# Global Information Assurance Certification Paper

**Securing NT: Step-by-Step**
**Stephen Collins Steve.C005**

This 150 question multiple-choice examination is based on the information presented by Jason Fossen at the SANS Parliament Hill 2000 session.

They are divided into 3 sections corresponding to the 3 books used during the session and are in the following format:

1) *Question……:(Page reference, correct choice)*
   A) *Option 1*
   B) *Option 2*
   C) *Option 3*
   D) *Option4*

---

Start Questions: Securing Windows NT: Step-by-step

1) NBTSTAT can be used to obtain what kind of information? (p. 20-21, B)
   A) CPU, ram, hard drive space and manufacturer of a system
   B) Logged-on users, domain, groups, services and agents running on a system
   C) Network protocols, NIC drivers, encryption types on a system
   D) Password policies and logon history of users

2) Port scanning is useful because it: (p. 17-18, C)
   A) Allows you to list and attach to open shares on a system
   B) Displays usernames and password hashes when clients logon
   C) Shows what ports are listening on a system
   D) Lists the IP range a computer is accepting data from

3) The InterNIC can be used to obtain information on: (p. 17, B)
   A) All fully qualified domain names on the internet
   B) All fully qualified domain names on the internet except military and government records
   C) Only military and government records
   D) The correct spelling of all domain names

4) NS lookup is used to query a: (p. 17, B)
   A) Web server for the named services running on it
   B) DNS server for hostnames and IP address in a domain
   C) Firewall for the internal networks naming schema
   D) File server to look for null sessions

5) A network's topology can be mapped-out once active hosts are found by using: (p. 17, A)
   A) Tracert
   B) Net
   C) Nbtstat
   D) Ping

6) A "Wardialer" utility can be used to help circumvent a firewall by: (p. 23, C)
   A) Sending a large number of fragmented packets, overloading the firewall
   B) Entering the actual IP address' of systems behind the firewall to get around it
   C) Automatically dial all the telephone numbers a company uses to discover computer modems
   D) Repeatedly calling the system administrator and distract him while you try to hack the firewall

7) Social Engineering is: (p. 23-24, C)
   A) Programming your computer to speak the same language as your target's network in order to gain access
   B) Designing a "TEST" network the same as your target's to discover any weakness
   C) A way of tricking users and administrators into revealing information which can be used to break into their network
   D) Training your employees to exercise caution on the interest

8) If an administrator has had some technical/security problems with their network, this information might be found on: (p. 16, C)
   A) The InterNIC
   B) www.hacking.org
   C) Usenet postings
   D) DNS servers

9) The single best defense against internet reconnaissance is: (p. 25, B)
   A) Locking your servers in a secure room
   B) A firewall
   C) A sound password policy
   D) Disable service accounts

10) RRAS, an upgrade to RAS, is more secure because it: (p. 25-26, A)
   A) Can enforce multiple packet-filtering rules on each interface
   B) Encrypts the data being sent over the modem
   C) Adds another layer of password protection to the system
   D) Hides the IP address of the server

11) A firewall should be designed to: (p. 300, C)
   A) Examine and filter all incoming packets
   B) Examine and filter all outgoing packets
   C) Examine and filter both incoming and outgoing packets
   D) Examine both incoming and outgoing packets

12) A firewall that can dynamically open and close holes in the filtering rules on-the-fly is called: (p. 26, B)
   A) A bastion host
   B) A stateful firewall
   C) A static firewall
   D) A passfilt firewall

13) An automated protocol analyzer is used to: (p. 27, C)
   A) Track and log client network usage
   B) Cache logon credentials for password verification
   C) Detect and respond to scanning and other suspicious activities in realtime
   D) Limit certain types of traffic based on available bandwidth

14) An I.D.S., when threatening pockets are detected, can: (p. 27, D)
   A) Change your network's IP address
   B) Launch an automated DoS attack against the offending system
   C) Re-route the traffic to a competitor's network
   D) Trigger alerts, signal the firewall to block an IP address, and reset TCP sessions

15) A WINS server provides: (p. 28, D)
   A) Host name to IP address mappings
   B) Service name to IP address mappings
   C) E-mail address to IP address mappings
   D) Netbios name to IP address mapping

16) Public and private DNS servers should be located: (p. 28, D)
   A) On the Internet side of the firewall
   B) Public on the network side of firewall, private on the Internet side
   C) On the network side of the firewall
   D) Public on the Internet, private on the Network side of firewall

17) The DMZ DNS server should contain records for: (p. 28, D)
   A) Internal DNS servers, desktop systems and file servers
   B) All e-mail, web, FTP, and news servers
   C) All routers, switches and firewall devices
   D) Only hosts that need to be publicly accessible

