. NTPERMS.EXE

Correct answer is C. Windows NT page 144.

52. Which of the following Windows NT Resource Kit utilities can be used to manage shared folders and printers on remote systems?

A. RMTSHARE.EXE
B. REMOTE.EXE
C. RSHARE.EXE
D. RMANAGE.EXE

Correct answer is A. Windows NT page 144.

53. The Windows NT Resource Kit utility _____ allows you to see all the shares on multiple systems simultaneously.

    a. SHAREVIEW.EXE
    b. NETVIEW.EXE
    c. NETWATCH.EXE
    d. SHOWSHRS.EXE

    Correct answer is C. Windows NT pages 147 and 148.

54. To prevent null session users from listing sharenames, the following registry value is added to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

    A. DisAllow
    B. RestrictAnonymous
    C. DenyAnonymous
    D. RevokeAnonymous

    Correct answer is B. Windows NT page 149.

55. The %systemroot% folder, typically WINNT is shared as _____ and given the _____ permission.

    A. WINNT$, change
    B. ADMIN$, read only
    C. EXEC$, read only
    D. EXEC$, change

    Correct answer is B. Windows NT page 150.

56. Permissions set on the _____ registry key determine remote access permissions to the registry.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\

    A. RegCtl
    B. Winreg
    C. RegPermit
    D. RegAllow

    Correct answer is B. Windows NT page 153.

57. What is a named pipe?

    A. A share name to which remote services and applications can connect implemented as the NPFS file system.
    B. The service that manages both long and short names of a file.
    C. A cache that opens the most frequently used files.
    D. A NetWare compatible file system.

    Correct answer is A. Windows NT page158.

58. Windows NT offers an upgrade over the native packet filtering. The upgrade is called _____ and can filter packets based on Source IP address, Destination IP address, source port, destination port, protocol type, and direction of travel.

    A. Network Monitor
    B. Systems Management Service
    C. Routing and Remote Access Service (RRAS)
    D. Routing Internet Protocol (RIP)

    Correct answer is C. Windows NT page 164.

59. The authentication protocol used by dial-in clients and RAS servers is

    a. CHAP
    b. SLIP
    c. L2F
    d. PPP

    Correct answer is A. Windows NT page 162.

60. A rootkit can be defined as

    a. A Windows NT Resource Kit used to test NT for security holes.
    b. A set of files that patch or replace critical operating system files to allow undetected complete control of a system.
    c. A utility that tests the boot sector of a Windows NT system to determine if a boot sector virus has infected the system.
    d. A Microsoft TechNet collection of articles related to NT Security.

    Correct answer is B. Windows NT page 174.

61. Which of the following statements is TRUE.

    a. When implementing Auditing, the administrator should audit all files and folders on the server. There is no performance penalty associated with auditing.
    b. Only failed logons and failed attempts to access files and folders can be audited.
    c. Audit policy on a domain controller applies to all domain controllers.
    d. Administrators, Server Operators, and Account Operators can establish the audit policy.

    Correct answer is C. Windows NT page 177.

62. Custom events can be written to the audit logs of local or remote systems by using the Windows NT Resource Kit command line utility

    a. EVNTLOG.EXE
    b. LOGEVENT.EXE
    c. LOGCOPY.EXE
    d. AUDITLOG.EXE

    Correct answer is B. Windows NT page 180.

63. Which of the following is not a valid Event Log

    a. System
    b. User
    c. Security
    d. Application

    Correct answer is B. Windows NT page 185.

64. The default event log size is

    A. 1 MB
    B. 5 MB
    C. 512K
    D. 10 MB

    Correct answer is C. Windows NT page 188.

65. When an event log fills to its maximum capacity the wrapping options include all except:

    a. Overwrite Events as Needed.
    b. Overwrite Events older than X days, where X is configurable
    c. Archive existing log automatically and generate new daily log.
    d. Do not Overwrite Events.

    Correct answer is C. Windows NT page 188.

66. In high security environments it is possible to cause a server to shutdown when the Security log fails by changing the registry setting to a value of 1 for

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

    a. StopOnLogFilled
    b. CrashOnAuditFail
    c. SecurityLogStop
    d. ServerLogFail

    Correct answer is B. Windows NT page 190.

