Global Information Assurance Certification Paper

This is my submission for my practical assignment for the SANS Parliament Hill 2000 Windows NT Track. I have chosen Option 3 - Create a test that demonstrates your knowledge of the subject area.

The exam is multiple choice and consist of 150 questions, 30 from Day 1, 30 from Day 2 and 30 from Day 3, Securing NT Step by Step and 30 from IIS and 30 from Active Directory. For each question there is a listing of the book, file, and page number the question is based on and the correct answer. The correct answer is highlighted in blue. For the all questions choose the best answer, unless otherwise stated.1. Because not all hackers follow the typical phases of attack in order, or all steps why should we be aware of the typical phases of attack?

A) A hacker may not be as skilled and therefore miss steps, in which would give you a better way to trace them.
B) By organizing your defences around the typical phases of attack, you can secure your network in logical and comprehensive way.
C) A hacker who does not do proper reconnaissance will fail, and not provide a validated attack.
D) Hackers are aware of theses phases of attack and have changed their way of exploiting your network.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 12

2. In regards to the typical phases of attack, what is Reconnaissance?

A.) Reconnaissance is the physical act of exploring where your network is located.
B.) Reconnaissance is exploiting known security holes within your network.

C.) Reconnaissance is the gathering of information that is potentially useful for further intrusion or attack.
D.) None of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 14

3. How would deploying a network firewall help against the Reconnaissance phase of attack?

A) It defends your network by blocking over-the-internet reconnaissance such as port scanning.
B) It completely "Stealth's" your network from the Internet.
C) It only allows authorized access from specific IP's from the Internet.
D) It allows all information to in and out of your network, but logs all activity.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 25

4. Why should public information be limited about your network? (Choose all that apply)

A.) None. General information does not compromise your network.
B.) Public information can be used to obtain IP addresses of your private network.
C.) Public information can be used to use the NSLOOKUP command, to obtain hostname to IP records of your network.
D.) Private search engines, company directories, and USENET news groups can provide information that can be used for Social Engineering.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Pages – 28-31

5. How can you hide RAS Servers in your network? (Choose Two)

A.) Have the RAS servers located in an off site location.
B.) Do not publish the RAS server phone number in any publication.
C.) Have the RAS server phone number within your company's block of phone numbers.
D.) Require that your RAS server phone number be outside your company's block of phone numbers.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Pages – 32-33

6. Which of the following best describes a personal Firewall?

A.) A network firewall with specific rules for your user account.
B.) A term for software that allows a user to bypass the network firewall security settings.
C.) Packet-filtering software that runs on only one PC and is intended to protect only that computer in which it is installed.
D.) Packet-filtering software that runs on only one PC and is intended to protect all computers in the network.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 35

7. What types of effects would you see with a Denial of Service (DoS) attack?

A) Locked out accounts.
B) Heavy bandwidth usage
C) 100% CPU Utilization.
D) Services fail or slow.
E) All of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde

Part 1 - Day 1, Monday, 21 August 2000
Page 39

8. How can you prepare and protect your network from Denial of Service attacks?
(Choose Two)

A.) Allow the Everyone group Read access to all resources
B.) Install the latest Microsoft Service Pack and Hot fixes.
C.) Allow all ports to be open on your network firewall.
D.) Disable all non-essential Services and options.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Pages - 41-47

9. Why should you preserve free space for temporary and paging files, in regards to Denial of Service attacks?

A.) It allows Windows NT Event Log Service to adapt to a DoS Attack.
B.) If the temporary and paging files run out of free space, Windows NT may crash.
C.) A DoS attack is more likely to effect CPU utilization then the temp and paging files.
D.) Not required, because DoS attacks only affect physical RAM.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page - 50

10. What of the following is recommended to prevent a Blue screen (BSOD) caused by the lack of free space? (Choose Two)

A.) Dedicate 1 partition for the OS files.
B.) Use programmed I/O (PIO) controllers instead of Bus-Mastering hard drive controllers.
C.) Place a paging file on the OS partition at the size of half of the installed physical RAM.

D.) Configure the maximum audit log sizes to be as large as necessary, and ensure there is enough free space for these logs to grow to their maximum.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 51

11. If you have multiple installations of NT, current ERD Disks, and perhaps "ready to go disk drives", what can these tools help accomplish in regards to a Denial of Service attack?

A.) When you become a victim of a DoS attack it will help you recover in a quick and efficient manner.
B.) It can help you track where the DoS attack originated from.
C.) It can help you compare the system files and status before attack.
D.) They can help rollback your production servers from a bad service pack / hot fix install.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Pages 56-62

12. To prevent a successful Denial of Service attack from being used over and over on your network, you need to analyse the attack in order to prevent it. What would you use to gather this information?

A.) NETSTAT
B.) REGEDIT
C.) NBTSTAT
D.) Protocol Analyser

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 63

13. Why would some hackers bypass the Denial of Service phase of attack? (Choose all that apply)

A) It sends red flags to the network administrator, that something is out of the normal and to take further action.
B) Attackers want to cause financial damage.
C) Attackers are attempting to gain administrative privileges without alerting the network administrators.
D) Attacker is not competent enough to perform a DoS attack.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 37

14. In general, a user account is needed by a hacker to perform:

A.) DoS attacks
B.) SYN Flood attacks
C.) Stealing, altering, and/or destroying data.
D.) Providing need reconnaissance information.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 71

15. A Domain controller will register NetBios names that include the name of the controller. What utility included with Windows NT will allow you to view / perform this action?

A) NETSTAT
B) PING
C) TRACERT
D) NBTSTAT

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 72

16. During a Windows NT install there are two default users created, what are these two accounts, which are strongly recommended to be renamed?

A) Guest & Administrator
B) Null session & System
C) Administrator & Guest
D) Administrator & System

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 73

17. What is a very powerful tool that hackers can use, and cannot be defended against by any service packs or system settings and can only be defended against by education?

A) LOpht crack
B) Social Engineering
C) Null Sessions
D) Legion

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 75

18. Since Service Pack 4, a new tool was made available to network administrators called Microsoft Security Configuration Editor. What is it?