18) In order to resolve fully qualified domain names, internal DNS servers: (p. 29, C)
   A) Forward these queries to the InterNIC for resolution
   B) Forward these queries to a WINS server in the DMZ
   C) Forward these queries to a DNS server in the DMZ
   D) Forward these queries to the "Yahoo" servers for resolution

19) The DMZ DNS server can contain records of non-existent servers and Honey-pot bastion hosts in order to: (p. 29, C)
   A) Forward these queries to the correct servers
   B) Fill all DNS records
   C) Detect wherever these devices are probed using an automated protocol analyzer
   D) Allow for future network expansion by reserving the record space

20) WINS servers should have internet access through the firewall: (p. 29, A)
   A) Never
   B) To verify records on the DMZ DNS server
   C) To communicate with the InterNIC and resolve names
   D) To allow replication with external WINS servers

21) Remote Access Servers can be hidden by: (p. 32, B)
   A) Locking the modems in a closet with restricted access
   B) Using a telephone number outside of the standard range of public numbers assigned to you by Bell
   C) Running the modem lines through a "honey pot" server
   D) Disconnecting them from the network

22) Packet-filtering software that runs on an end-users computer in order to protect it is known as a: (p. 34, C)
   A) Hacker tracker
   B) Proxy server
   C) Personal firewall
   D) Single-homed Host

23) As part of an attack sequence, an attacker might run a DoS attack and crash a server in order to: (p. 37, C)
   A) Annoy the administrators with the colour blue
   B) Disable the helpdesk
   C) Allow an installed trojan horse program to run after the reboot
   D) Download the password database

24) A Denial of Service attack is meant to: (p. 39, A)
   A) Cause a system or some of the services on a system to stop working
   B) Re-configure a computer to secretly send information over the internet
   C) Deny a hacker access to services available to regular clients
   D) Install a DoS agent on a host system

25) A common DoS attack method consists of: (p. 40, B)
   A) Sending a Blue Screen of Death instruction to a system
   B) Sending modified/fragmented/too many packets to a system
   C) Sending a logon request using a known invalid user
   D) Sending source-routed packets to a system

26) You should suspect a DoS attack on an internet accessible server when: (p. 39, D)
   A) It repeatedly suffers BSoDs
   B) Services become usually and unexplainably slow
   C) CPU utilization suddenly and continuously runs at + 95%
   D) All of the above

27) An extremely large ICMP packet that is fragmented in transit and overflows the buffers when being reassembled on a target system is called: (p. 40, C)
   A) A SYN flood
   B) WIN Nuke
   C) Ping of death
   D) Telnet-crash

28) A SYN flood attack is the result of: (p. 40, D)
   A) Sending synthesized data packets to a host
   B) Telneting to a non-telnet port and entering unexpected data
   C) Sending an extremely large ICMP packet to a host
   D) Sending a stream of TCP handshake packets that each request a new TCP session to begin with a non-existent host

29) WIN Nuke can cause a crash or 100% CPU utilization by attaching to port 139 and: (p. 40, D)
   A) Flooding the server service with TCP session requests
   B) Transferring data from all open shares
   C) Repeatedly pinging the messenger service
   D) Sending out-of-band data

30) The most important defense against a DoS attack after deploying a firewall is: (p. 41, C)
   A) A high bandwidth internet connection
   B) Installing a "panic disconnect" script
   C) Installing the latest service pack
   D) Clearing the browser cache after each use

31) Service packs are available in domestic and export versions that support encryption levels of: (p. 41, D)
   A) 256 bit and 128 bit respectably
   B) 128 bit and 64 bit respectably
   C) 1024 bit and 512 bit respectably
   D) 128 bit and 40 bit respectably

32) Service packs must be re-applied whenever: (p. 42, C)
   A) A system crashes due to a DoS attack
   B) The service agreement on the server has expired
   C) The configuration of a server is changed
   D) Never

33) Disabling non-essential services and options can improve a server by: (p. 43, B)
   A) Requiring less network bandwidth
   B) Reducing one's potential exposure to attack and also boost performance
   C) Permitting more CPU cycles to handle the screen saver
   D) Freeing-up space for the swap file

34) An example of a subsystem that can generally be removed from a server is: (p. 45, D)
   A) Messenger
   B) WIN-32
   C) MS-DOS
   D) OS/2

35) Patches and hotfixes are continually being released to repair bugs and security issues. These items must be: (p. 47, C)
   A) Installed using the "update.exe" utility
   B) Installed into the "i386" directory on top of older files
   C) Installed in a certain order
   D) Installed on production servers prior to testing

36) Servers that run out of hard drive space for paging and temp files are at risk of crashing. You can keep track of the free space on up to 25 remote computers over the network using: (p. 52, D)
   A) Disk manager
   B) Server manager
   C) Security configuration editor
   D) Performance monitor

37) SYN floods are commonly used for Distributed Denial of Service attacks because: (p. 53, B)
   A) It is easier to program then many of the other attacks
   B) It normally can pass through a firewall
   C) It can bypass a network based IDS system
   D) It's small size allows for easy installation on "zombies"

