Global Information Assurance Certification Paper

NT Practical Parliament Hill SANS
Submitted by Dave Weir Sept. 18, 2000

Contact Information: Dave Weir
Suite 606, Atlantic Place
215 Water Street
St. John's, NF, Canada
A1C 6C9

90 Questions from Securing Windows NT

What is the stealthy gathering of information which may be potentially useful for further attack called?
a) Social Engineering
b) Port Scanning
c) Reconnaissance
d) Lurking

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 14

What is the single best defense against Internet reconnaissance?
a) Deploy a firewall
b) Screen the information available to the public
c) Educate users about Social Engineering
d) Install the latest service packs

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 25

What should you use to detect and respond to scanning and other suspicious activities in real time?
a) Process Explode Utility from the NT Resource Kit
b) An automated Protocol Analyzer
c) Event Viewer
d) Performance Monitor

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 27

If the firewall should block all external access to both internal DNS and WINS servers what should be used to allow internal clients to resolve any FQDN?
a) A secondary WINS server placed in the DMZ
b) DNS forwarding
c) A secondary DNS server that resides on the DMZ
d) An Internal DNS server by means of iterative queries

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 29

Which two things should you educate employees about to insure they do not inadvertently provide useful information to the public?
a) Social Engineering and Lack of Privacy on the Internet
b) Lack of Privacy on the Internet and Private Search engines

c) Company Directories and Lack of Privacy on the Internet
d) Lack of Privacy on the Internet and Hacker statistics

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 31

What step can you take to help protect your RAS server from being detected by a hacker using a wardialer?
a) Publish its phone number in Company publications
b) Use a phone number that is not part of the range assigned to the company by the phone company.
c) Use a phone number in the middle of the range of numbers assigned to the company
d) Use an unlisted number

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 33

Besides causing financial harm by preventing access to essential services what other purpose may a DOS attack serve?
a) To hide the audit trail of previous attacks
b) To prevent users from detecting their presence
c) To force a reboot for changes to take effect by causing a BSOD
d) To secretly acquire an administrative account

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 37

After you have developed a feel for what is "normal" for a server at any given time what can be taken as an indication of a DOS attack?
a) Any significant deviation from the norm
b) Things are unusually quiet
c) The server is performing much better than usual
d) Failed hardware

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 37

After deploying a firewall what is the most important defense against DOS attacks?
a) Deploy an Automated Protocol Analyzer
b) Educate users about Social Engineering
c) Screen the information available to the public
d) Install the latest service packs

Answer: D
Securing Windows NT: Step by Step Part 1,2 and 3 Page 41

Since it is impossible to predict what new DOS attacks will be discovered in the future the prudent step to reduce exposure is to:
a) Disable any non-essential services and options
b) Consult a psychic on a regular basis
c) Deploy an Automated Protocol Analyzer
d) Educate users about social engineering

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 43

Why must you place data, such as logs, which can grow uncontrollably into its own partition?
a) So as it can be secured with the appropriate permissions

b) To hide it from attackers
c) Because if you run out of temp or paging space the server may crash
d) It is easier maintain if it has its own area

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 50

What effect does setting HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\SysAttackProtect to the value 2 have?
a) No Syn Flood Protection
b) Eliminate the damage caused by Syn Floods
c) Mitigate the damage caused by Syn Floods
d) Returns the system to it's default setting

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 54

Since DOS attacks are a fact of Internet life what 2 things must you be prepared to do?
a) Recover quickly and analyze the attack
b) Unplug from the Internet and find alternate means of communication
c) Block all access to the Internet and wait for the attacker to go away
d) Recover quickly and report the attack to the authorities

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 55

What can be done to allow for quick recovery from DOS attacks that damage OS files or the Registry?
a) Install NT twice on the same server
b) Keep your latest backup in the tape drive
c) Store Backups off site
d) Buy a fast tape drive

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 56

Since it can be time-consuming to restore a server from tape it is recommended that in addition to the tape backup a recent _____ be maintained.
a) Boot Disk
b) Emergency Repair Disk
c) Redundant Server
d) Inventory of spares

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 57

What is the most important tool for analyzing DOS attacks?
a) A log viewer utility
b) A parser
c) A Protocol Analyzer
d) A laptop

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 63

In addition to a sniffer _____ is useful in analyzing DOS attack strategy.
a) A Protocol Analyzer

b) Examining the logs
c) A laptop
d) A firewall

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 67

_____ can be used as a stepping stone to further penetrate the network.
a) A user account
b) A port scanner
c) A phone number
d) A group name

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 71

What can be used to target a domain controller in order to download usernames with descriptions, users last logon date and time, local and global group names, a list of running services and device drivers and more?
a) A Null Session
b) The Guest Account
c) NBTSTAT
d) A Port Scanner

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 72-73

Which two reasons make the Administrator account the most often targeted for password guessing?
a) It cannot be renamed and does not get locked out for bad logon attempts.
b) It cannot be deleted and does not get locked out for bad logon attempts.
c) It is the most powerful account and does not get locked out for bad logon attempts.
d) It is the most powerful and cannot be renamed.