A.) A tool to trace hacker attempts.
B.) A Microsoft supplied protocol analyser.
C.) An interactive tool to audit logons in real time.
D.) Tools to define, compare, and match security configuration templates against a local machine.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 76

19. When a user attempts to access data or services on a remote Windows NT computer, and the users request is rejected, some applications will still attempt to establish a connection with a _____?

A) Null Session
B) SMB Connection
C) Anonymous Session
D) FTP Logon

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 80

20. In Windows NT 4.0, why are Null Sessions allowed? (Choose all that apply)

A) To allow network protocol analysers full access to the network.
B) It is built in to the OS
C.) Used for administrative purposes when one's user account lacks sufficient rights.
D.) The local system account can only connect to remote machines with null user sessions.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 81

21. Null Sessions can be used to list usernames on remote domains. This is an unacceptable security risk for your network. You are asked to disable all null sessions for your network. What should be discussed with your managers before this is done?

A) Nothing. Null Sessions are not required.
B) That some system and applications require null sessions in order to function properly and may disrupt the operation of the network.
C) That they have been misinformed, null sessions cannot be used to get a username list.
D) None of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3

Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 86

22. Why should the Administrator account be renamed? (Choose all that apply)

A) It is a known account with a great deal of power.
B) It cannot be locked out by bad attempts.
C) There is a flaw in Windows NT that that account is misspelled.
D) To keep password cracking utilities from being functional on any account with administrative rights.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 87

23. Because an account with administrator privileges is so powerful, which of the following would be a good password scheme for these accounts?

A) Minimum 4 letters and never change password.
B) Minimum 4 letters and password expires every 12 months
C) A minimum 8 characters with extended ASCII characters and expires every 2 months.
D) Minimum of 8 letters only and expires every 4 months.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 87

24. Since service pack 3 from Microsoft, there is a utility named PASSPROP.EXE. What is its purpose in regards to the Administrator account?

A) It allows anybody to log on with administrative rights.
B) It allows for the Administrator account to have a blank password.
C) It allows more auditing options for the administrator account.

D) It allows the administrator account to be locked out from over the network logon attempts.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 88

25. The Administrator account has been copied and has been given no significant user rights, permissions, or group memberships and has a mediocre password. What would this situation be referred to as?

A) RAS account
B) Null session account
C) Honey Pot account
D) Security nightmare account.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 89

26. Why should the guest account be disabled and not have a blank password?

A) Remote users can logon as a guest even if the username and password supplied do not exist.
B) Remote users can be logged on with administrative privileges if this situation exists.
C) Not required, there are no security gaps with the guest account.
D) None of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 90

27. Windows NT allows multiple users to be logged on with the same account (Shared Accounts). What would be a reason that this activity should not be allowed?

A) Shared Accounts are not subject to auditing.
B) A shared account makes auditing less useful.
C) A shared account makes auditing more useful.
D) Shared accounts allow many people to access resources, lessening the administrative resources of managing their accounts.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 92

28. The NBTSTAT utility that comes with Windows NT can be used to:

A) Show the state of shares on a remote machine.
B) Provide current status of IP addresses.
C) Provide a list of NetBios names a remote system is using on a network.
D) Download a remote WINS database.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 19

29. A hacker commonly uses what to find your networks RAS Servers?

A) NBTSTAT
B) IPCONFIG
C) TRACERT
D) WarDialing

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 23

30. Why is the “SYN Flood” Distributed Denial of Service (DDoS), potentially so dangerous?

A) It is normally allowed to pass through firewalls.
B) There is currently no defence for this attack.
C) A SYN Flood attack disrupts the Kernel code directly.
D) Network packet sniffers cannot pick up packets from a DDoS.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 1 - Day 1, Monday, 21 August 2000
Page 53

1. Why should you have a solid user and group creation policy in regards to avoiding identically named accounts?

A.) Global accounts can potentially be used to log onto any computer in the domain or trusting domain.
B.) If a global & local account have the same username / password pair, a remote share or service may be connected with a transparent logon.
C.) Local accounts with the same username / password pair in different domains with no trusts, can give the illusion that trusts are not needed, because network logons can be made without any errors.
D.) All of the above

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 96

2. All processes under NT must run under the content of an account. Services run under the content of the service account. What is the way to prevent the executables of these services to be replaced by malicious programs?

A.) Assign NTFS permissions to the exe's under the services such that only Administrators and the relevant service accounts can access the executables.
B.) Do not use the built-in service accounts.
C.) Prefer a domain user account over a local user account during the set-up of a service.
E.) Assign NTFS permissions to service accounts at the same level as administrative accounts.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 99

3. PASSFILT.dll is an optional filter, which can require a user to have complex passwords. Why is this a good requirement for a medium security network?

A.) It provides a user with the option of having the administrators know their password.
B.) It will require passwords to have a combination of any 3 uppercase, lowercase, numbers, or special characters.
C.) It provides less protection from directory based cracking programs.
D.) It provides more protection by sending and storing passwords to a remote location on your network in clear text.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 102

4. In a medium security network, what of the following would be recommended for a default account & password polices? (Choose all that apply)

A.) Lockout duration – 4 hours
B.) Maximum Password age – 120 to 180 days.
C.) Reset counter – After 15 mins.
D.) Password Uniqueness – Remember 9-12 passwords.
E.) Account lockout – Never

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde

Part 2 - Day 2, Tuesday, 22 August 2000
Page 104-105

5. You are looking to secure your Domain Controllers, ERD Disks and Tape Backups so that the SAM can be strongly encrypted. What utility from Microsoft can you use?

A.) PASSFILT.DLL
B.) LOPHT.CRK
C.) SYSKDL.EXE
D.) SYSKEY.EXE

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 109

6. To prevent password sniffing on your network, you upgrade all your servers to SP6 and set the registry to only except NTLMv2 Authentication. Your network client machines are running Windows 98 and 2000 Professional. Do you have to configure anything on the clients?