38) Recovery from the damage caused by a DoS attack can be quick if you prepare by: (p. 55, A)
   A) Installing multiply copies of NT on your boot drive
   B) Quickly disconnecting from the network
   C) Have an NT boot diskette available
   D) Encrypt the WINNT\Repair folder

39) To use an emergency repair disk, it is necessary to: (p. 58, D)
   A) Put the ERD in the drive and boot from it
   B) Boot from a MS-DOS floppy diskette first and then the ERD
   C) Boot from the ERD and then the NT setup diskettes
   D) Boot from the NT setup disks and then use the ERD

40) In order to ensure that a current copy of the SAM database is copied to your ERD disk you need to run: (p. 59, D)
   A) Rdisk /sam
   B) Rdisk /s-
   C) Rdisk -s
   D) Rdisk /s

41) The most important tool for analyzing DoS packets is a protocol analyzer. Windows NT includes a rudimentary "packet sniffer" called: (p. 63, A)
   A) Network Monitor
   B) NetXray
   C) TCP Scanner
   D) SMS

42) A utility bundled with Windows NT that can log performance data on the internal processes and generate alerts or execute custom commands when configurable limits are exceeded is: (p. 65, B)
   A) Network Monitor
   B) Performance Monitor
   C) Net Watcher
   D) Syskey

43) If a DoS attack is causing a BSoD, it is possible to save the contents of RAM at the time of failure for later analysis. It is saved to: (p. 68, B)
   A) A file called memory.dmp
   B) The paging file on your OS partition then copied to memory.dmp at the next reboot
   C) A file called crashdump.log
   D) Your battery backed-up CMOS RAM

44) After obtaining a list of usernames from a system a hacker will often try to logon using: (p. 73, C)
   A) The users last names
   B) Brute force
   C) A password guessing program
   D) A null session

45) The NTLM user logon authentication session can be captured by a packet sniffer. The passwords can then be obtained because: (p. 74, D)
   A) They are in clear text
   B) They are pulled from the server by the packet sniffer
   C) They are easy to crack with PGP
   D) The password hash can be cracked by a dictionary or brute force method

46) The microsoft security configuration editor stores it's configuration settings in: (p. 76, A)
   A) Templates
   B) The Microsoft management console
   C) \%SYSTEMROOT%\SCE$
   D) The PDC SAM

47) A null session is an over-the-network logon where the username and password are: (p. 80, D)
   A) "null" and "null"
   B) "user" and "password"
   C) "guest" and no password
   D) The null character

48) Many network services run in the context of the local System account and can only connect to remote machines via: (p. 81, C)
   A) The guest account
   B) A domain administrator account
   C) A null user session
   D) A anonymous user account

49) If username listing via null sessions has been disabled it could: (p. 85, B)
   A) Cause failed logons for some users
   B) Cause some services to fail
   C) Cause intermittent authentication
   D) Risk exposing the SAM database

50) To protect an Administrator account a very strong password can include: (p. 87, A)
   A) Extended ASCII characters
   B) An encryption key
   C) Graphics
   D) Secondary data streams

51) An Administrator account that has had lockout enabled by Passprop and has been locked-out due to logon errors: (p. 88, C)
   A) Cannot be used for interactive console logon
   B) Can only be used for over-the-network logon
   C) Can only be used for interactive console logon
   D) Cannot logon at all until unlocked by another Administrator

52) The Guest account on Windows NT is by default: (p. 90, B)
   A) Enabled on Server and disabled on Workstation
   B) Disabled on Server and enabled on Workstation
   C) Enabled on both Server and Workstation
   D) Disabled on both Server and Workstation

53) Remote users will automatically be logged onto an enabled Guest account if: (p. 90, D)
   A) Their username is valid but they type in the wrong password
   B) They try to logon as a null user
   C) They do not have a valid username
   D) They do not have a valid username and the Guest account password is blank

54) Two accounts with the same usernames and passwords on different domains can be accessed by users in either domain if: (p. 96, A)
   A) Both are local accounts
   B) Both are global accounts
   C) The global account in one domain is trying to access the local account in another domain
   D) The local account in one domain is trying to access the global account in another domain

55) Services can run under the context of a: (p. 98, D)
   A) System account
   B) Regular user account
   C) Domain user account
   D) All of the above

56) Complex passwords that are much harder to guess and crack can be made mandatory on a server by: (p. 101, C)
   A) Writing a password policy and handing it out to your clients
   B) Selecting the "complex password" box in system policies
   C) Enabling the passfilt.dll on a SP3 or greater system
   D) Enabling the password.dll on a SP3 or greater system

57) In order to prevent a user from quickly cycling through a number of password changes to get back their favorite password, an administrator would set this policy: (p. 105, C)
   A) Maximum password age
   B) Lockout after bad logon attempts
   C) Minimum password age
   D) Lockout duration