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 73

What tool would you use to perform the following tasks: defining security configuration templates, comparing the local machines settings against the template, and configuring the local machine to match the template.
a) Policy Editor
b) Security Configuration Editor
c) Zero Administration Kit
d) Perl Scripts

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 76

An over the network logon where the username and password are both the null character is referred to as a:
a) Null Session
b) System Session
c) Guest Logon
d) Pass Through Authentication

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 80

Why do null sessions exist?

a) To allow the system account access to files and services on the local server
b) For administrative purposes where one's user account is unavailable or has insufficient rights.
c) To allow replication to work.
d) To allow guests to logon

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 81

What registry setting must be set to block username listing?
a) HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous value set to 0
b) HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous value set to 1
c) HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\RestrictAnonymous value set to 0
d) HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\RestrictAnonymous value set to 1

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 86

What consequences arise from blocking username listing?
a) The last logged on user is no longer displayed
b) Someone logging on in a trusting/domain will be unable to list users an groups from the trusted/accounts domain
c) Net show command will no longer display a list of usernames
d) In user manager you will no longer be able to choose other domains.

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 86

What is an excellent way to get very strong passwords?
a) Use passfilt.dll
b) Include special keys in your password such as !
c) Include extended ASCII characters in your password
d) Set it to the maximum size of 15 characters

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 87

Which 2 things should be done to protect the Administrator account?
a) Rename it and audit it
b) Rename it and enable account lockout
c) Enable account lock out and audit the account
d) Delete it and use a different account that is a member of DomainAdmins

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 89

What two things should be done to secure the guest account?
a) Delete it and create a temporary account for guests
b) Set a password and disable the account.
c) Rename the account and set a password.
d) Remove it from the everyone group and disable it.

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 90

What is special about the Guest account which makes it different from all other accounts?
a) It is a member of the new authenticated users group

b) It is used by IIS if you allow anonymous access to FTP
c) If enabled and with password left blank anyone trying to logon with an unknown username will automatically be logged on as guest.
d) It is a member of Domain Users

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 90

Why should "Role Based" accounts not be used?
a) They make auditing less useful
b) They require more administrative overhead
c) They can not be added to local groups
d) They are members of the Everyone group

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 92

Why should you avoid identically named accounts?
a) They will have the same SID
b) It is easy to logon with the wrong account
c) Because they have the same name the generated password hash will be the same
d) Because NT will generate an error if you attempt to do this

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 96

What is a service account?
a) An account whose context services run under
b) It is the system account on a server
c) It is the owner/creator context on a server
d) It is an account that is created by default for temporary contractors

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 98

What is the order of preference for service accounts?
a) System, Local, Global
b) Local, Global, System
c) Global, Local, System
d) Local, System, Global

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 98

What two things should be done to the executables of services?
a) Secure them to restrict access to only administrators and the relevant service accounts and audit failed access attempts
b) Secure them to restrict access to only the relevant service accounts and audit failed access attempts
c) Secure them to restrict access to only the relevant service accounts and audit successful access attempts
d) Secure them to restrict access to only Domain Admins and audit failed access attempts

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 100

Which registry key is used to enable password filtering?

a) HKLM\System\CurrentControlSet\Control\LSA\NotificationPackages value set to Passfilt
b) HKLM\Software\Microsoft\WindowsNT\CurrentVersion\NotificationPackages value set to Passfilt
c) HKLM\System\CurrentControlSet\Control\LSA\NotificationPackages value set to Passfilter
d) HKLM\Software\Microsoft\WindowsNT\CurrentVersion\NotificationPackages value set to Passfilter

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 101

Which six options are available to enforce sound account and password Policies?
a) Maximum password length, account reset time, maximum password age, maximum password age, account disable, and disable duration
b) Account lockout duration, account lockout, password history list, maximum password length, minimum password age, account reset time
c) Maximum password age, minimum password length, minimum password age, password history list, account lockout, and lockout duration
d) Maximum password age, minimum password length, minimum password age, force alphanumeric password, account lockout, and lockout duration