67. The Windows NT Resource Kit includes a command-line utility named _____ used to dump the contents of a log to an ASCII text file.

    a. DUMPLOG.EXE
    b. LOGDUMP.EXE
    c. DUMPEL.EXE
    d. EVNTDUMP.EXE

    Correct answer is C. Windows NT page 193.

68. Which of the following methods may not be effective against a rootkit.

    a. Reapply the service pack that was copied to the server.
    b. Use the Windows NT Resource Kit WinDiff utility.
    c. Use a third-party tool such as Tripwire or INTACT
    d. Reapply a service pack from CD-ROM

    Correct answer is A. A hacker may have compromised the files in a directory on the server that stores the service pack as well as the operating system files. Windows NT page 198.

69. The program used to create a system policy is

    a. POLICY.EXE
    b. SYSPOL.EXE
    c. POLEDIT.EXE
    d. POLMNGR.EXE

    Correct answer is C. Windows NT page 208.

70. System policy settings are stored in a file called _____ for Windows NT and _____ for Windows 9x users.

A. NTCONFIG.POL, 9XCONFIG.POL
B. NTCONFIG.POL, CONFIG.POL
C. CONFIGNT.POL, CONFIG95.POL
D. NTPOL.CON, 95POL.CON

Correct answer is B. Windows NT page 210.

71. Systems will look for the policy files in a special share called

    a. REPL
    b. ADMIN
    c. NETLOGON
    d. POLICY

    Correct answer is C. Windows NT page 210.

72. The location of the share that systems search for policy files is

    a. %systemroot%\system32\config
    b. %systemroot%\system32\policy
    c. %systemroot%\system32\repl\import\scripts
    d. %systemroot%\system32\repl\export

    Correct answer is C. Windows NT page 210.

73. A system policy template defines which registry settings an Administrator has the option of configuring. Templates are ASCII files with an extension of

    a. MSI
    b. ADM
    c. POL
    d. TXT

    Correct answer is B. Windows NT page 211.

74. A Windows NT Resource utility that can be used to modify the registry from the command line is by accepting a text file that defines registry settings is

    a. REGINI.EXE
    b. REGMOD.EXE
    c. REGALTER.EXE
    d. REGFIX.EXE

    Correct answer is A. Windows NT page 217.

75. A Windows NT Resource Kit utility that allows a user to bypass entering a User account and password when logging on is

    a. PASSLOG.EXE
    b. AUTOLOG.EXE
    c. AUTOPASS.EXE
    d. AUTOPSWD.EXE

    Correct answer is B. Windows NT page 218.

76. Cached credentials are used by Windows NT when

    a. A user attempts to logon, but no domain controller is available for authentication.
    b. Used only by the SYSTEM Account to logon on.
    c. Can only be used by a member of the Administrators group.
    d. Refer to Digital Certificates not user authentication

    Correct answer is A. Windows NT page 221.

77. By default Windows NT caches the credentials of the last ___ logged on users.

    A. 5
    B. 10
    C. 15
    D. 20

    Correct answer is B. Windows NT page 221.

78. Windows NT Network Monitor is

    a. A protocol analyzer.
    b. A Resource Kit utility used to monitor processor utilization of selected servers.
    c. A utility to inform administrators real-time as to when selected users log in
    d. An SNMP manager

    Correct answer is A. Windows NT page 226.

79. Which statement is true?

    a. In Windows NT, printer drivers run in user mode.
    b. In Windows NT, printer drivers run in kernel mode.
    c. By default, regular users cannot install printer drivers.
    d. It is not possible to make registry changes that allow only Administrators, Print Operators and Power users to install printer drivers.

    Correct answer is B. Windows NT page 233.

80. The command line to submit a job to the Schedule service is _____. The Windows NT Resource Kit GUI program to schedule jobs is called _____.

    a. STARTAT.EXE, WINSTART.EXE
    b. AT.EXE, WINAT.EXE
    c. SCHEDULE.EXE, WINSCHED.EXE
    d. SCHEDAT.EXE WINSCHED.EXE

    Correct answer is B. Windows NT page 234.

