Global Information Assurance Certification Paper

Practical Assignment for
GIAC Certified Windows NT Security Administrator (CGNT)
90 Multiple Choice Question Examination

Tim Buchanan

September 23, 2000

1. In which of the following typical phases of attack does a hacker gather information that could be potentially useful for further intrusion or attack?
   A. Denial of Service attacks
   B. Access resources over the network
   C. Reconnaissance
   D. Avoid detection

   Best answer is C, page 14 of Windows NT Security: Step-by-Step v3.5

2. Once a hacker has determined the IP addresses of a company's DNS servers, what utility can be used to obtain hostnames and IP addresses for the same company's computer systems?
   A. NSLOOKUP.EXE
   B. PING.EXE
   C. NBTSTAT.EXE
   D. HOSTNAME.EXE

   Best answer is A, page 17 of Windows NT Security: Step-by-Step v3.5

3. Once a hacker has determined the IP addresses of a company's active computer systems, what utility can be used to obtain NetBios names to help determine what Windows NT services are running on the active computer systems?
   A. NSLOOKUP.EXE
   B. PING.EXE
   C. NBTSTAT.EXE
   D. HOSTNAME.EXE

   Best answer is C, page 18 of Windows NT Security: Step-by-Step v3.5

4. The definition of wardialer is:
   A. A utility used by hackers to automate the dialing of the same phone number repeatedly with the intention of damaging RAS servers or modems attached to personal computers
   B. A utility used by hackers to automate the dialing of every phone number in a given range with the intention of discovery RAS servers and modems attached to personal computers
   C. A utility used by hackers to implement IP address spoofing
   D. None of the above

   Best answer is B, page 22 of Windows NT Security: Step-by-Step v3.5

5. Which of the following is the single best defense against Internet reconnaissance?
   A. Installing the latest Microsoft service pack
   B. Deploying a firewall
   C. Deploying an automated protocol analyzer
   D. Installing Microsoft or Netscape proxy server

   Best answer is B, page 24 of Windows NT Security: Step-by-Step v3.5

6. Which of the following is not true regarding automated protocol analyzers?
   A. Is a complete Intrusion Detection System (IDS)
   B. Detects and responds to scanning and other suspicious activities in real-time
   C. Can send administrative alerts, launch programs, and perform TCP resets
   D. Should be deployed outside the firewall

   Best answer is A, page 31 of Windows NT Security: Step-by-Step v3.5

7. Which of the following does not limit information from DNS and WINS servers?
   A. Implement public and private DNS servers
   B. Maintain only essential records on public DNS servers
   C. Maintain false records on public DNS servers
   D. Block Internet access to internal DNS and WINS servers

   Best answer is C, page 32 of Windows NT Security: Step-by-Step v3.5

8. Which of the following is not a method to conceal or hide the presence of RAS servers:
   A. Not publishing the RAS servers phone numbers on the company website or phone directory
   B. Educating employees not to reveal the phone number to others
   C. Using a phone number for the RAS server that does not fall into the range of public phone numbers used by the company
   D. Installing a honeypot RAS server

   Best answer is D, pages 36-37 of Windows NT Security: Step-by-Step v3.5

9. Which of the following is a purpose of Denial of Service (DOS) attacks:
   A. To simply annoy the system administrators
   B. Seek financial harm against the firm by preventing access to essential services for significant periods of time
   C. To purposely reboot a server once a Trojan Horse has been installed
   D. All of the above

   Best answer is D, page 41 of Windows NT Security: Step-by-Step v3.5

10. What are the characteristics of a DOS attacks on an Internet accessible server?
    A. The server suddenly and continuously running at 95% CPU utilization or above
    B. The server having repeated Blue Screen of Deaths
    C. The server services unexpectedly fail
    D. All of the above

    Best answer is D, page 43 of Windows NT Security: Step-by-Step v3.5

11. A _____ is a stream of TCP handshake packets that each request a new TCP session to begin.
    A. SYN Flood
    B. Ping of Death
    C. WinNuke
    D. BSOD

    Best answer is A, page 44 of Windows NT Security: Step-by-Step v3.5

12. What is the second best defense against DOS attacks?
    A. Installing the latest Microsoft service pack
    B. Deploying a firewall
    C. Deploying an automated protocol analyzer
    D. Installing Microsoft or Netscape proxy server