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 104

What are the three ways of making the syskey available?
a) key on disk, key hidden on server, generated from a password that must be typed at startup
b) generated from a password that must be typed at startup, key store in SAM of domain controller, key on disk
c) key on disk, key hidden on server, key stored in SAM of domain controller
d) key stored in BIOS, key stored on disk, key hidden on server

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 110

What can you do to protect against password sniffing?
a) disable LANMAN compatibility
b) use NTLM Authentication
c) use NTLMv2 Authentication
d) use Microsoft CHAP Authentication

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 112

What systems support NTLMv2 authentication?
a) Windows NT Service Pack 4 or later, Windows 9x with the Directory Services Client from Windows 2000 CD, Windows 2000
b) Windows NT Service Pack 5 or later, Windows 9x with the directory services client from Windows 2000 CD, Windows 2000
c) Windows NT service pack 4 or later and Windows 2000
d) Windows NT service pack 5 or later and Windows 2000

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 112-113

_____ is the Service that handles pass-through authentication and account synchronization.
a) Netlogon Channel
b) Replicator
c) Local Security Authority
d) Local Security Agent

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 118

Which registry key is used to secure Netlogon Channel?
a) HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
b) HKLM\System\CurrentControlSet\Control\LSA\Winlogon
c) HKLM\System\CurrentControlSet\Control\LSA\Netlogon
d) HKLM\System\CurrentControlSet\services\netlogon\parameters

Answer: D
Securing Windows NT: Step by Step Part 1,2 and 3 Page 120

The devious art of tricking users into revealing information that will assist one in overcoming a networks security measures is known as?
a) Social Engineering
b) Naivity
c) Lurking
d) Reconnaissance

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 122

Who are the primary threat to network security?
a) Script Kiddies
b) Foreign Espionage Agents
c) Your own users
d) Industrial spies

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 131

Which file system should be used to store critical data because its permissions apply over the network and at the console, allows auditing, and is transactional and fault tolerant?
a) FAT
b) FAT32
c) NTFS
d) CDFS

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 136

The _____ permission is the effective one when you combine NTFS and share permissions.
a) Least restrictive
b) Cumulative
c) Most Restrictive
d) Inherited

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 137

You should use _____ instead of Full Control when assigning rights.
a) Write
b) Execute
c) Change
d) Read

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 140

Apply the principle of _____ when assigning share and NTFS permissions.
a) Most privilege
b) Least privilege
c) Economics
d) SNIGTH

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 140

As a rule of thumb only _____, _____, and _____ should have the full control permission.
a) Administrators, the System account, and Creator Owners
b) Administrators, Account Operators, and the System account
c) Administrators, Backup Operators, and Server Operators
d) Administrators, Backup Operators, an Account Operators

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 141

Instead of the everyone group you should use the _____ group for NTFS and share permissions.
a) Domain Guests
b) Authenticated Users
c) Power Users
d) Local Users

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 142

Which registry value prevents null users from listing share names?
a) Restrict Null
b) Restrict Anonymous
c) Restrict Share
d) Secure Channel

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 149

Which registry setting is used to disable administrative shares on a server?
a) HKLM\System\CurrentControlSet\Control\LanmanServer\Parameters\AutoshareServer value set to 0
b) HKLM\System\CurrentControlSet\Services\Lanmanserver\ParametersAutoshareserver value set to 0
c) HKLM\System\CurrentControlSet\Control\LanmanServer\Parameters\AutoshareServer value set to 1
d) HKLM\System\CurrentControlSet\Services\Lanmanserver\ParametersAutoshareserver value set to 1

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 150

Which registry key's security settings are used to control remote access permissions to a system registry?
a) HKLM\System\Software\Microsoft\CurrentVersion\Winreg
b) HKLM\SystemCurrentControlSet\Control\SecurePipeServers\Winreg
c) HKLM\System\CurrentControlSet\Services\Winreg
d) HKLM\System\CurrentControlSet\Control\LSA\Winreg

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 153

Where in the registry would you set exceptions to the winreg permissions?
a) HKLM\System\Software\Microsoft\CurrentVersion\Winreg\AllowedPaths\Machine
b) HKLM\SystemCurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine
c) HKLM\System\CurrentControlSet\Services\Winreg\AllowedPaths\Machine
d) HKLM\System\CurrentControlSet\Control\LSA\Winreg\AllowedPaths\Machine