A.) No. Windows 98 and 2000 Professional support NTLMv2.
B.) Yes. All clients must be running Windows 2000 Professional.
C.) Yes. Windows 98 needs Directory Services Installed.
D.) No. The Domain Controllers must be upgraded to Windows 2000 Server.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 112

7. The Net logon channel is the service, which handles pass-through authentication and account synchronization. Prior to Service Pack 4, the net logon channel is open to what kind of attack?

A.) Man-in-the-middle.
B.) DoS
C.) LOpht crack.
D.) Trojan PASSFILT.DLL

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 119

8. A well-versed Hacker will often use Social Engineering to acquire information. What is Social Engineering?

A.) The use of a hacker's personal Information to get a user account.
B.) The art of applying for a job within a company to acquire a network administrative position.
C.) The art of tricking users into revealing information that will assist a hacker in overcoming a networks security measures.
D.) None of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 122

9. In phase 4, Access network resources, of the typical phases of attack, what could you as a security administrator commonly expect a hacker to do? (Choose 2).

A.) Perform DoS attacks.
B.) Exploit miss-configured shares and permissions.
C.) Perform Man-in-the-Middle attacks by attacking SMB Sessions.
D.) By not using a RAS connection

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 132

10. Proper implementation of policies for groups, rights permissions, and storing critical data on NTFS volumes, are examples of?

A.) Not nessacery, the Windows NT defaults are a good security measure.
B.) Needed measures because Windows NT defaults are not good security measures.
C.) Perform Man-in-the-Middle attacks by attacking SMB Sessions.
D.) By not using a RAS connection

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3

Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Pages 133-134

11. It is recommended to change the default NTFS and Share Permissions and Default NTFS Group Permissions to?

A.) Full control for everyone and Full control for everyone.
B.) Change for everyone and Full control for authenticated users.
C.) Read for everyone and read for authenticated users.
D.) No access for everyone and no access for everyone.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Pages 140-143

12. How can a hacker view a list of folders and printer share names?

A.) By establishing a null user session, then using the using the NetVIEW.cmd.
B.) By establishing a null user session, then using the using the NBTSTAT.cmd.
C.) By establishing a null user session, then using the using the TCPRO.cmd.
D.) By establishing a null user session, then using the using the NetSTAT.cmd

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 149

13. What would be the reason that you as an Administrator might want to disable the Administrative Shares to (C$, D$, etc.) on a NT Workstation?

A.) To disable the ability to accept null sessions.
B.) To protect the local SAM database.
C.) To protect the workstation from administrators themselves.
D.) To disable the ability to connect to RAS Servers.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 150

14. What Key in the Windows NT Registry controls access to the Registry?

A.) Current Control Key.
B.) System Key.
C.) HKLM Key.
D.) WinReg Key.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 153

15. In Windows NT 4.0, what is a Named Pipe?

A.) A system share required for proper operation.
B.) A programming object which allows a process on one system to communicate with another process on different system.
C.) A system null session used for application updates.
D.) A programming object which allows an unsupported object non-NTFS volume to be mounted and read.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 157

16. Why are RAS Servers and accounts with dial-in permissions so attractive to hackers?

A.) When a hacker uses a RAS connection, his action cannot be logged.
B.) RAS connections are run at an Administrative service level.
C.) Dialling in through a RAS server is an excellent way to circumvent Firewall protection.
D.) A hacker can be logged on and run packet sniffers without being detected.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3

Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 160

17. Why should network monitor agents be severely restricted or not even installed?

A.) Network monitor agents password scheme is easy to defeat, therefore hackers can use your own agents.
B.) Network monitor agent actively polls for connection from any user.
C.) Network monitor agents provide very little information.
D.) Network monitor agents are used to bypass network firewall security.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 165

18. If your network can handle a 10% reduction in efficiency for SMB Sessions, what can you implement in order to prevent SMB hijacking or replay attacks?

A.) Disable SMB Sessions.
B.) SMB null sessions.
C.) SMB NTLMv2 encryption.
D.) SMB Message signing.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 166

19. Internet Information Server is Microsoft's HTTP and FTP Servers. What should you have to remember when installing ITS? (Choose all that apply)

A.) If an install of IIS is miss configured it can give hackers complete control over the NT system.
B.) Do not install any features that will not be used.
C.) Unbind WINS Client (TCP/IP) from the network adapter card attached to the Internet.

D.) Delete all sample files and scripts that come with IIS.

Reference: Securing Windows NT: Step-by-Step
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 169

20. In the 5th phase, of the typical phases of attack, avoiding detection, how might an attacker avoid detection?

A.) Disable, modifies, flush or destroy Audit logs.
B.) Use a regular user account and impersonate them.
C.) Install a trapdoor or a Windows NT Root kit.
D.) All of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 172-174

21. To detect intruders on your network, what is the most important step to take?

A.) Disable Logging.
B.) Enable Syslog Logging.
C.) Enable Logging.
D.) Disable Syslog Logging.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 175

22. When applying an audit Policy on your network, on a Domain Controller, which statement is true?

A.) An audit policy on a Domain Controller has to be applied to all Domain Controllers.
B.) An audit policy on a Domain Controller applies to all Domain Controllers.

C.) An audit policy on a Domain Controller applies to all Workstations.
D.) None of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 177

23. Which of the following events can be audited? (Choose all that apply)

A.) Rebooting or shutdown of the server.
B.) Any custom event a programmer or administrator may wish to include.
C.) Use of user rights.
D.) Access to the Registry Keys.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 175

24. After File and Object Access auditing has been enabled in user manager, those objects must be individually configured with the auditing options desired. What does Microsoft provide for manually configuring SACL's on Objects?