58) SYSKEY.EXE can be used to strongly encrypt the SAM and require that a System Key be available in order for the computer to boot up. The System Key can be hidden on the computer itself, generated from a password up to 128 characters long or: (p. 110, B)
   A) Stored in CMOS
   B) Stored on a floppy disk
   C) Stored on a magnetic strip card
   D) Stored on a backup tape

59) Ntlmv2 authentication is not susceptible to replay attacks because: (p. 114, C)
   A) L0phtcrack is unable to extract the password hash
   B) It uses HMAC-MD5 for the 128-bit password hashes
   C) The server's challenge is different each time
   D) It uses a timestamp to verify that response is timely

60) Netlogon channels are used for: (p. 118, C)
   A) Account verification on a stand-alone NT system
   B) Copying the SAM file between 2 PDCs on the same domain
   C) Synchronization of the user accounts database and pass-through authentication
   D) Synchronization of the user accounts database and verification of domain administrator accounts

61) Reverse Social Engineering is when: (p. 124, C)
   A) A hacker contacts the help desk pretending to be a client
   B) A hacker pretends to be the vendor of a product the target owns and mails bogus "patches" containing break-in tools
   C) A hacker creates a situation where the target will contact him for help
   D) A hacker is tricked by the target into revealing his true intentions

62) The majority of computer security breeches are committed by: (p. 131, A)
   A) Full-time employees
   B) Part-time employees
   C) Contract employees
   D) Computer crackers

63) When NTFS and Share permissions are combined (p. 137, C)
   A) The effective permissions are the most powerful ones
   B) Equivalent rights cancel each other out
   C) The most restrictive permission is the effective one
   D) Fault-tolerance is disabled

64) The FAT file system is secure because: (p. 136, D)
   A) It allows you to boot to another operating system
   B) It allows for file system auditing
   C) The permissions apply over the network
   D) It is not secure

65) The default NTFS and Share permission is: (p. 140, A)
   A) Full Control for the Everyone Group
   B) Full Control for the Authenticated Users Group
   C) No Access for the Everyone Group
   D) No Access for Null Users

66) Using DACL and SACL tools it is possible for a rogue administrator to (p. 146, B)
   A) Delete files on a domain that he normally has no rights to
   B) Assign ownership to another user in order to shift blame for damage or loss
   C) Remotely hack an IIS website
   D) Create hidden administrator accounts

67) It is possible to see all the shares on multiple systems at once using the: (p. 147, C)
   A) Netviewer utility
   B) Sharewatch utility
   C) Netwatch utility
   D) Sharestat utility

68) By default Win NT shares the root of all volumes as a hidden share with full control. These are accessible to (p. 150, B)
A) Power users only
B) Administrators only
C) Domain users only
D) Service account only

69) The likelihood of a hacker using an account with RAS access to break into a network can be significantly reduced if: (p. 162, B)
A) The option to disconnect users with expired logon hours is enabled
B) The callback option is enabled
C) The telephone number is unlisted
D) The RRAS upgrade is installed

70) Network Monitor Agents are password protected with: (p. 165, C)
A) A very secure, high-encryption scheme
B) Non-encrypted, plain text passwords
C) An easy to defeat encryption scheme
D) They are not password protected at all

71) Using Server Message Block Signing for file and print sharing will thwart attacks that capture, modify and retransmit SMB packets. The cost of this extra security is: (p. 168, A)
A) Efficiency is reduced by at least 10% because every packet is checked
B) Because the SMB packet size is increased, efficiency is reduced by at least 10%
C) The encrypted data takes longer to travel through routers
D) More RAM must be installed to accommodate the process

72) One stealthy method a hacker might use to destroy evidence of his intrusion would be to: (p. 173, C)
A) Disable auditing
B) Destroy the audit logs
C) Flush the audit logs
D) Change the permissions on the audit logs

73) One of the most important things you can do to detect intruders is: (p. 175, B)
A) Check file access times
B) Enable auditing
C) Listen for telephones ringing in sequence during the night
D) Run performance monitor

74) The purpose of a "Honey Pot" is to: (p. 181, C)
A) Catch bugs in a program
B) Act as a firewall between an internet hacker and a server
C) Draw fire from the real servers and hold an attacker while alerts are sent out
D) House malicious code in hopes that a hacker will take it

75) Log files wrapping options should be set in most environments to: (p. 188, B)
A) Overwrite events as needed
B) Overwrite events older than X days (Configurable)
C) Do not overwrite events
D) Crash on the failure of auditing

76) An intrusion Detection System has 2 main parts: (p. 195, B)
A) An automated protocol analyzer and an email client
B) An automated protocol analyzer and an automated event log analyzer
C) An automated protocol analyzer and a firewall connection
D) An automated event log analyzer and a firewall connection