    Best answer is A, page 45 of Windows NT Security: Step-by-Step v3.5

13. Service Packs must be reapplied whenever the configuration of the server is changed.
    A. True
    B. False

    Best answer is A, page 46 of Windows NT Security: Step-by-Step v3.5

14. Which of the following does not prevent against DOS attacks on Windows NT?
    A. Disable non-essential services, options, protocols, protocol bindings and drivers
    B. Install the latest patches and hotfixes
    C. Ensure that the system partition is formatted as FAT
    D. Stay on top of new developments in security

    Best answer is C, pages 47-53 of Windows NT Security: Step-by-Step v3.5

15. Which of the following does not prevent against a Blue Screen of Death caused by lack of diskspace?
    A. Dedicating one partition just for the operation system files
    B. On a print server, changing the location of the spool files
    C. Using Programmed I/O (PIO) hard drive controllers which rely upon the system CPU rather than bus-mastering hard drive controllers
    D. Placing a page file sized at RAM+11MB in at least one other partition, preferably on a different physical drive

    Best answer is C, pages 55-56 of Windows NT Security: Step-by-Step v3.5

16. One approach to prepare for recovery of DOS attacks is to install multiple installation of Windows NT into different folders on the same volume. However the number of times Windows NT can be installed on a single volume is restricted to:
    A. Two installations
    B. Three installations
    C. Four installations
    D. The free space available on the installation volume

    Best answer is D, page 58 of Windows NT Security: Step-by-Step v3.5

17. Which of the following statements is false regarding Emergency Repair Disks (ERD)?
    A. An ERD can be used to boot the computer
    B. An ERD can repair essential registry hives: user accounts database, security policy, new user profile, default user profile, software information and system configuration
    C. An ERD can compare the checksums of operating systems files against the checksums listed in Setup.log
    D. An ERD can inspect and replace the boot sector on x86 systems only

    Best answer is A, pages 60-61 of Windows NT Security: Step-by-Step v3.5

18. Which of the following commands is use to create the three Windows NT setups disks?
    A. SETUP.EXE /S
    B. WINNT.EXE /S
    C. SETUP.EXE /OX
    D. WINNT.EXE /OX

    Best answer is D, page 61 of Windows NT Security: Step-by-Step v3.5

19. RDISK.EXE command line copies the original SAM to the ERD with only the original Administrator and Guest accounts with their original passwords.
    A. True
    B. False

    Best answer is A, page 62 of Windows NT Security: Step-by-Step v3.5

20. Which of the following two statements best facilitate a quick recovery of crashed servers after a DOS attack?
    A. Maintaining up-to-date binary drive images of servers fully configured hard drives
    B. Configuring the servers with a hard drive caddy to allow the interchange of fully configured hard drives
    C. Maintaining up-to-date server backups with regular testing
    D. Maintaining server installation CDs and up-to-date configuration documentation in a safe, well known location

    Best answers are A and B, page 64 of Windows NT Security: Step-by-Step v3.5

21. Which of the Windows NT utilities listed below would not be appropriate for DOS Attack analysis?
    A. Network Monitor, preferably the version shipped with Microsoft Systems Management Server (SMS)
    B. Performance Monitor
    C. Event Viewer
    D. User Manager for Domains

    Best answer is D, pages 66-70 of Windows NT Security: Step-by-Step v3.5

22. Which two of the following statements is true regarding Windows NT built-in Administrator and Guest accounts?
    A. Both the Administrator and Guest accounts are disabled by default
    B. Both the Administrator and Guest accounts can be deleted
    C. Both the Administrator and Guest accounts can be renamed
    D. The Administrator account cannot be locked out due to bad logon attempts

    Best answers are C and D, page 76 of Windows NT Security: Step-by-Step v3.5

23. A _____ attack is the hijacking of the SMB session between a client and a server enabling the hacker to impersonate a legitimate user and exploit that user's access rights.
    A. Password guessing
    B. Wscript.KakWorm virus
    C. Man-in-the-middle
    D. None of the above

    Best answer is C, page 77 of Windows NT Security: Step-by-Step v3.5

24. Which of the following statements is false regarding Microsoft Security Configuration Editor (SCE)?
    A. The graphical SCE is Microsoft Management Console snap-in
    B. The graphical SCE can compare the local and remote system settings against a template
    C. The command-line SCE is SECEDIT.EXE
    D. In Windows 2000, all options configurable through the SCE can be implemented through Group Policy to automate the configuration of remote systems