A.) Windows Explorer.
B.) Regedit32.exe.
C.) Printer folder icon.
D.) All of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 179

25. The Windows NT Resource Kit includes a utility named LOGEVENT.exe. What is LOGEVENT.exe?

A.) A command line utility to write custom events to audit logs of local or remote systems.
B.) An event log utility to manage event log events.
C.) An event log command utility to purge event logs on remote systems.
D.) None of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 180

26. When referring to "Honey Pot Tactics" deployed on your network, what does this mean?

A.) Securing your network so that it does not look like an easy target network for hackers.
B.) A server or resource designed to ensnare intruders, log their actions and Alert the administrator.
C.) A server or resource designed to provide hackers with an alternative route to your network.
D.) Honey Pot tactics refers to the administrative mode for remote administration that cannot be used by hackers.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 181

27. If you are going to implement Honey Pot Tactics on your network, which of the following are considered to be Honey Pot Tactics? (Choose all that apply)

A.) Marked files.
B.) Honey Pot RAS Servers.
C.) Honey Pot Firewalls.
D.) Poison Honey Pot.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000

Page 183

28. You can use SYSKEY.exe to strongly encrypt the SAM database. The system key can be hidden on the computer itself, and what are the other two options?

A.) The system key can be stored and used on a floppy.
B.) The system key can be generated from a password.
C.) The system key can be used and stored in a user account.
D.) The system key can be stored and used from a bootable CD.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 110

29. Which of the following is a reason that the NT hash used in NTLMv1 is stronger than the LM Hash?

A.) Upper case and Lower case sensitivity are not retained.
B.) The NT Hash adds "salt" to the NT Hash.
C.) Upper case and Lower case sensitivity are retained.
D.) Pre-computed directory attacks cannot be used.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 114

30. What are the most likely targets for hackers to exploit using social engineering? (Choose Two)

A.) The server managers of your companies' structure.
B.) The Company that supplies your service hardware.
C.) Non-technical users who have contact with the public.
D.) Administrators.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde

Part 2 - Day 2, Tuesday, 22 August 2000
Page 127

31. Statistically, a 1996 FBI report on computer crime estimated that approximately 75% of security breaches are done by?

A.) Hackers.
B.) Security Companies.
C.) Government agents.
D.) Legitimate internal users.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 2 - Day 2, Tuesday, 22 August 2000
Page 131

1. The three event logs visible in the Event Viewer are stored as individual files in the \%System Root%\System32\ config folder. You should assign NTFS permissions to these files for which users?

A.) System accounts and local administrator group full control.
B.) Local Administrators and Groups and Everyone Group full control.
C.) Authenticated users and system accounts full control.
D.) System accounts and local administrator group read only.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 185

2. In user manager, there is a right that gives a user the power to configure SACL's, to view and to clear the security logs. What is this right?

A.) Change account policy.
B.) Change registry access.
C.) Manage auditing and security log.
D.) Manage Security configuration templates.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000

Page 186

3. Proper Configuration of Log size and wrapping options are critical to keep information from being flushed or changed by hackers, where do you configure this?

A.) User Manager.
B.) Server Manager.
C.) Security Configuration editor.
D.) Event Viewer.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 188

4. You can add a value to the registry to cause the system to shutdown when the audit log fills to its maximum size. What is a possible drawback to setting this option?

A.) Could possibly be used in DoS attacks.
B.) Could possibly be used as a point of entry for a hacker.
C.) Could possibly be used to bypass auditing of hackers attempts.
D.) Could not be used for any of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 191

5. You can use the event viewer (save as…) to save event viewer data. What is recommended when doing this?

A.) Save all log files from all machines to one central location.
B.) Schedule to save and clean the audit log on a regular bases.
C.) Set the log to overwrite files as needed.
D.) Answers A and B.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde

Part 3 - Day 3, Wednesday, 23 August 2000
Page 192

6. Thousands of events can be logged to Event Viewer, resulting in a vast amount of information that may not get immediately looked at. Some events should be known as they happen. What tool can you use to accomplish this?

A.) Use an automated Event Log Analyser.
B.) Use the host based application monitor
C.) Use a dedicated security Administrator to view logs
D.) Use scripts to dump the Event Viewer logs to a central location.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 195

7. When tampering is suspected on your network servers, you need to locate modified files, what can you use to find modified files?

A.) Event Viewer
B.) WinDiff.
C.) Protocol Analyser.
D.) NetCat.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 198

8. An intruder has been detected by your network security measures, what should you have already in place to avoid harm, time loss and general chaos?

A.) A poisoned Honey Pot.
B.) A network IP Tracing Package.
C.) A contact from your ISP.
D.) An incident Response Plan.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde

Part 3 - Day 3, Wednesday, 23 August 2000
Page 200

9. In phase 6 of the typical phases of attack, exploiting physical access to workstations, what can you generally expect? (Choose all that apply)

A.) Packet Sniffing.
B.) Personal Modems.
C.) Accessing RAS Servers.
D.) Station Hopping.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 203-205

10. You can use System policy in Windows NT 4.0 and Group policy in Windows 2000 to effectively?

A.) Make registry changes to many computers and these changes follow users as well.
B.) Make driver upgrades to many computers.
C.) Make local hardware changes in network workstations identifiable and send to a central database.
D.) Make OS upgrades to all Microsoft operating systems.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 206

11. How does Windows NT 4.0 handle conflicts with system policies for groups?

A.) If a user is a member of multiple groups, Administrators can rank groups by setting higher priority groups to override lower group settings.
B.) If a user is a member of multiple groups, the group policies are applied by Alphabetical order.
C.) If a user is a member of multiple groups, the group policy is defaulted to the user's settings.
D.) If a user is a member of multiple groups, users can Rank groups by setting higher priority groups to override lower group settings.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 208

12. System policy settings are automatically attempted to be downloaded from the Domain Controller that authenticates the logon. What files are stored in the Net Logon folder for Windows NT clients and Windows 9x clients?

A.) NTCONFIG.SYS and CONFIG.SYS.
B.) WINNT.ADM and WINDOWS.ADM.
C.) WINNT.POL and WINDOWS.POL.
D.) NTCONFIG and CONFIG.POL.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 210

13. There are other ways to change Registry setting such as security configuration editor. What should users be made aware of regarding Hyperlinks to Registry files?