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 154

Which two registry keys control which shares null users can access?
a) RestrictAnonymous and NullShares
b) RestrictAnonymous and NullSession
c) RestrictNullSessAccess and NullSessionShares
d) RestrictNullAccess and NullSessionShares

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 155

A _____ is a programming object which allows a process on one system to communicate with another process on a different system.
a) Pipe
b) Service
c) Thread
d) Slice

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 157

Which registry key lists the named pipes that can be accessed by null sessions?
a) HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes
b) HKLM\System\CurrentControlSet\Control\LSA\NullSessionPipes
c) HKLM\System\CurrentControlSet\Control\LSA\Parameters\NullSessionPipes
d) HKLM\System\Software\Microsoft\CurrentVersion\AllowedParameters\NullSessionPipes

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 159

How can you force the use of MS-Chapv2 for dialup users?
a) set HKLM\System\CurrentControlSet\Services\Authentication\ppp\chap\uselmpassword to 0
b) set HKLM\System\CurrentControlSet\Services\Authentication\ppp\chap\uselmpassword to 1
c) set HKLM\System\CurrentControlSet\Services\Rasman\ppp\chap\uselmpassword to 0
d) set HKLM\System\CurrentControlSet\Services\Rasman\ppp\chap\uselmpassword to 1

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 163

What can be used to thwart attacks that capture, modify, and retransmit SMB Packets?
a) SMB Certificates
b) SMB Signing
c) SMB Authentication
d) SMB Checking

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 166-167

What is the most important step to take to detect intruders?
a) Scan security logs frequently
b) Deploy a firewall
c) Enable Auditing
d) Use router ACL's

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 175

A _____ is a server or resource designed to ensnare intruders, log their actions, and alert Administrators.
a) Bastion Host
b) Honey Pot
c) Marked file
d) Decoy

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 181

Which 3 things should you do to secure the event log files?
a) Assign share permissions, audit the log files and control the manage auditing and security right
b) Assign NTFS permissions, audit the log files and control the manage auditing and security right
c) Assign NTFS permissions, audit the event viewer executable and control the manage auditing and security right
d) Assign share permissions, audit the event viewer executable and control the manage auditing and security right

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 185-186

Which log setting should not be used?
a) Do not overwrite events
b) Overwrite events as needed
c) Log Size equals
d) Overwrite events older than x days

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 188

What registry setting can be set to insure logs are never flushed?
a) HKLM\System\CurrentControlSet\Control\LSA\ShutdownOnAuditFail\1
b) HKLM\System\CurrentControlSet\Control\LSA\ShutdownOnLogFull\1
c) HKLM\System\CurrentControlSet\Control\LSA\CrashOnAuditFail\1
d) HKLM\System\CurrentControlSet\Control\LSA\ShutdownOnAuditFail\1

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 190

_____ continuously scans event logs in search of patterns of entries that indicate attacks, break-ins, or suspicious behavior.
a) Network IDS
b) Host Based IDS
c) Scan Engines

d) Performance Monitor

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 195

The best way to detect root kits or modified operating files in general – is to
a) Frequently reapply the latest service pack
b) Run nightly backups
c) Detect file modifications and restore clean copies
d) Write a script to search for strange file names

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 197

Which tools are used to make registry changes on hundreds of computers?
a) Regedit and regedt32
b) System Config and Group Manager
c) System Policy and Group Policy
d) System Editor and Group Modifier

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 206

How are conflicts between groups resolved in system policies?
a) By a random number generator
b) By allowing Administrators to weight different policies
c) By allowing Administrators to rank groups by priority
d) By applying the groups in alphabetical order

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 208

Windows systems automatically look for the policy file in the _____ share.
a) Sysvol
b) Bin
c) Root
d) Netlogon

Answer: D
Securing Windows NT: Step by Step Part 1,2 and 3 Page 210

Settings such as disable automatic logon, do not display last logged on username, logon banner, etc are all set with?
a) System Policy
b) Advanced User Rights
c) Logon Scripts
d) Startup Scripts

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 214

What registry setting disables cached credentials?
a) HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\CachedLogonsCount value set to 0
b) HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\CachedCredentials value set to 0
c) HKLM\CurrentControlSet\Control\LSA\Winlogon\CachedCredentials value set to 0

d) HKLM\CurrentControlSet\Control\Services\LanmanServer\Winlogon\CachedLogonsCount value set to 0