    Best answer is B, pages 79-81 of Windows NT Security: Step-by-Step v3.5

25. Which of the commands can be used to establish a "null session" with the Windows NT server named SERVER1?
    A. NET USE \\SERVER1\IPC$ "" /USER:""
    B. NET USE * \\SERVER1
    C. NET USE \\SERVER1\IPC$ "" /USER:GUEST
    D. NET USE \\SERVER1\C$ "" /USER:""

    Best answer is A, page 84 of Windows NT Security: Step-by-Step v3.5

26. What Windows NT Resource Kit utility can be used to list all user accounts that have dial-in permission?
    A. RASUSERS.EXE
    B. NTUSER.EXE
    C. LIST.EXE
    D. RASLIST.EXE

    Best answer is A, page 85 of Windows NT Security: Step-by-Step v3.5

27. Which of the following is both a GUI and command-line third-party application for viewing security information such as usernames, groups, rights, services, and password policies?
    A. DumpSec
    B. User Manager for Domains
    C. SuperCACLS
    D. NT Command Line Security Tool

    Best answer is A, page 87 of Windows NT Security: Step-by-Step v3.5

28. Which of the following is not an approach to protect the Administrator account?
    A. Assign a very strong password that includes extended ASCII characters
    B. Enable account lockout with the Service Pack 3 or later utility called PASSPROP.EXE
    C. Disable the default Administrator account
    D. Rename the default Administrator account and create a honeypot Administrator account

    Best answer is C, pages 89-91 of Windows NT Security: Step-by-Step v3.5

29. Which of the following statements is true regarding Guest accounts? Select all that apply.
    A. By default, the Guest account is disabled on Windows NT Workstation and Windows NT Server
    B. The Guest account can be deleted
    C. The Guest account cannot be renamed and therefore a honeypot Guest account cannot be created
    D. None of the above

    Best answer is D, pages 92 of Windows NT Security: Step-by-Step v3.5

30. Which of the following statements is false regarding role (or shared) accounts?
    A. Role accounts should never be used
    B. Role accounts should have strictly limited in rights, permissions and functionality through mandatory profiles, system policy, workstation restrictions, etc.
    C. Role accounts should never be used as a general-purpose account
    D. None of the above statements are false

    Best answer is A, pages 93-94 of Windows NT Security: Step-by-Step v3.5

31. Which of the following suggestions is false regarding contractors, guests and temporaries?
    A. Consider creating a temporary domain with a two-way trust with the company domain just for contractors until their work is finished
    B. The user accounts of the contractors, temporaries and guests should be configured when appropriate with logon hour restrictions, workstation restrictions, no dial-in permission, and account expiration dates
    C. Use the Description field of an account's properties to name the company employee who is in charge of that contractor, temporary or guest
    D. None of the above

    Best answer is A, pages 95-96 of Windows NT Security: Step-by-Step v3.5

32. Due to network logons occur transparently (unless access is initially denied), identical local accounts and passwords in separate domains behave as if trust relationships are not required with accessing foreign domains. The same is true for identical global accounts and password in separate domains.
    A. True
    B. False

    Best answer is B, page 97 of Windows NT Security: Step-by-Step v3.5

33. When a service starts it is run under a service account. When assigning a service account to a service what is the preferred order of preference from a security standpoint?
    A. Local account, global account, system account
    B. System account, local account, global account
    C. Services should only be run with global accounts with a strong password
    D. Services should only be run with system accounts allowing the service to interact with the desktop

    Best answer is B, pages 98-99 of Windows NT Security: Step-by-Step v3.5

34. Service Pack 3 and later includes an optional password filter which can require more complex passwords which include a combination of uppercase, lowercase, numbers and non-alphanumeric symbols. The name of this password filter is _____.
    A. PASSFILT.DLL
    B. PASSFILT.EXE
    C. SYSKEY.DLL
    D. SYSKEY.EXE

    Best answer is A, pages 101-102 of Windows NT Security: Step-by-Step v3.5

35. Except for password expiration, it is not possible to enforce different account and password policies for different users.
    A. True
    B. False