77) Once a hacker has broken into a system, they will probably install a method for secretly getting back in at a later time. A common way of doing this is to: (p. 197, C)
A) Create a new administrator account
B) Install Tripwire
C) Install a rootkit
D) Delete the event logs

78) It is possible for the registry settings in System Policy for Groups to conflict if a user is a member of numerous groups. How are these conflicts resolved? (p. 208, D)
A) The groups are prioritized using REGEDT32
B) The groups are prioritized alphabetically
C) The groups are filtered through Netlogon
D) An administrator can rank all groups according to their priority

79) System Policies for Windows 9x and Windows NT are stored in: (p. 210, C)
A) The netlogon share with a filename of config.pol
B) The logon share with filenames of config.9x and config.nt
C) The netlogon share with filenames of config.pol and ntconfig.pol
D) The logon share with a filename of settings.pol

80) Cached Logon Credentials are dangerous because they: (p. 221, C)
A) Allow another user to logon using someone else's credentials
B) Can be read by a null session over the network
C) Allow someone to logon to the local system when a domain controller is unreachable
D) Can be used to disable a users account

81) The risk of someone using a protocol analyzer to sniff data on a network is greatly reduced if: (p. 227, D)
   A) The network card is run in promiscuous mode
   B) The network is configured to work full-duplex
   C) The event viewer is configured to log sniffing
   D) The network is connected using a switching hub

82) An Enterprise management System is used to: (p. 228, A)
   A) Monitor the configuration of a workstation including hardware, drivers, software and security options.
   B) Monitor what users are logged on to their systems at any given time
   C) Perform full backups on all the systems in a domain
   D) Control the email logging for Exchange

83) The preferred method of virus scanning is: (p. 231, B)
   A) Scanning email at the gateway
   B) On access scanning on hosts and servers
   C) Scheduled scanning
   D) Scan at the firewall and proxy server

84) Printer drivers should have auditing enabled and installation restricted to administrators, print operators and power users because: (p. 233, D)
   A) They run in system context with full system access
   B) They run in administrator context with full system access
   C) If the files are corrupted, the system could crash
   D) They run in kernel mode and have full system access

85) In order to use the Schedule Service for their own purpose, a hacker with a user level account could possibly: (p. 234, B)
   A) Enter a job into the Schedule Service using AT.EXE
   B) Replace the program or batch file already scheduled with one of their own
   C) Change the time of a job to run when they are logged on
   D) Delete all scheduled jobs

86) To reduce the risk of a user leaving their system unlocked and logged on: (p. 223, D)
   A) Have company policy state that it must be off before they leave
   B) Install a program that requires the user to click OK every 10 minutes or it locks-out the system
   C) Configure the CMOS powersave features to blank the screen after 10 minutes of inactivity
   D) Install a password protected screen saver with a short time-out

87) After a username and password are submitted to Windows NT's authentication package MSV1_0.DLL, by default, MSV1_0.DLL then looks for: (p. 237, B)
   A) PASSFILT.DLL
   B) FPNWCLNT.DLL
   C) NTCONFIG.POL
   D) NETLOGON.DLL

88) The only way anything can be protected on a Win NT 4.0 server that has been physically compromised is if: (p. 243, D)
   A) The backup tapes are locked-up in a different room
   B) The floppy drive has been disabled in the password protected CMOS
   C) A password protected screen saver has been installed
   D) Third party encryption software is in use

89) Honey pot files can be used for prosecuting an attacker provided they are: (p. 269, C)
   A) Easy to access but unadvertised
   B) Well advertised but highly encrypted
   C) Well marked as confidential and unique in the world
   D) Available from a number of different protected locations

90) It is unwise to counter-attack a hacker because: (p. 273, D)
   A) It is illegal to take the law into your own hands
   B) The apparent source of the attack may not be the hacker's systems
   C) You might make him mad
   D) All of the above

End Questions: Securing Windows NT: Step-by-step

Start Questions: Internet Information Server for Windows 2000

91) Once a web server has been located through a search engine, determining the type of web server is often as easy as: (p. 12, C)
   A) Pinging the IP address and viewing the response
   B) Running a port scanner to detect the listening ports 20,21 and 80
   C) Telnet to port 80, issue a "GET / HTTP/1.0" and read the reply
   D) Run "netstat -a IPaddress" and view the reply

92) One of the important tools commonly used to analyze a web server through port scanning, entering information and viewing text responses is a free utility called: (p. 11, C)
A) Grinder
B) Netstat
C) Netcat
D) Webreaper

93) Hackers will use a URL Scanner in order to: (p. 14, B)
A) Download the entire contents of a web site to a local machine
B) Locate accessible web servers and attempt to download a specific URL
C) Scan the content of a URL for IP paths to other resources
D) Download the CGI code for a specific URL