A.) That it will improve the performance of their workstation.
B.) That importing Registry files are dangerous.
C.) That Hyperlinks cannot import Registry files.
F.) None of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 216

14. Windows NT Resource Kit includes a utility named Autolog.exe, which permits a user to be automatically logged on during boot up. Windows 9x machines can use a utility called Tweak UI to do the same. Why should these utilities be disallowed? (Choose 2)

A.) They circumvent the bulk of user level security.

B.) They have little impact on the networks security.
C.) They store the password and user names in plain text.
D.) They are not effective with Service Pack 6 installed.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 216

15. You should be aware of programs that elevate a user account to Administrator level, such as Get Admin and SecHole. A good security administrator should?

A.) Stay abreast of new developments of exports.
B.) Apply the latest Service Packs and Hot Fixes.
C.) Set permissions an powerful Registry Keys.
D.) All of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 219

16. Windows NT caches the credentials by default, of the last 10 users. A user can still logon when no Domain Controller is available. Why should this be disabled?

A.) If a user is a member of multiple groups, Administrators can rank groups by setting higher priority groups to override lower group settings.
B.) If a user is a member of multiple groups, the group policies are applied by Alphabetical order.
C.) If a user is a member of multiple groups, the group policy is defaulted to the user's settings.
D.) If a user is a member of multiple groups, users can Rank groups by setting higher priority groups to override lower group settings.

Reference: Securing Windows NT: Step-by-Step
Fossen – Kolde
Document Version: 3.6
Part 3 - Day 3, Wednesday, 22 August 2000
Page 208

17. Users commonly don't log off when they leave their desks for a short period of time. What could you tell the users about to use to make their workstations more secure when they do step out? (Choose 2)

A.) Turn off the monitor.
B.) Lock Workstation.
C.) Screen savers with passwords.
D.) Remove the keyboard and mouse.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Pages 222-223

18. What should you educate users about password security?

A.) To let other co-workers know their password.
B.) To write their password down.
C.) To recycle their favourite password.
D.) That hackers know to look under keyboards, around the room, and know common passwords for your employment.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 224

19. Protocol Analyzers capture raw packets from the network stream, which sometimes contain passwords in clear context. How can you find packet sniffer in use?

A.) LOpht Antisniff.
B.) Switch Hubs.
C.) NBTSTAT.
D.) Packet Sniffers themselves.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 227

20. Printer drivers run in Kernel mode, meaning that Trojan Horse printer drivers have unlimited access to the operating system. How can you prevent this?

A.) Restrict printer driver installations to Administrators.
B.) Printer drivers do not operate at the Kernel mode.
C.) Apply NTFS permissions on existing printer driver files.
D.) Answer A and B.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 233

21. AT.EXE is a utility used to submit jobs to scheduled servers. What context does the AT utility run in?

A.) Kernel mode.
B.) Systems account.
C.) Administrator account.
D.) Everyone account.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 234

22. NT automatically creates 8.3 names for long file folder names for backwards compatibility with older MS-DOS and Win16 applications. What bug is known about this?

A.) Two files with the same eight characters and extensions can possibly give access to a user that does not have proper rights.
B.) Two files with the same eight characters and extensions can possibly over right other.
C.) Two files with the same eight characters and extensions can possibly be lost by the operating system
D.) Two files with the same eight characters and extensions can possibly be used in a DOS attack.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6

Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 240

23. What can you expect to see during Phase 7, of the typical phases of attack, access to Targeted Servers? (Choose all that apply)

A.) Stolen tape backups.
B.) Destruction or sabotage of tape backups and ERD's.
C.) Administrators who are seeking revenge.
D.) Rebooted servers to use floppy to gain full access to the servers file system.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 244

24. Server hardware should be secure from all human threats. Which of the following fulfill this statement?

A.) Have a server in a common room.
B.) Have a server in a locked room.
C.) Provide temperature and humidity control.
D.) Do not enforce access policies.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 246

25. A way to circumvent Windows NT security and NTFS permissions is to boot the computer into another operating system from a floppy. Which of the following can prevent unauthorized rebooting and floppy access?

A.) Use a password in the BIOS and set the boot sequence to boot from the hard drive first.
B.) Do not use a password in the BIOS that requires a password on boot up.
C.) Disable the floppy in the BIOS.
D.) Set the boot sequence to boot from the floppy first.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 250

26. You as a network Administrator can audit users rights in regards to Backing up files and directories and Restoring files and directories, this can result in thousands of entries being generated in the event viewer. What is a valid alterative to this method?

A.) Audit the server operators group.
B.) Audit the systems accounts.
C.) Audit the executables of the backup applications themselves.
D.) Audit the schedule service.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 252

27. As an administrator of a network you have vast knowledge about the ability to quickly cripple an organization. What would be a good practice for handling Malicious or disgruntled Administrators?

A.) Discuss termination of administrators.
B.) Perform background checks.
C.) Treat administrators fairly.
D.) All of the above.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page - 254

28. Which of the following statements is true for local accounts?

A.) All Windows computers support local accounts.
B.) Local accounts on a domain controller can be used to log on to any Domain controller.
C.) Domain controllers only have global account databases

D.) Local accounts are the same on all domain controllers and workstations within a domain.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 256

29. As an administrator you can delegate administrative authority in Windows NT 4.0 safety by? (Choose all that apply)

A.) Properly managing Rights and Groups.
B.) Use of third-party management software.
C.) Placing resources and accounts into a trusting domain.
D.) Upgrading to Windows 2000.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 257-259

30. You should always have a strict inventory, offsite storage, and secured storage for backup media. Why?

A.) Insures data integrity.
B.) Insures data will not become corrupt.
C.) Insures data protection and helps prevent data theft.
D.) Insures less workload on administrators.

Reference: Securing Windows NT: Step-by-Step, Parts 1,2 & 3
Document Version: 3.6
Fossen - Kolde
Part 3 - Day 3, Wednesday, 23 August 2000
Page 249

1. The Active Directory database includes?

A.) User account properties and passwords

B.) DFS shared folders
C.) Trust relationships
D.) Anything else desired, since the database is extensible
E.) All of the above.