    Best answer is A, page 104 of Windows NT Security: Step-by-Step v3.5

36. Which one of the following third-party utilities can attach to multiple domain controllers and remotely check the strength of the SAM database passwords. This utility uses a pre-computed database of approximately 60 million password hashes and if a weak password is found it can: force the user to change the password at next logon, disable the account, send an email to the administrator and/or execute a batch file or program?
    A. L0phtCrack
    B. Quakenbush Password Appraiser
    C. SomarSoft DumpSec
    D. CyberSafe Centrax

    Best answer is B, pages 106-107 of Windows NT Security: Step-by-Step v3.5

37. Which of the following third-party utilities can extract and attempt to crack password hashes taken from: local or remote domain controllers with administrative rights, Emergency Repair Disks, tape backups of domain controllers and over-the-network authentication sessions with a special packet sniffer?
    A. L0phtCrack
    B. Quakenbush Password Appraiser
    C. SomarSoft DumpSec
    D. CyberSafe Centrax

    Best answer is A, page 109 of Windows NT Security: Step-by-Step v3.5

38. The _____ utility is available with Service Pack 3 or later and can strongly encrypt the passwords in the SAM.
    A. PASSFILT.DLL
    B. PASSFILT.EXE
    C. SYSKEY.DLL
    D. SYSKEY.EXE

    Best answer is D, page 109-110 of Windows NT Security: Step-by-Step v3.5

39. NTLMv2 authentication, which prevents password sniffer utilities from extracting password hashes from over-the-network logon sessions, is not automatically enabled when Service Pack 4 is installed.
    A. True
    B. False

    Best answer is A, pages 112-113 of Windows NT Security: Step-by-Step v3.5

40. Which of the following statement is false regarding NetLogon channel?
    A. The NetLogon channel is a two-way, SMB named pipe for RPC communications which implement pass-through authentication and accounts synchronization.
    B. All Windows NT computers (PDC, BDC, member server and stand-alone) establish NetLogon channels
    C. With Service Pack 4 installed combined with a registry setting, all NetLogon channel data can be encrypted and digitally signed for integrity to increase security
    D. None of the above statements are false

    Best answer is B, pages 114-117 of Windows NT Security: Step-by-Step v3.5

41. The definition of Social Engineering is:
    A. The devious art of tricking users into revealing information that will assist one in overcoming a network's security measures such as fooling users into revealing their usernames and passwords
    B. The gathering of information that is potentially useful for further intrusion or attack
    C. The informing of employees of appropriate organizational computer policies and penalties
    D. None of the above

    Best answer is A, page 118 of Windows NT Security: Step-by-Step v3.5

42. Identify the three parts of Reverse Social Engineering below.
    A. The hacker directly contacting the administrator in an attempt to obtain a user account and password
    B. The hacker making the targets aware that the he or she is available for help
    C. The hacker causing or waiting for problems to occur
    D. The hacker extracting useful information and building trust while assisting the targets with their problems

    Best answers are B, C and D, pages121-122 of Windows NT Security: Step-by-Step v3.5

43. Which of the following simple and inexpensive defenses against Social Engineering is false?
    A. Educated your users by printing labels to be placed on users computer or monitors indicating that the only computer support they should call for assistant is, for example, (425) 649-4357
    B. Post flyers on the bulletin boards in break areas and lunchrooms with the same message as above but also include the company's RAS numbers
    C. Once every quarter, the administrator sends an email to the entire organization with different security reminders
    D. Provide technical support staff with an online database of employee names, phone numbers, email addresses and departmental information

    Best answer is B, pages 123-125 of Windows NT Security: Step-by-Step v3.5

44. According to 1996 FBI report on computer crime, approximately 75% of security breeches are perpetrated by legitimate internal users. Which of the following lists the internal users from most to the least threat?
    A. Full-time employees, part-time and contract employees, and computer hackers
    B. Part-time and contract employees, computer hackers, and full-time employees
    C. Computer hackers, full-time employees, part-time and contract employees
    D. None of the above

    Best answer is A, page 127 of Windows NT Security: Step-by-Step v3.5

45. Which of the following is not a best practice for administering groups, rights and permissions?
    A. Organize users into Global Groups based on common needs and roles
    B. Assign rights and permissions to Local Groups and then add Global Groups to the Local Groups
    C. Assign rights and permissions to Global Groups
    D. Devise a group naming standard which indicates its proper rights and/or permissions

    Best answer is C, page 130-131 of Windows NT Security: Step-by-Step v3.5

46. NTFS permissions are not effective when an administrator logs into the server console and accesses the server's local hard drives.
    A. True
    B. False

    Best answer is B, page 132 of Windows NT Security: Step-by-Step v3.5

47. Tony is a member of three groups: Accounting, Payroll and Budget. What is his effective permission on the 2000 shared folder on an NTFS volume given the following?