94) Servers and the web-based applications running on them can sometimes be coaxed into revealing sensitive information by: (p. 15, D)
A) Determining the name of the application running
B) Examining the output of an application during normal use
C) Determining the encryption scheme used
D) Entering unexpected or altered input and viewing the error message generated

95) CGI Scripts and Active Server Pages represent a risk to the web server because: (p. 18, A)
A) The source code, if revealed, may contain delicate information like names, IP addresses, usernames, passwords and security holes
B) The source code is downloaded by the browser and could reveal delicate information like names, IP addresses, usernames, passwords, and security holes
C) They are significantly slower than .html
D) They are more vulnerable to DoS attacks

96) The most commonly used threat against IIS servers are: (p. 20, B)
A) Attempts to obtain an administrator accounts
B) Denial of Service attacks
C) Session Hijacking
D) DNS poisoning

97) Distributed Denial of Service in different from a regular DoS because: (p. 22, D)
A) It's attack is distributed to every service running on the server
B) It targets the server and all other devices on the same network
C) It uses the processing power of the server to attack itself
D) Installed agents on many systems attack the target at the same time

98) Hackers can run programs of their choosing on web servers under the correct circumstances. One common method is: (p. 27, A)
   A) Send commands directly to script engines placed in the wrong directory
   B) Send a URL to the server that points to a malicious program
   C) DoS attack the server and inject your own code while it recovers
   D) Hijack a session

99) Data transmitted over HTTP and FTP is: (p. 29, C)
   A) Strongly encrypted and difficult to intercept
   B) Lightly encrypted but difficult to intercept
   C) Essentially in clear text and easy to intercept
   D) Easy to intercept but difficult to decrypt

100) HTTP Session Hijacking is possible because: (p. 31, B)
   A) Passwords are easy to crack
   B) HTTP is a stateless protocol and Session ID#s are accessible
   C) VPN tunnels are easy to get into
   D) Web sites are susceptible to brute force password attacks

101) While IIS should ideally be behind a firewall, a free alternative that has quite flexible static packet filtering is: (p. 38, D)
   A) The native packet filtering capabilities of NT 4.0
   B) MS Proxy Server
   C) Performance Monitor
   D) Routing and Remote Access Service

102) In designing a firewall, it is important not to rely on a single firewall component for total protection. An internal network should be viewed as: (p. 41, C)
   A) A single homogeneous unit
   B) A Honey pot bastion host
   C) An onion with additional security layers protecting the most critical parts
   D) A choke point for all traffic

103) Packets coming from the internet or DMZ with source IP address in the range of those from the inside network are said to be: (p. 43, D)
   A) Source Routed
   B) Translated by a NAT
   C) Smurfed
   D) Spoofed

104) The advantage of not having the root folder of a Web or FTP site on the IIS server itself is: (p. 49, B)
A) The web application can read data quicker from another system
B) The IIS server becomes generic and if damaged can quickly be replaced or restored without risking data loss
C) The firewall is better able to filter any attacks
D) There is no advantage except the saving of storage space

105) An IIS web server should ideally be configured for security reasons as a: (p. 52, C)
A) Backup Domain Controller
B) Member Server
C) Stand-Alone Server
D) Primary Domain Controller

106) For IIS to run as a web-only server, which service could be disabled to reduce one's exposure to attack: (p. 55, A)
A) Server Service
B) Event Log Service
C) Protected Storage Service
D) Remote Procedure Call Service

107) Authentication on a web server is important because: (p. 68, B)
A) With many people accessing a web site concurrently, IIS needs to keep track of who is where in order to serve the proper pages
B) This is how IIS uses the security infrastructure of Win NT/2000
C) It is not. All connections are anonymous.
D) It prevents hackers from using web servers as an attack platform

108) HTTP users who have been Anonymously authenticated on IIS are generally notified by: (p. 72, B)
A) The "lock or key" icon being closed on the bottom of their browser
B) They are not notified
C) The "lock or key" icon being opened on the bottom of their browser
D) A pop-up dialogue box indicating a successful login

109) When using Basic authentication and SSL encryption a user's credentials will: (p. 76, C)
A) Always be protected during initial logon and thereafter
B) Be protected during initial logon and not sent thereafter
C) Be protected during initial logon but exposed when jumping from an SSL-encrypted page to a non-SSL encrypted page
D) Never be sent over the internet

110) A Digital Certificate is a document created by a Certifying Authority(CA) that: (p. 94, D)
   A) Allows you to decrypt a file encrypted with PGP
   B) Contains a digital fingerprint of your computer
   C) Is only present on E-Commerce servers
   D) Contains your public key, your credentials and is then encrypted with the CA's private key

111) If a Certificate Trust List is not installed on the IIS server to let it know which Certificate Authority (CA) to trust: (p. 102, B)
   A) It will not trust any CAs
   B) It will trust all CAs
   C) It will check the CAs database when verification is required
   D) The server will not function