81. By default, which of the following groups can submit new jobs to the schedule service

    a. Administrators and Server Operators only.
    b. Administrators and Power Users only.
    c. Any member of the Users Group
    d. Administrators, Server Operators, Backup Operators

    Correct answer is B. Windows NT page 235.

82. The Windows NT Resource Kit utility _____runs as a service and prevents all users except Administrators and Power Users from accessing floppy drives on a system.

A. FLOPHALT.EXE
B. FLOPSTOP.EXE
C. FLOPLOCK.EXE
D. FLOPFAIL.EXE

Correct answer is C. Windows NT page 236.

83. Windows NT includes one sub-authentication and notification package by default:

    a. OS2CLNT.DLL
    b. POSIX.DLL
    c. FPNWCLNT.DLL
    d. UNIXCLNT.DLL

    Correct answer is C. Windows NT page 238.

84. Which of the following statements is true?

A. Windows NT NTFS support native file encryption.
B. Windows 2000 NTFS supports EFS, Encrypting File System.
C. Neither Windows NT nor Windows 2000 support file encryption.
D. If an encrypted file system is backed up to tape, the files are decrypted first.

Correct answer is B. Windows NT page 249.

85. In order to audit who has performed a tape backup

A. It is sufficient to audit the use of user rights
B. In addition to auditing the use of user rights, the following registry change must be made:

HKEY_LOCAL_MACHINE\System\CurrentControl\Set\Control\Lsa
Add the value name FullPrivilegeAuditing and set it to data value 1

C. Only the above registry change need be made.
D. It is not possible to audit who has performed a tape backup.

Correct answer is B. Windows NT page 252.

86. On a Domain Controller, members of the Server Operators built-in group can by default

A. Add a workstation to the domain.
B. Create and Manage user accounts
C. Manager folder shares
D. Create and manage local groups.

Correct answer is C. Windows NT page 257.

87. On a domain Controller, members of the Account Operators built-in group can

A. Assign User rights
B. Manage Auditing of system events
C. Create and manage global groups
D. Format hard drives

Correct answer is C. Windows NT page 257.

88. A marked file in relation to honey pots

A. Is a file with the archive bit set
B. Is a file with special identifying traits that when found on a hacker's system could only have originated from the honey pot system.
C. A file set for deletion
D. A file that has been found to be corrupt possibly due to a virus.

Correct answer is B. Windows NT page 269.

89. Which Statement concerning a Firewall is not considered to be a best practice?

A. A firewall should deny all traffic not explicitly permitted.
B. A Firewall should permit all traffic not explicitly denied.
C. A Firewall should fail in such a way that it denies access and closes connections.
D. The only path to and from the network should be the firewall.

Correct answer is B. Windows NT page 300.

90. Which of the following statements regarding firewalls is true.

A. Firewalls should reject source-routed packets.
B. Packets from the Internet with source addresses of the internal network should be rejected.
C. A and B are both true
D. A and B are both False.

Correct answer is C. Windows NT page 300.

IIS

1. Which of the following commands could a hacker use to determine the NetBios names registered on a remote system that has an IP address of 204.86.29.10?

   A. netstat –a 204.86.29.10
   B. nbtstat –A 204.86.29.10
   C. nslookup –a 204.86.29.10
   D. nbtstat –R 204.86.29.110

   Correct answer is B. IIS Security page 13.

2. When using basic authentication to password protect a file, passwords are encoded in

   A. DES
   B. MD5
   C. Base64
   D. IPSec

   Correct answer is C. IIS Security page 27.

3.When setting up a filter for an HTTP only server you should permit only _____ and _____ if using SSL.

   A. TCP port 80, TCP port 443
   B. TCP port 80, UDP port 443
   C. UDP port 80, TCP port 443
   D. UDP port 80, UDP port 443

   Correct answer A. IIS Security page 35

4.The Windows NT Resource Kit _____ program is a command-line utility that can be used to dump the contents of local or remote event logs to a text file.