Groups	*NTFS Permissions on 2000*	*Share Permission on 2000*
Accounting	Change	Read
Payroll	Change	Full Control
Budget	Read	Change

A. Change
B. Read
C. Full Control
D. None of the above

Best answer is A, pages 133-134 of Windows NT Security: Step-by-Step v3.5

48. The default NTFS permission is _____ for the Everyone group and the default Share permission is _____ for the Everyone group.
A. Null (no permission assigned), null
B. No access, no access
C. Full control, full control
D. Read, Read

Best answer is C, page 136 of Windows NT Security: Step-by-Step v3.5

49. Select all that apply. The Everyone group includes:
A. Users from untrusted domains
B. Users who have no Windows NT domain
C. Anonymous Internet users
D. Null session users

Best answer is A, B, C and D, page 138 of Windows NT Security: Step-by-Step v3.5

50. Which of the following groups is only available after Service Pack 3 or later is installed and is the set of all domain users from the local domain and all trusted domains?
A. Network
B. Everyone
C. Interactive
D. Authenticated Users

Best answer is D, page 138 of Windows NT Security: Step-by-Step v3.5

51. Which of the following two programs are third-party utilities used to better manage NTFS permissions?
A. Security Configuration Manager
B. SuperCACLS
C. NT Command Line Security Tool
D. CACLS.EXE

Best answers are C and D, pages 140-141 of Windows NT Security: Step-by-Step v3.5

52. Which of the two groups have all three rights: Backup Files and Directories, Restore Files and Directories, and the Bypass Traverse Checking?
    A. Everyone
    B. Backup Operators
    C. Domain Users
    D. Server Operators

    Best answers are B and D, page 142-143 of Windows NT Security: Step-by-Step v3.5

53. The _____ Windows NT Resource Kit utility allows you to see all shares on multiple systems simultaneously from Explorer. In particular, this utility allows you to view hidden shares, filter to see only those shares in use, list the exact files open on each share and see the users who are accessing them.
    A. NETWATCH.EXE
    B. NTUSER.EXE
    C. BROWSTAT.EXE
    D. LIST.EXE

    Best answer is A, pages 143-144 of Windows NT Security: Step-by-Step v3.5

54. What value name is added to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA registry to preventing null users from listing folder and printer share names?
    A. RestrictAnonymous
    B. RestrictShares
    C. NoShares
    D. NoAnonymous

    Best answer is A, page 145 of Windows NT Security: Step-by-Step v3.5

55. Administrative shares in Windows NT includes the hidden shares of the root of all volumes (e.g., C$, D$, E$, etc.) with Full Control permissions to Administrators, as well as the hidden share of the %SystemRoot% folder (e.g., usually C:\Winnt) shared as _____ with _____ permissions to the Administrators.
    A. WINNT$, Full Control
    B. WINNT$, Read
    C. ADMIN$, Full Control
    D. ADMIN$, Read

    Best answer is D, pages 146-147 of Windows NT Security: Step-by-Step v3.5

56. Which of the following two statements regarding network access to the registry is true?
    A. By default on Windows NT Server, only Administrators can access the registry
    B. By default on Windows NT Workstation, only Administrators can access the registry
    C. By default on Windows NT Server, the Everyone group has read access to certain portions of the registry such as HKEY_LOCAL_MACHINE\Software and HKEY_LOCAL_MACHINES\System
    D. By default on Windows NT Workstation, the Everyone group has read access to certain portions of the registry such as HKEY_LOCAL_MACHINE\Software and HKEY_LOCAL_MACHINES\System

    Best answers are A and D, page 148 of Windows NT Security: Step-by-Step v3.5

57. By default, the permissions granted to the null session user will be the permissions assigned to the Everyone group when accessing shares.
    A. True
    B. False

    Best answer is A, page 151 of Windows NT Security: Step-by-Step v3.5

58. Which of the following statements regarding named pipes is false?
    A. A named pipe is a share name in which users can connect to
    B. A named pipe is implemented as a file system: named piped file system (NPFS)
    C. The UNC pathname for named pipes has the form \\servername\pipe\pipename
    D. A named pipe is secretly used by applications and services to communicate with one another