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 9

2. All Windows 2000 domain controllers must be secured to protect the Active Directory database (NTDS. Dit). The NTFS permissions on the NTDS folder should be set to?

A.) Administrators to no access
B.) System to change
C.) Everyone Read
D.) Everyone Full Control

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 23

3. ADSI is a generic interface for a Vendors directory services including? (Choose all that apply)

A.) Windows 2000 Active Directory
B.) Microsoft Exchange Server
C.) IBM Lotus Notes
D.) Netscape Commerce Server

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 29

4. In Windows 2000, there are five FSMO Master Roles. From the following choose the correct answer or answers that apply.

A.) PCC Emulator Master
B.) Infrastructure Master
C.) Schema Master
D.) Domain Naming Master
E.) RDD Master

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 37

5. In Windows 2000, _____ defines classes of objects in Active Directory and their attributes. Which answer best fills the blank?

A.) Regsvr32
B.) FSMO
C.) KCC
D.) Schema

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 40

6. In Windows 2000, which three of the following are major sections in the Active Directory Database?

A.) Configuration Naming Context
B.) FQDN Naming Context
C.) Domain Naming Context
D.) Schema Naming Context

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 43

7. Like Windows NT 4.0 domains, Windows 2000 domains cannot have?

A.) Nested Domains
B.) Names following the DNS Standard
C.) Two-way Transitive trusts
D.) None of the above.

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 48

8. In Windows 2000 most Networks will consist of one Domain. Windows NT Domains will generally be replaced with?

A.) Tree
B.) OU
C.) Forest
D.) Schema

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 52

9. User Groups have become more flexible in Windows 2000. One group, Universal Group, is an enterprise-wide group. What can a Universal Group contain?

A.) User and global groups
B.) Global groups and local groups
C.) Local groups and Users
D.) Users and Distribution groups

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 56

10. There are a few more properties for User accounts in Windows 2000 that are relevant to security. Choose all that are relevant tabs that are on the properties sheet for a user account, from the choices below.

A.) Store passwords using reversible encryption.
B.) Smart card is not required for Interactive Logon.
C.) Account is trusted for Delegation.
D.) Account is Sensitive and cannot be delegated.

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Pages – 60-64

11. The potential complexity of Active Directory permissions in Windows 2000 can be overwhelming. The preferred method to reduce this complexity is to?

A.) Use Inheritance as much as possible.
B.) Use orphans
C.) Use generic permissions instead of specific
D.) None of the above.

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 72

12. In Windows 2000 the ability to delegate power will likely far exceed the needs of most organizations. Choose all examples from below of how can powers be delegated?

A.) A user could have full control over all users in an OU, but no others.
B.) A user could create user accounts in a Domain, but not be able to delete, edit, or read their properties afterwards.
C.) A user could be given the power to change a single property of all user accounts, but change nothing else.
D.) A group could have full control over all shared folders on all computers in a site.

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 77

13. Choose the answer or answers that give guidelines for delegating control in Windows 2000:

A.) Use specific permissions instead of generic
B.) Delegate to individuals rather that groups
C.) Audit delegates
D.) Grant the least power, which will still enable delegates to work.

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 77

14. Group policy is one of the most important security features of Windows 2000, which of the following answers is an example of Group policy?

A.) Change NTFS permissions and auditing
B.) Change registry key permissions and auditing
C.) Change registry values
D.) Manage user rights
E.) All of the above

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 81

15. Group policies in Windows 2000 cannot be linked to what of the following? (Choose all that apply)

A.) Sites
B.) Trees
C.) Domains
D.) OU

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 84

16. Group Policy Objects in Windows 2000 and System Policy in Windows NT 4.0 are applied in a specific order. Which of the following GPO's is applied last, therefore having the highest priority?

A.) NT 4.0 System Policy
B.) Local GPO's
C.) Site GPO's
D.) Domain GPO's
E.) OU GPO's (in nested order)

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 89

17. A user in Windows 2000 must have at least what permissions in order to have a Group Policy Object applied to their desktop?

A.) Deny Read and Deny Apply Group Policy permissions
B.) Read and Apply Group Policy permissions
C.) Change and Read Group Policy permissions
D.) Full Control and Change Group Policy permissions

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 95

18. In Windows 2000, a user requires at least what permissions in order to create or edit a Group Policy Object?

A.) Read and Write permissions on that GPO
B.) Full Control permissions on that GPO
C.) Read and Add permissions on that GPO
D.) Deny apply Group Policy Permissions

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 96

19. In Windows 2000, Group Policy can be used to install, update, repair, and remove applications. GPO application management applications must support a special installation script with what filename extension?

A.) .GPO
B.) .MIS
C.) .ISM
D.) .MSI

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 98

20. Windows 2000 Group Policy Objects assigned scripts can be run when the computer Starts up / Shuts Down and when the user Logs on / Logs off. Which of the following statements is true?

A.) Logon/Logoff scripts run as the system, while Start-up/Shutdown scripts run as the user.
B.) Logon/Logoff scripts run as the user, while Start-up/Shutdown scripts run as the system.
C.) All scripts run as the system
D.) All scripts run as the User

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 101

21. In Windows 2000, the Windows Settings \ Security Settings container in a Group Policy Object can contain and control?

A.) IPsec Policies
B.) Registry Contents
C.) System Services
D.) Account Policies
E.) All of the above

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0

Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 103

22. Windows 2000 Group Policy Objects Administrative Templates replace what from Windows NT 4.0?

A.) Poledit
B.) Group Policy
C.) System Policy
D.) User Policy

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 108

23. Windows 2000 Group Policy Object command line utilities can be used to manage and troubleshoot Group Policy. Where can you find these utilities and a reference for understanding Group Policy options?

A.) Windows 2000 installation CD
B.) Windows 2000 AD
C.) Windows 2000 Resource Kit
D.) All of the above

Reference: Active Directory for Windows 2000 in a Nutshell
Document Version 1.0
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 111

24. Windows 2000 DNS provides a number of new features over Windows NT 4.0 DNS, such as Active Directory integration, SRV Records and Dynamic updates. Which of the following statements is true regarding DNS for Windows 2000 domain controllers?