   A. event.exe
   B. logrpt.exe
   C. dumpel.exe
   D. listevnt.exe

   Correct answer C. IIS Security pages 39-40.

5. When a hacker attempts to slip packets past a firewall by spoofing the hacker is:

A. Using an IP option indicating that the packet should not be routed according to the router's tables but instead by information found in the header of the packet.

B. Sending packets with a return IP address that is valid on the company's internal network.

C. Flooding the destination with packets that are the maximum transmission size.

D. Attempting to get the destination to execute an illegal command in system mode.

Correct answer B. IIS Security page 40.

6.Packet filtering routers and bastion hosts can be configured to double-check the hardware addresses they receive against their source IP addresses. MAC antries may be placed in cache by using the command:

A. arp –c
B. rarp –c
C. rarp –s
D. arp –s

Correct answer D. IIS Security page 41.

7. If an IIS server in the DMZ has virtual folders which map to shared folders inside the LAN, the interior router will have to be opened to allow _____ traffic to the LAN.

A. http
B. smb-NetBios
C. ftp
D. NetBEUI

Correct answer B. IIS Security page 45.

8. _____ combines the shared folders of multiple machines into a single virtual directory structure.

A. NCP
B. NFS
C. DFS
D. PFS

Correct Answer C. IIS security page 47.

9. The LMHOSTS file on an IIS server located in the DMZ may need to be configured with the IP address of a domain controller. The LMHOSTS file can be found in:

A. %SystemRoot%\system32\repl\import\scripts
B. %SystemRoot%\system32\drivers\etc
C. %SystemRoot%\system32\netlogon
D. %SystemRoot%\system32\config

Correct answer B. IIS Security page 51.

10. Ideally, an IIS server should be installed as:

A. A Primary Domain Controller (PDC)
B. A. Backup Domain Controller (BDC)
C. A stand alone Windows NT Server
D. A DHCP Server

Correct answer C. IIS Security page 51.

11.An IIS server used as a Web server only requires the _____ service

A. Spooler
B. DHCP Client
C. Computer Browser
D. Remote Procedure Call (RPC)

Correct answer D. IIS Security page 53.

12. Which of the following statements is true?

A. The anonymous user account on an IIS server is identical to the null user account.
B. The anonymous user account on an IIS server is identical to the System account.
C. The anonymous user account on an IIS server is identical to the Guest account.
D. IIS creates a specific user account IUSR_*computername* to represent the anonymous user.

Correct answer D. IIS Security page 62.

13. Your clients use Netscape as their browser. Which of the following authentication methods are supported?

A. Digest
B. Integrated Windows
C. Basic
D. Fortezza

Correct answer C. IIS Security page 65.

14. The authentication method developed by the NSA and used by some government agencies is:

A. SSL
B. Fortezza
C. RSA
D. MD5

Correct answer B. IIS Security page 78.

15. _____ authentication takes precedence over all other authentication methods.

A. Anonymous
B. Digest
C. Certificate
E. Basic

Correct answer C. IIS Security page 79

16. To access Certificate Services from your browser, you must access

A. http://servername/certsrv
B. http://servername/IIS
C. http://servername/inetpub
D. http://servername/wwwroot

Correct answer A. IIS Security page 86.

17. Which of the following statements is true?

A. If you do not install a Certificate Trust List on the IIS server to let it know which CA's to trust, then IIS will not trust any Certificate Authorities.

B. If you do not install a Certificate Trust List on the IIS server to let it know which CA's to trust, then IIS will trust all Certificate Authorities.

C. If you do not install a Certificate Trust List on the IIS server, the SSL authentication method is not available.

D. If you do not install a Certificate Trust List on the IIS server, your browser will prompt you to identify the Certificate Authority when necessary.

Correct answer B. IIS Security page 89.

18. Which of the following statements regarding Directory Service certificate authentication is true?

A. To use DS mapping, the IIS 5.0 server must be a stand-alone server.

B. Once DS mapping is enabled on the IIS server, no other certificate authentication option will function.

C. DS mapping does not allow you to benefit from many-to-one mapping.

D. Extensive manual configuration of mapping rules is required if DS mapping is enabled.

Correct answer B. IIS Security page 95.