    Best answer is A, pages 153-156 of Windows NT Security: Step-by-Step v3.5

59. Which of the following statements is not an advantage of MS-CHAPv2?
    A. MS-CHAPv2 uses the NT method of response during challenge/response authentication
    B. MS-CHAPv2 has stronger encryption keys that are different every session
    C. MS-CHAPv2 uses different encryption keys for the send and receive paths
    D. None of the above

    Best answer is D, page 158 of Windows NT Security: Step-by-Step v3.5

60. When a user on the LAN remains connected even after his or her logon hours have expired, Windows NT forces the user to logoff. Similarly, for a RAS user who remains logged on after their logon hours expire, Windows NT can forcibly disconnect the user.
    A. True
    B. False

    Best answer is B, page 159 of Windows NT Security: Step-by-Step v3.5

61. Which of the following statements is false regarding Network Monitoring Agents?
    A. Network Monitor Agent is a protocol analyzer or packet sniffer
    B. The Network Monitor console does the actual work of capturing packets
    C. Access to the Network Monitor Agent is password protected but the encryption scheme is easily defeated
    D. You can use the Network Monitor console application itself to detect other Network Monitor users

    Best answer is B, page 161 of Windows NT Security: Step-by-Step v3.5

62. Microsoft operating systems uses the _____ protocol to access shared folders, printers and named pipes over the network.
    A. NetBios
    B. TCP/IP
    C. Server Message Block (SMB)
    D. NCP

    Best answer is C, page 162 of Windows NT Security: Step-by-Step v3.5

63. Assume a Windows NT Server has Service Pack 3 or later installed and the required registry setting has been set to enable digital signing of SMB messages. Which two of the following situations will not use SMB signing?
    A. When the client logs in with the Guest account
    B. When the null session is used to attach
    C. When the client logs in with the Administrator account
    D. None of the above

    Best answer A and B, pages 162-164 of Windows NT Security: Step-by-Step v3.5

64. Which of the following Internet Information Server (IIS) security tips is false?
    A. Remove any IIS features that are not being used (e.g., FTP, SMTP, NNTP, Index Server, etc.)
    B. Disable the IIS anonymous account (e.g., IUSR_servername)
    C. Unbind the Wins Client (TCP/IP) from the network adapter card attached to the Internet
    D. Delete all sample file and scripts that come with IIS

    Best answer is B, page 165 of Windows NT Security: Step-by-Step v3.5

65. In order for a skilled intruder to avoid detection, which of the following actions from a hacker can an administrator expect? Select all that apply.
    A. The hacker may disable, modify, flush or destroy audit logs
    B. The hacker may use accounts of others to impersonate them
    C. The hacker may install a trapdoor to permit re-entry later
    D. The hacker may install a Windows NT rootkit

    Best answers are A, B, C, and D, pages 168-170 of Windows NT Security: Step-by-Step v3.5

66. A _____ is a set of files that patch or replace critical operating system files in order to allow undetected and complete control of a system.
    A. Trojan horse
    B. Rootkit
    C. Virus
    D. Patch

    Best answer is B, page 170 of Windows NT Security: Step-by-Step v3.5

67. To detect intruders, the most important step to take is to _____.
    A. Enable auditing
    B. Setup a honeypot server
    C. Detect modified operation system files
    D. All of the above

    Best answer is A, page 171 of Windows NT Security: Step-by-Step v3.5

68. Which of the following statements regarding Windows NT auditing is true? Select all that apply.
    A. Windows NT auditing is enabled in User Manager
    B. An audit policy on a domain controller applies to all domain controllers while an audit policy on a Windows NT Workstation, member server or stand-alone applies to just that one system
    C. After auditing has been enabled, folders, files, registry keys or printers must be individually configured with auditing options desired
    D. Excessive auditing can significantly slow system performance

    Best answers A, B, C, and D, pages 173-174 of Windows NT Security: Step-by-Step v3.5

69. What Windows NT Resource Kit utility can you use to write your own custom events from the command line or scripts?
    A. LOGEVENT.EXE
    B. DUMPEL.EXE
    C. DUMPEVT.EXE
    D. EVNTSLOG.EXE