A.) Windows 2000 Domain Controllers and Clients require DNS.
B.) Windows 2000 Domain Controllers and Clients do not require DNS.
C.) Windows 2000 Domain Controllers and Clients require WINS.
D.) Windows 2000 Domain Controllers and Clients require NetBios.

Reference: Active Directory for Windows 2000 in a Nutshell
Windows 2000 Dynamic DNS Insert
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 1 (Self Numbered)

25. Windows 2000 DNS Zone data can be stored in?

A.) Active Directory or in system RAM.
B.) Text files or in System RAM.
C.) Active Directory Only.
D.) Text Files or in Active Directory.

Reference: Active Directory for Windows 2000 in a Nutshell
Windows 2000 Dynamic DNS Insert
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 4 (Self Numbered)

26. When Windows 2000 DNS Zone records are stored in Active Directory, it supports Multi-Master Replication, Incremental Zone Transfers, fault tolerance, and better security. That means that in Windows 2000 there is no longer primary and secondary DNS servers, how does this change affect Non-AD enabled clients?

A.) A D – integrated DNS Servers can not be used.
B.) A D – integrated DNS Servers can only be secondary DNS Servers.
C.) A D – integrated DNS Servers can only be primary DNS Servers.
D.) AD – integrated DNS Servers can only be both primary and secondary Servers.

Reference: Active Directory for Windows 2000 in a Nutshell
Windows 2000 Dynamic DNS Insert
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 6 (Self Numbered)

28. Windows 2000 DNS Servers support SRV records, which are required for Windows 2000 compatibility. The purpose of SRV records is to identify?

A.) Services available on a host.
B.)FQDN of host.
C.) Port number.

D.) All the above.

Reference: Active Directory for Windows 2000 in a Nutshell
Windows 2000 Dynamic DNS Insert
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 7 (Self Numbered)

28. Windows 2000 DNS Server supports secure dynamic updates, which of these Statements are true?

A.) Secure updates are possible with any client and DNS and DNS Servers.
B.) Secure updates are possible only with AD- integrated DNS Servers.
C.) Secure updates are not possible with AD – integrated DNS Servers.
D.) Secure updates are possible only with BIND 8.2.1 systems.

Reference: Active Directory for Windows 2000 in a Nutshell
Windows 2000 Dynamic DNS Insert
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 10 (Self Numbered)

29. In Windows 2000, the DNS snap-in includes a Zone Transfers tab. If you are using AD-integrated DNS Zones and no non-AD secondary, what is recommended?

A.) Allow zone transfers.
B.) Allow zone transfers only to servers listed.
C.) Disable zone transfers entirely.
D.) Allow zone transfers only to servers on the Name Servers tab.

Reference: Active Directory for Windows 2000 in a Nutshell
Windows 2000 Dynamic DNS Insert
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 16 (Self Numbered)

30. What is DNS cache poisoning?

A.) Attacks in which incorrect or bogus query response are sent to a DNS Server.

B.) A DoS attack on an IIS server found in your DNS Records.
C.) When virus-scanning software corrupts DNS records.
D.) None of the above.

Reference: Active Directory for Windows 2000 in a Nutshell
Windows 2000 Dynamic DNS Insert
Fossen
Part 4, Day 4 Thursday, August 24 2000.
Page – 18 (Self Numbered)

1. Internet Information Server is a favourite target for Hackers. As a Security Administrator, what is a common saying regarding security?

A.) It is impossible to secure a product without knowing how to attack it
B.) There are very few security holes IIS
C.) What you don't know won't hurt you
D.) IIS is not a target of Hackers

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 8

2. An attacker can easily determine that a web server is running Internet Information Server, as opposed to Lotus Domino or Apache, by?

A.) Telnet into port 110, enter GET / HTTP/1.0
B.) Telnet into port 80, enter GET / SERV INFO
C.) Telnet into port 80, enter GET / HTTP/1.0
D.) Telnet into port 110, enter GET / SERV INFO

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 12

3. Web-based applications and the server itself sometimes reveal sensitive information when error messages are produced. Which of following answers do hackers use to accomplish this task? (Choose two answers)

A.) Enter large amounts of data into search forms.
B.) Refresh the main web page over and over.
C.) Try to download the entire web site for offline browsing.
D.) Replace data in a web sites cookie with large amounts of data, and then return to the site.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 16

4. Denial of Service (DoS) attacks are the most common threat to Internet Information Server. Which of the following may result from a DoS attack?

A.) Blue Screen of Death (BSOD)
B.) Crash of the Inetinfo.exe process
C.) Slow the IIS server
D.) All of the above.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 20

5. A security administrator may prevent execution of malicious commands and programs on an Internet Information Server By? (Choose all that apply)

A.) Not having the write and execute permissions on the same folder.
B.) Not having the script engines and scripts in the same folder.
C.) Having the script engines and scripts in the same folder.
D.) Having the write and execute permissions on the same folder.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 27

6. On Internet Information Server, HTTP and FTP transmit data essentially in clear text allowing Hackers to intercept usernames, passwords, etc. Which of the following may aid a Hacker to do this?

A.) Installing a connection interception program on port 80.
B.) Packet Sniffers
C.) Netcat
E.) All of the above

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Pages – 29-30

7. In order to defend your Internet Information Server, Which of the following is not recommended for the security administrator?

A.) Subscribe to Security Email bulletins
B.) Lurking in hacking chat / news groups.
C.) Browse websites relating to security.
D.) Post detailed information about your site on the web.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 35

8. The purpose of a Network Firewall is?

A.) To allow more open access for everyone
B.) To allow more ease of use for everyone
C.) To decrease the complexity of security measures
D.) To protect your LAN from the internet

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 40

9. It is permissible and often beneficial to combine Firewall components and Security components in which of the following ways?