19. Identify the false statement.

A. SSL is a technology for the encryption of data transmitted between webserver and browser.

B. SSL is a technology for the verification that this data has not been altered or corrupted during transit.

C. SSL is a technology available for http and ftp.

D. SSL is a technology that verifies the identity of the webserver to the client.

Correct answer C. IIS Security page 100.

20. SSL uses either _____ or _____bit session encryption keys

A. 40,64
B. 56,64
C. 40,128
D. 56,128

Correct answer C. IIS Security page 103.

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

A. none
B. Scripts Only
C. Scripts and Executables
D. Directory Browsing.

Correct answer D. IIS Security page 108.

22. Which of the following IP address restrictions will have an adverse effect on performance when used for IP blocking.

A. Listing single IP addresses to block.
B. Using a range of IP addresses based on the network ID and the subnet mask.
C. Using a domain name.
D. Using supernetting with non-default subnet masks

Correct answer C. IIS Security page 115.

23. The Internet Server Security Configuration Tool, _____, helps to automate the configuration of IIS 5.0 on Windows 2000.

A. IISecure.exe
B. IISLock.exe
C. IISManage.exe
D. IISConfig

Correct answer B. IIS Security page 119.

24. An individual who has been setup as a website operator can perform all of the following except:

A. Set content expiration.
B. Set content ratings
C. Enable logging.
D. Throttle Bandwidth

Correct answer D. IIS Security page 134.

25. The main IIS process is called _____. Web-based applications can run within it.

A. inetinfo.exe
B. iisadmin.exe
C. iisapp.exe
D. iisweb.exe

Correct answer A. IIS Security page 144.

26. When web applications run isolated or out-of-process, the user account under which they run is:

A. IUSR_*computername*
B. Administrator
C. IWAM_*computername*
D. anonymous

Correct answer C. IIS Security page 147.

27. If you are 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 do this is.

A. regedit scrrun.dll /u
B. regedt32 scrrub.dll /u
C. regsvr32 scrrun.dll /u
D. regrest scrrub.dll /u

Correct answer C. IIS Security page 152

28. IIS has its own configuration database located:

A. %systemroot%\system32\drivers\etc\metabase.bin
B. %systemroot%\system32\repl\metabase.bin
C. %systemroot%\system32\Inetserv\metabase.bin
D. %systemroot%\system32\inetpub\metabase.bin

Correct answer C. IIS Security page 158.

29. The utility _____ is intended for use in a clustered environment with multiple identical IIS boxes. This utility will copy metabase data from the local server to other servers over the network.

A. IISCopy.exe
B. IISMerge.exe
C. Iissync.exe
D. IISdup.exe

Correct answer C. IIS Security page 160.

30. A utility to convert W3C Extended log files to NCSA common format is

A. Convert.exe
B. Convlog.exe
C. translate.exe
D. W3CNCSA.exe

Correct answer B. IIS Security page 165.

Active Directory

1. The command to promote a Windows 2000 server to a domain controller is

A. UPGRADE.EXE
B. DCPROMO.EXE
C. DCSETUP.EXE
D. DCCONTROL.EXE

Correct answer B. Active Directory page 12.

2. The system volume is a folder shared as _____ containing logon scripts, NT 4.0 System policy files, and Windows 2000 Group Policy information.

A. SYSMGR
B. WINVOL
C. SYSVOL
D. WINSYS

Correct answer C. Active Directory page 15.

3. The default location for the Active directory database file is

A. %systemroot%\system32\repl\ntdis.dit
B. %systemroot%\sam\ntdis.dit
C. %systemroot%\config\ntdis.dit
D.%systemroot%\NTDS\ntds.dit

Correct answer D. Active Directory page 21.

4. The AD GUI tool _____ is an LDAP query and edit utility while the _____ AD GUI displays and manages replication topology.

A. lquery.exe, replmon.exe
B. ldp.exe, replmon.exe
C. ldp.exe, repl.exe
D. lquery.exe, repl.exe

Correct answer B. Active Directory page 24.