    Best answer is A, page 176 of Windows NT Security: Step-by-Step v3.5

70. What is the name of a server or resource designed to ensnare intruders, log their actions, and alert administrators?
    A. Poison honeypot
    B. Honeypot
    C. Bastion host
    D. DMZ

    Best answer is B, page 177 of Windows NT Security: Step-by-Step v3.5

71. Which of the following statements regarding Event Logs is false?
    A. The three event logs visible in Event Viewer are stored as individual files in the \%SystemRoot%\System32 folder
    B. The volume containing these files should be formatted with NTFS
    C. NTFS auditing should also be applied to the event log files themselves
    D. The Manage Auditing and Security Log right should be assigned only to the Administrators group and perhaps only to certain individuals within that group

    Best answer is A, pages 181-182 of Windows NT Security: Step-by-Step v3.5

72. The default size of the System, Security and Application event log is _____ and can be configured to a maximum size of approximately _____.
    A. 512KB, 4.2GB
    B. 1MB, 4.2GB
    C. 512KB, 1MB
    D. 1MB, 1MB

    Best answer is A, page 184 of Windows NT Security: Step-by-Step v3.5

73. When the CrashOnAuditFail has been set to 1 in a server's HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa and the Security logs fills to capacity, the server is automatically shutdown. CrashOnAuditFail will automatically be set to 2 and when the server is rebooted only the Administrator will be able to logon at the console or over the network.
    A. True
    B. False

    Best answer is A, page 186 of Windows NT Security: Step-by-Step v3.5

74. Which of the following Event Log utilities can: alter the Event Log data so that it will be more easily imported in SQL, Access, Oracle, etc.; dump only previously undumped data to avoid duplicates; and dump binary data even from remote machines.
    A. DUMPEL.EXE
    B. DUMPEVT.EXE
    C. Event Log Monitor
    D. Aelita Event Admin

    Best answer is B, pages 188-190 of Windows NT Security: Step-by-Step v3.5

75. Which of the following statements are true regarding Automated Event Log Analyzers? Select all that apply.
    A. An Automated Event Log Analyzer is one of two components of an Intrusion Detection System (IDS)
    B. An Automated Event Log Analyzer continuously scans event logs in search of patterns of entries that indicate attacks, break-ins or suspicious behavior
    C. An Automated Event Log Analyzer can take defensive action send alerts, run "panic scripts", disable the user's account, etc.
    D. None of the above

    Best answers A, B, and C, pages 191-192 of Windows NT Security: Step-by-Step v3.5

76. Which of the following is not an approach to locate modified files if tampering is suspected?
    A. Reapply the Service Pack and post-Service Pack hotfixes from copies on the server's hard drive
    B. Run a comparison of files on the hard drive against a tape backup drive
    C. Purchase and install Tripwire for Windows NT
    D. Run CSDIFF on a file that you suspect has been modified with a reference copy

    Best answer is A, pages 193-194 of Windows NT Security: Step-by-Step v3.5

77. What document should be proactively created in order to save time, prevent harm, reduce chaos, and even avoid legal problems in an event that an intruder is actually discovered?
    A. Risk management plan
    B. Incident Response plan
    C. Security policy and procedure document
    D. Risk analysis document

    Best answer is B, page 196 of Windows NT Security: Step-by-Step v3.5

78. What utility creates system policies that will allow the administrator to make registry changes to hundreds of computers and these changes will follow the user from system to system?
    A. SYSEDIT.EXE
    B. POLEDIT.EXE
    C. POLMGR.EXE
    D. REGEDT32.EXE

    Best answer is B, page 202-204 of Windows NT Security: Step-by-Step v3.5

79. A System Policy file contains the settings for all users, groups and computers in the domain; there is not a separate file for each of these objects.
    A. True
    B. False

    Best answer is A, page 206 of Windows NT Security: Step-by-Step v3.5

80. The _____ Windows NT Resource Kit utility permits a user to configure the system to automatically log on with a specifiable username and password. In addition, what value name is added to the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon registry can an administrator add to each workstation to prevent this utility from running?
    A. AUTOLOG.EXE, DefaultUserName and Default Password
    B. AUTOLOGON.EXE, DefaultUserName and Default Password
    C. AUTOLOG.EXE, DisableAutoLogon
    D. AUTOLOGON.EXE, DisableAutoLogon