A.) Have a single Firewall connecting a LAN to the Internet.
B.) Not to combine the Internet attached router and a bastion host into one computer.
C.) Have multiple bastions hosts in the DMZ, or place some bastions in the

DMZ and others inside the LAN.
D.) Use multiple interior LAN attached routers connected to the same DMZ.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 44

10. Some HTTP based applications require multiple servers to work in concert. Which of the following is acceptable in Firewalling a distributed server arrangement?

A.) Use standard packet filtering.
B.) Use a reverse proxy Server or NAT router in the DMZ.
C.) Use a reverse proxy Server or NAT router, but also add another relay system to the chain that performs filtering and validation.
D.) All of the above.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 50

11. In regards to Internet Information Server security, why should a service or feature that is not in use, be disabled or uninstalled?

A.) To speed up web page access.
B.) It reduces the potential number of security holes.
C.) It allows Hackers more exploits options.
D.) Increases the potential number of security holes.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 54

12. Choose the following authentication method that is not built into Internet Information Server.

A.) Anonymous
B.) Basic

C.) QBasic
D.) NTLM

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 67

13. Whenever a file is accessed on a windows 2000 / NT machine, it must be under the context of a user account. What context are your web site users represented under?

A.) IUSER_*computername*
B.) IUSER_anonymous
C.) Null Session
D.) IUSER_system

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 71

14. Choose two of the following answers that indicates the advantages of basic authentication. (Choose Two)

A.) Virtually every browser supports Basic.
B.) Basic cannot pass thru proxy servers or Firewalls.
C.) Basic uses a complex method of encoding passwords.
D.) Basic will always open a dialog box prompting for username and password.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 75

15. Digest authentication is intended to replace the weak Basic authentication method. Choose the best answer / answers that show that advantages of Digest over Basic.

A.) Most browsers do not support it.

B.) Encryption is drastically better.
C.) Works with proxies and Firewalls.
D.) Digest requires the reversible encryption option.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 78

16. In Internet Information Server 5.0, the Integrated Windows method uses Kerberos in parallel with NTLM. What is an advantage of this set up?

A.) All versions of Internet Explorer are compatible.
B.) Kerberos is stronger than Digest.
C.) Can be used with proxies.
D.) NTLM is stronger than Digest.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 81

17. Multiple authentication methods can be enabled simultaneously in Internet Information Server. Place the following five items in order of preferred use.

1. Basic 2. Certificate 3. Digest 4. Anonymous 5. Integrated Windows

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

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 89

18. What is a Digital Certificate?

A.) A file with one's credentials and public key.
B.) Encrypted documents with the private key of one's certifying authority.
C.) A document that has your public and private key.
D.) All of the above.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 19

19. When configuring Certificate authentications on Internet Information Server, how can you control access via client certificates?

A.) One-to-Many
B.) DS Mapping
C.) Any trusted Certificate accepted.
D.) All of the above.

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 104

20. Internet Information Server 5.0 supports SSL. What is SSL?

A.) Secondary Storage Location
B.) Secure Sockets Layer
C.) Secure Storage Layer
E.) Secondary Socket Layer

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 110

21. When configuring Internet Information Server access permissions it is best to follow the principle of least privilege. What two answers satisfy this statement?

A.) Have read and execute on folders
B.) Allow Directory Browsing
C.) Don not enable Script source access except when necessary
D.) Reset script permissions to none

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 121

22. Internet Information Server can block access based on the client's source IP address. IP blocking rules can be applied to?

A.) Files
B.) Folders
C.) Website
D.) All of the above

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 125

23. When you have a properly installed version of Windows NT 4.0 Server, then you install Internet Information Server, IIS is able to take advantage of?

A.) NTFS
B.) HPSF
C.) CDFS
D.) UXFS

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 123

24. Internet Information Server comes with Web Distributed Access and Development (WebDav). What does WebDav allow you to do?

A.) To securely manage files with HTTP
B.) To securely manage files with SMB
C.) To securely manage files with FTP
D.) To securely manage files with Front Page

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 135

25. In Internet Information Server, what is recommended to secure the Metabase?

A.) Not to rename or to move the Metabase
B.) Set NTFS permissions on the Metabase to authenticated users to change
C.) Secure the Registry key which determines the Metabase location
D.) Leave all ROOT folders on the %systemroot% volume

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 158

26. A single Internet Information Server can host multiple websites. You can delegate users to have power over just a specific website. With these permissions, a Website Operator cannot?

A.) Enable Logging
B.) Configure the anonymous user account or password
C.) Set content ratings
E.) Change IIS permissions

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 164

27. VNC is a free alternative to pcAnywhere. If you choose to inplement VNC on

your network, what is recommended to secure VNC? (Choose all that apply)

A.) Change the port number VNC server listens on
B.) Do not filter the IP addresses from which clients can connect.
C.) Use IPsec with VNC on Windows 2000
D.) Frequently check for updates and new add-ons

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 169

28. When configuring Event Viewer auditing with NTFS, which of the following is not recommended?

A.) Audit access by the everyone group, not just Domain Users
B.) Audit all access to the scripts and Bin folders
C.) Protect the Event Viewer Logs themselves by giving Everyone Change permissions
D.) Use a host based Intrusion Detection System

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 173

29. In Internet Information Server when you are configuring HTTP and FTP logging, which of the following should you not follow?

A.) Using the W3C Extended format
B.) Not using a network based Intrusion Detection System
C.) Log all access to the scripts and Bin folders
D.) Log Date, IP, username, method, bytes received, URI stem and Query

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 173

30. Microsoft Index Server is used with Internet Information Server to provide content indexing and keyword searches of Volumes on Local and remote systems. When securing Index Server, what should you not consider for security?

A.) Make the Index Server search pages accessible to Internet users.
B.) Uninstall (NT) or stop the Indexing service (Windows 2000) if not in use
C.) Only Index files on NTFS volumes
D.) Add sensitive words to the NOISE.DAT that should not be searched for

Reference: Internet Information Server for Windows 2000, Parts 1 & 2
Document Version: 2.0
Fossen
IIS – Tuesday and Wednesday Nights, 22-23 August 2000
Page – 177