112) The data transmitted over an HTTPS session is encrypted with: (p. 110, D)
   A) The server's private key
   B) The client's private key
   C) A session key randomly generated by the server
   D) A session key randomly generated by the client

113) With IIS Permissions, the Read permission on a folder: (p. 119, B)
   A) Permits someone to see the contents of a folder
   B) Permits someone to download a file from the folder
   C) Allows someone to run a script or executable
   D) Allows someone to view the source of a script

114) When someone has logged onto an IIS server anonymously, requests to files on NTFS volumes the permissions are checked against: (p. 123, D)
   A) Those of the Everyone Group
   B) Those of the Null User
   C) Those of the Guest account
   D) Those of the IUSR_*COMPUTERNAME* account

115) WebDAV allows authors to edit, create and manage files in folders on remote web servers. It also allows: (p. 135, A)
   A) authors to lock a file while it is being edited
   B) authors to FTP files back and fourth
   C) administrators to run diagnostic checks on the web server
   D) administration of internet printing

116) To obtain the best performance for web applications, they should be run: (p. 144, D)
A) in an isolated process
B) in a pooled process
C) in a Web Application Manager
D) in process

117) You should unmap any unused ISAPI Extensions because: (p. 148, B)
A) it will increase the performance of an IIS server
B) these extensions are vulnerable to DoS and buffer overflow attacks
C) these extensions are vulnerable to URL spoofing
D) you should not unmap any, as the ISAPI Filters will be disabled as well

118) IIS has its own version of a configurations database somewhat like the registry, called the: (p. 156, A)
A) metaBase
B) IISReg
C) InetBase
D) SuperReg

119) If Microsoft Index Server has been installed on the IIS server, it will not index any keywords found in: (p. 177, B)
A) the noindex.dat file
B) the noise.dat file
C) the private.dat file
D) the IServer.dat file

120) If each FTP user is required to log in with their individual domain username and password, for security the server should use: (p. 180, C)
A) NTLM authentication
B) Certificate authentication
C) Virtual Private Networking
D) Basic authentication

End Questions: Internet Information Server for Windows 2000

Start Questions: Active Directory for Windows 2000 in a Nutshell

121) Active directory services are installed on a Windows 2000 server when: (p. 12, B)
A) It is initially setup
B) It is upgraded from a non-domain controller to a domain controller
C) A new tree is added to the forest
D) Netbios has been removed

122) It is imperative that you decrypt your email and encrypting file system files, and export your current encryption keys: (p. 13, D)
   A) After running DCPROMO.EXE
   B) When the Schema is about to be changed
   C) Before you switch from Native mode to Mixed mode
   D) Before running DCPROMO.EXE

123) For performance and recovery reasons, the Active Directory Database and Log should be located: (p.14, C)
   A) In the same directory
   B) In different directories on the same system
   C) In different hard drives
   D) On different computers

124) If you set the option "Permissions Compatible with Pre-Windows 2000 Servers" while running DCPROMO, you are effectively enabling: (p.15, D)
   A) Communications with Windows NT 4.0 Servers
   B) 8.3 filenames
   C) Ability to perform NTLM authentication
   D) The Everyone group, who by default have read access to account names in AD

125) A Windows 2000 domain controller can run in "Native" mode when: (p. 16, A)
   A) All clients are either Windows 2000, have been upgraded to support AD and Kerberos, and all domain controllers are Windows 2000
   B) There is a combination of Windows NT domain controllers and servers, Windows 9x and NT WS clients, and Windows 2000 domain controllers
   C) The domain controller has had the Active Directory service disabled
   D) Only during the upgrade process.

126) A Windows 2000 Server running in "Native" mode supports what type of logon authentication? (p.17, A)
   A) Kerberos only
   B) Kerberos and NTLM
   C) NTLM only
   D) Basic only

127) A Windows 2000 Server running in "Native" mode can use by default: (p. 18, D)
   A) SMB with NetBios
   B) SMB without NetBios
   C) No SMB
   D) SMB with NetBios and SMB without NetBios in parallel

128) A windows 2000 DC must be physically secured against tampering because: (p. 22, B)
A) If it is brought down a portion of the clients will be unable to authenticate
B) If the AD database were modified in any detrimental way, it will replicate to all other domain controllers in the domain
C) If it is the primary domain controller, all authentication would be delayed
D) If it is the backup domain controller, the NETLOGON share would no longer be available

129) The Microsoft Management Console Snap-in "SIDWalker" is for: (p. 24, A)
A) Migrating NT 4.0 resources into a Windows 2000 domain
B) Transferring account information from one Windows 2000 server to another
C) Editing, deleting and adding SIDs
D) Modifying the AD database directly

130) You cannot install the Schema Manager Snap-in until: (p. 27, B)
A) ADSI Edit Snap-in has been installed
B) The Schema Manager's DLL has been registered with the OS
C) Local Computer Policy Snap-in has been installed
D) LDAP has been bound to a directory server.