    Best answer is A, page 214 of Windows NT Security: Step-by-Step v3.5

81. If Service Pack 4 or previous is installed, which utilities can add the user account of a locally logged on user to the Administrator or Domain Admins group? Select all that apply.
    A. GetAdmin
    B. SecHole
    C. SecHoleD
    D. L0phtCrack

    Best answers are A, B, and C, page 215 of Windows NT Security: Step-by-Step v3.5

82. Which of the following is false regarding caching of logon credentials?
    A. By default, Windows NT caches the credentials of the last ten logged on users
    B. Cached credentials are a security risk because it can allow a user to log on even if that user's account has been disabled or deleted
    C. To disable cached credentials, set HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount to 0.
    D. Disabling cached credentials will also prevent the last user to successfully login from appearing in the Windows NT security window

    Best answer is D, page 217 of Windows NT Security: Step-by-Step v3.5

83. Which of the following it false regarding screen savers to better secure workstations?
    A. It is recommended that a password-protected screensaver be enabled on every system with short (10 to 15 minutes) timeout period
    B. Password protected Windows NT screensavers are not synchronized with the user's regular account password
    C. When the screensaver is activated, it has the same effect as locking the workstation
    D. Some personal firewall products include a feature to disable all network communications when the screensaver activates

    Best answer is B, page 219 of Windows NT Security: Step-by-Step v3.5

84. Which of the following is not a recommended approach to locate or prevent protocol analyzers on a network?
    A. Windows NT Network Monitor utility can be used to discover other Network Monitor users
    B. Use an Enterprise Management System to search for the files of the most popular protocol analyzer applications on the hard drives of users
    C. Execute L0phtCrack to locate protocol analyzers
    D. Implement a 100% switched network

    Best answer is C, pages 222-223 of Windows NT Security: Step-by-Step v3.5

85. A company is recommended to make their virus scanning software available to employees for use at home since they will probably bring in software from home and transfer data files back and forth.
    A. True
    B. False

    Best answer is A, page 228 of Windows NT Security: Step-by-Step v3.5

86. The worst-case scenario is when hackers have physical access to target servers.
    A. True
    B. False

    Best answer is A, page 239 of Windows NT Security: Step-by-Step v3.5

87. Which of the following are recommended actions to better secure backup media? Select all that apply.
    A. Set backup software to encrypt the data written to the tape
    B. Lock backup media in a fireproof safe or cabinet for short-term storage
    C. For long-term storage, arrange for backup media to be stored at a trusted offsite location
    D. Enforce a strict inventory backup media at all times

    Best answers are A, B, C, and D, pages 244-245 of Windows NT Security: Step-by-Step v3.5

88. To prevent a hacker from booting a Windows NT server into another operating system from a floppy and then using utilities to access NTFS volumes without regard to permissions, which of the following actions should an administrator perform? Select all that apply.
    A. Set the boot priority in the BIOS to boot first from the hard drive and then from the floppy drive; a password must be set to protect the BIOS from modification
    B. Disable the floppy drive in the BIOS; a password must be set to protect the BIOS from modification
    C. Set a password in the BIOS that is required to boot the server into any operating systems, not just Windows NT
    D. Physically remove the floppy and CD-ROM drive because the BIOS password can be easily compromised

    Best answer is D, pages 246-247 of Windows NT Security: Step-by-Step v3.5

89. Which of the following actions should a company not perform to improve the likelihood that users will be informed appropriate use policies and penalties?
    A. The Security Administrator should include computer use policies in the employee manual
    B. The Security Administrator should include a summary of policies on the network logon banner
    C. The Security Administrator should install keyboard and mouse monitoring software on every users computer and log all information
    D. The Security Administrator should email policies that send receipts when opened by recipients

    Best answer is C, page 261 of Windows NT Security: Step-by-Step v3.5

90. Which of the following actions are recommended for a Security Administrator to protect him or herself? Select all that apply.
    A. The Security Administrator is advised to log and document his or her actions to the fullest extent reasonably possible
    B. The Security Administrator is advised to log and document his or her correspondence with management and other administrators
    C. The Security Administrator is advised to obtain complete authority over any given project, or no authority whatsoever.
    D. The Security Administrator is advised to not make false claims of expertise

    Best answer is A, B, C, and D, pages 271-272 of Windows NT Security: Step-by-Step v3.5