5. The Schema manager snap-in cannot be installed until its DLL has been registered with the operating system. This is accomplished with the command

A. regedit.exe schmmgmt.dll
B. regedt32.exe schmmgmt.dll
C. regsvr32.exe schmmgmt.dll
D. setup schmmgmt.dll

Correct answer C. Active Directory page 27.

6. The main protocol used to query and edit AD is

   A. HTTP
   B. LDAP
   C. SSL
   D. SMNP

   Correct answer is B. Active Directory page 28.

7. The Active Directory Services Interface (ADSI) is a generic interface for any vendor's directory services. Which of the following can NOT be accessed via ADSI?

   A. IBM Lotus Notes
   B. Netscape Commerce Server
   C. Microsoft Exchange Server
   D. SQL Server 7.0

   Correct Answer D. SQL Server is a Relational Database Management System (RDBMS) not an LDAP Directory. Active Directory page 29.

8. There are two ways to run WSH. From the command line use _____. For GUI interaction use _____.

   A. WSCRIPT.EXE, CSCRIPT.EXE
   B. CSCRIPT.EXE, WSCRIPT.EXE
   C. CSCRIPT.EXE, VBSCRIPT.EXE
   D. CSRUN.EXE, WSRUN.EXE

   Correct answer is B. Active Directory page 30.

9. Replication between sites is manually configured. Inter-Site transports to convey data between DCs in different sites can be either _____ for fast reliable links or _____ for slow or unreliable links.

   A. RPC-over-IP, SMTP
   B. RPC-over-IP, SNMP
   C. SMTP, RPC-over-IP
   D. SMB-over-IP, SNMP

   Correct answer is A. Active Directory pages 32 and 33.

10. The SYSVOL share is replicated automatically by

    A. SMTP
    B. Distributed File System (DFS)
    C. File Replication Service (FRS)
    D. Replicator

    Correct answer is C. Active Directory page 34.

11. _____ Servers contain the most often needed data from the AD of all domains in the enterprise.

    A. Schema Master
    B. RID Master Server
    C. PDC Emulator Master Server
    D. Global Catalog Server

    Correct answer is D. Active Directory page 35

12. Which of the following is NOT a major section in the Active Directory database called “naming contexts”

    A. Domain Naming Context
    B. Schema Naming Context
    C. User Naming Context
    D. Configuration Naming Context.

    Correct answer is C. Active Directory page 43.

13. Which of the following is an example of a User Principal name (UPN)

    A. cn=james,ou=Engineering,dc=bigco,dc=net
    B. james@bigco.net
    C. james.engineering.bigco.net
    D. james

    Correct answer is B. Active Directory page 47.

14. A Windows 2000 domain and its subdomains all have, effectively

    A. No trusts between them.
    B. One-way non-transitive trusts from the subdomains to the root domain
    C. Two-way transitive trusts between them
    D. One-way transitive trusts from the subdomains to the root domain.

    Correct answer is C. Active Directory page 49.

15. Trust relationships are implemented by:

    A. The Distributed File System Service (DFS)
    B. NetLogon RPC channels
    C. Kerberos
    D. SMB with NetBIOS

    Correct answer is B. Active Directory page 51.

16. Universal Groups can NOT contain the following:

    A. Users
    B. Global groups from any domain.
    C. Local Groups
    D. Other Universal Groups

    Correct answer is C. Active Directory page 56.

17. Which of the following statements is true?

    A. A distribution group cannot be assigned rights or permissions
    B. Universal security groups can be created in mixed mode.
    C. The more distribution groups a user is a member of, the more time it will take for the user to log in.
    D. A security group can be assigned rights and permissions but can not be used for e-mail distribution lists.

    Correct answer is A. Active Directory page 57 and 58.

18. The Windows 2000 Resource Kit includes a command-line utility for managing AD permissions. The name of this utility is:

    A.CACLS.EXE
    B. DSACLS.EXE
    C. ADACLS.EXE
    D. WINCLS.EXE

    Correct Answer is B. Active Directory page 66.