131) The main protocol used to edit and query Active Directory is: (p. 28, D)
A) TCP/IP
B) SMB
C) NetBios
D) LDAP

132) Windows 2000, including Active Directory, can be managed entirely through scripts. Microsoft provides default script engines for: (p. 30, B)
A) JScript and ActivePerl
B) JScript and VBScript
C) VBScript and ActivePerl
D) Kixtart and VBScript

133) Which items are automatically replicated among domain controllers: (p. 31, B)
A) NTDS.DIT and the NETLOGON directory
B) NTDS.DIT and the SYSVOL share
C) SYSVOL share and NETLOGON directory
D) NTDS.DIT and EDB.CHK

134) In order to be replicated, changes to Active Directory are received by: (p. 31, C)
A) A Windows 2000 PDC
B) A ADSI Server
C) A Windows 2000 DC
D) A Windows 2000 BDC

135) Intersite Replication between 2 domains is: (p. 32, A)
A) Conveyed with RPC-over-IP or SMTP and Manually configured
B) Automatic, and configured by the Knowledge Consistency Checker
C) Manually configured, and controlled by the Knowledge Consistency Checker
D) Conveyed with RPC-over-IP or SMTP and Automatically configured

136) In order to use a SMTP transport for replication you must have: (p. 33, C)
A) A fast, reliable link
B) PGP services to encrypt the SMTP data
C) Certificate Services on a domain controller and IIS-SMTP on the transport DC
D) Exchange Server running at both nodes

137) The properties of transport links can be configured to: (p. 33, D)
A) Test the available links and use the one with the most direct route
B) Use 2 links at once for redundancy
C) Schedule SMTP transport for off-peak hours
D) Choose the most cost-effective transport between multiple links

138) The File Replication Service automatically replicates: (p. 34, A)
A) The SYSVOL share and those created with the Distributed File System
B) The SYSVOL share and NTDS.DIT
C) The NETLOGON directory and shares created with the Distributed File System
D) Distributed File System shares and NTDS.DIT

139) A Global Catalog Server contains: (p. 35, B)
A) A catalog of all objects from all the domains in an enterprise
B) The most commonly accessed data from the AD of all domains in the enterprise
C) An index of the AD from all the domains in an enterprise
D) A listing of all users from all the domains in an enterprise

140) A Flexible Single Master Operation (FSMO) Server is used: (p. 37, A)
A) With services and data that are not suitable for multi-master replication
B) As a bridge between Windows NT 4.0 Servers and Windows 2000 Servers
C) As the root of a large Forest
D) As a bridge between Windows-based and non-Windows-based networks

141) To avoid missing bad references between domains, a Infrastructure Master Server should not also be a: (p. 38, B)
A) PDC Emulator Master
B) Global Catalog Server
C) Schema Master
D) Domain Naming Master

142) The Domain Naming Context contents are only fully replicated with: (p. 49, D)
A) Root Domain Controllers
B) Global Catalogue Servers
C) Domain Controllers in the same Forest
D) Domain Controllers in the same Domain

143) The trust model between a Windows 2000 Domain and all of it's sub-domains is: (p. 49, B)
A) Two-way
B) Two-way Transitive
C) One-way Transitive
D) Circular

144) A Forest is two or more trusting domains where: (p. 51, A)
A) One is not a DNS sub-domain of the other
B) They have a common DNS root domain
C) They do not share a common Schema, Configuration and Global Catalog
D) One is a DNS sub-domain of the other

145) Organizational Units are subdivisions of a: (p. 52, B)
A) Group
B) Domain
C) Site
D) Tree

146) Universal Groups can contain: (p. 56, C)
A) Global groups and Local groups
B) Individual users and Local groups
C) Individual users and Global groups
D) Global Groups and Domains

147) Universal Groups are unique in that : (p. 57, D)
A) Universal Distribution Groups cannot be created in mixed mode
B) Universal Distribution Groups cannot be created in native mode
C) Universal Security Groups cannot be created in native mode
D) Universal Security Groups cannot be created in mixed mode

148) To reduce the volume of replication traffic between domains, Universal Groups should only contain: (p. 58, A)
A) Global groups, not individual users
B) Individual users, not Global groups
C) Local Groups, not Global Groups
D) Distribution Groups

149) When an object or container doesn't inherit permissions from the parent container it is called: (p. 65, B)
   A) A Rebel
   B) An Orphan
   C) A Child
   D) Stand-Alone

150) Active Directory permissions of any user can be tested using the SU.EXE and RUNAS.EXE utilities. These allow an administrator to: (p. 75, C)
   A) Run a simulated logon and check access rights
   B) Compare a user's rights against a pre-defined template
   C) Launch a program under the security context of the user
   D) Check what rights a user exercised during their last session