19. A command line utility that can list the permissions on AD objects and containers but not set permissions is:

    A. DSACLS.EXE
    B. DSVIEW.EXE
    C. ENUMPROP.EXE
    D. ADSHOW.EXE

    Correct answer is C. Active Directory is C.

20. The _____ command which is part of the Resource Kit and the _____ command which comes with Windows 2000 allow you to launch programs under the security of a different user while you are logged on as an Administrator.

    A. SU.EXE, RUNAS.EXE
    B. RUNAS.EXE, SU.EXE
    C. RUNDIFF.EXE, SU.EXE
    D. SETUSER.EXE, RUNAS.EXE

    Correct answer is A. Active Directory page 75.

21. Null User LDAP access to your directory can be accomplished by.

A. WSH Scripts
B. LDP.EXE
C.A only
D. Both A and B.

Correct answer is D. Active Directory page 75.

22. Pedestal Software produces a host-based Intrusion Detection System called _____ that includes a module for detecting changes to LDAP compatible directories such as Microsoft Active Directory, Novell NDS, and Lotus Notes.

A. DETECT
B. INTACT
C. LDFIND
D. DISCOVER

Correct answer is B. Active Directory page 76.

23. Which of the following statements is true?

A. If a GPO is created but not linked to a site, domain, or OU then the GPO will not be used.
B. A single GPO can be linked to only one OU.
C. A GPO is a property of a site, domain, or OU. It is not an independent object.
D. If a GPO link is removed, the GPO itself deleted.

Correct answer is A. Active Directory page 86.

24. Consider the following list of GPOs and NT 4.0 System policies:

    1. Site GPOs
    2. NT 4.0 System Policy
    3. Domain GPOs
    4. Organizational Unit GPOs (in nested order)
    5. Local GPOs (stored on the machine not the AD)

    The correct order of application is:

    A. 1,2,3,4,5
    B. 2,5,1,3,4
    C. 5,2,1,3,4
    D. 2,5,4,3,1

    Correct answer is B. Following the acronym 4LSDOU. Active Directory page 89

25. Which of the following statements is FALSE?

    A. You can disable just the user-related settings or just the computer-related settings.
    B. You can disable a single setting within a GPO.
    C. Disabled settings in a parent container are not inherited by all subcontainers within it. Subcontainers settings remain in effect.
    D. If you create separate GPOs for user and computer settings, and then disable the unused portion of the GPO, logon performance will improve.

    Correct answer is C. Active Directory pages 93 and 94.

26. Which of the following statements is FALSE.

    A. To create or edit a GPO, a user requires at least Read and Write permissions on that GPO.
    B. To change permissions on a GPO, a user must have full control of it.
    C. If a user can read and write to a GPO, the user can assign the GPO to any container.
    D. It is possible for a user to link and unlink GPOs to a site, domain, or OU but not be able to modify the GPO.

    Correct answer is C. Active Directory page 96.

27. A Group Policy can be used to install, update, repair, or remove applications. These applications must support a special installation script with the _____ filename extension.

    A. MIS
    B. MSI
    C. ASP
    D. VBS

    Correct answer is B. Active Directory page 98.

28. Security Settings options are determined by a template used by the GPO. Templates define the options available and what they are set to by default. Template files are text files with an extension of _____ and are stored in _____

    A. txt, %systemroot%\system32\config
    B. oem, %systemroot%\system32\config
    C. inf, %systemroot%\security\templates
    D. vbs, %systemroot%\security\templates

    Correct answer is C. Active Directory page 105.

29. Which of the following statements regarding the Windows 2000 Security Configuration and Analysis snap-in is FALSE:

    A. You can compare your current configuration against a template.
    B. You can export and save your current configuration as a template.
    C. This snap-in can access both local and remote machines.
    D. This snap-in can only be used on the local machine.

    Correct answer is C. Active Directory page 107.

30. The GPO command line utility _____ checks GPO for consistency and version numbers, displays detailed information about GPOs not available in the snap-ins, and can browse GPOs based on their name or GUID.

    A. scangpo.exe
    B. gpotool.exe
    C. gpresult.exe
    D. gposhow.exe

    Correct answer is B. Active Directory page 111.

.