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 221

Users should either use _____ or use a _____ to protect their desktops when they are not at their desk.
a) A Kensigton Lock, Power on Password
b) BIOS Password, Power on Password
c) A Kensigton Lock, BIOS password
d) Lock workstation feature, password protected screensaver

Answer: D
Securing Windows NT: Step by Step Part 1,2 and 3 Page 222-223

You should educate users about passwords and make sure they are informed that violations of password commandments is a _____
a) minor inconvenience for IT staff
b) punishable offense
c) minor risk
d) misdemeanor

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 224

You can use an _____ to automate the searching for modem drivers.
a) URL
b) EMS
c) ERD
d) EBZ

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 225

What utility can you use to search for protocol analyzers?
a) Dumpel
b) L0pht Antisniff
c) Grinder
d) Brutus

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 227

You should always be scanning for _____.
a) new files
b) viruses
c) new utilities
d) new hardware

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 230

What registry key can be used to restrict the installation of print drivers to Administrators, Print Operators, and Power Users?
a) HKLM\Software\WintowNT\CurrentVersion\Printers\AddPrintDrivers value set to 1

b) HKLM\Software\CurrentControlSet\Control\Print\Providers\Servers\AddPrintDrivers value set to 1
c) HKLM\System\CurrentControlSet\Control\Print\Providers\LanmanPrintServices\Servers\AddPrintDrivers value set to 1
d) HKLM\System\CurrentControlSet\Print\Providers\LanmanServer\AddPrintDrivers value set to 1

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 233

What can you do to secure who can list scheduled jobs?
a) restrict access to HKLM\System\CurrentControlSet\Services\Schedule to the system account and the Administrator group
b) Restrict access to the AT service to the system account and the Administrators group
c) Restrict users that are members of the Scheduler group to the System Account and the Administrators group
d) Restrict access to HKLM\Software\WindowsNT\CurrentVersion\Schedule\Service to the system account and Administrator group

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 235

What happens to security if you add the following registry key
HKLM\System\CurrentControlSet\Control\LSA\SubmitControl value set to 1
a) Security is tightened and the group that can submit jobs is decreased
b) Security is weakened and the group that can submit jobs is expanded
c) Power Users are added to the group that can submit jobs
d) Account Operators are removed from the group that can submit jobs

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 78

How can you restrict use of floppy drives to only Administrators and Power Users?
a) By setting HKLM\System\CurrentControlSet\Control\Hardware\FloppyDriveLock\0
b) By using floplock.exe
c) By using passprop.exe
d) By setting a password on the floppy drive share

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 236

What two things should be done to protect authentication and subauthentication packages?
a) Insure the registry keys are restricted so only Administrators and the system account have write or modify access and audit access to these keys.
b) Remove Passfilt.dll and remove FPNWCLNT.dll
c) Restrict access to these keys so the everybody group has no access and audit for successful access to these keys
d) Add Passfilt.dll and add FPNWCLNT.dll

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 239

Which registry key do you set to disable 8.3 name generation?
a) HKLM\System\CurrentControlSet\Control\FileSystem\Ntfsdisable8dot3NameCreation value set to 0
b) HKLM\Software\Microsoft\WindowsNT\CurrentVersion\FileSyste\Ntfsdisable8dot3NameCreation value set to 0
c) HKLM\System\CurrentControlSet\Control\FileSystem\Ntfsdisable8dot3NameCreation value set to 1

d) HKLM\Software\Microsoft\WindowsNT\CurrentVersion\FileSyste\Ntfsdisable8dot3NameCreation value set to 1

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 240

What can be protected on an NT system if attackers have physical access to the target server?
a) NTFS Partitions
b) FAT Partitions
c) Nothing
d) Everything

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 243

Server hardware should be secured from all reasonable _____ and _____ threats.
a) security, viral
b) human, natural
c) unnatural, viral
d) digital, binary

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 246

In addition to securing servers themselves what other two items must be secured?
a) software and hardware
b) hard drives and cdrom drives
c) removable media and drives
d) backup tapes and hard drives

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 248

Setting boot priority in BIOS, disabling floppy drives at the hardware and or BIOS level, and using BIOS to require a password to reboot are all ways to prevent:
a) undesired shutdowns
b) undesired reboots
c) booting to another OS
d) unattended restarts

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 250-251

What is the most efficient way to audit backups?
a) Audit the executables of the backup application itself
b) Audit use of user rights
c) Set HKLM\System\CurrentControlSet\Control\LSA\FullPrivilegeAuditing\1
d) Audit backup operators group successful file reads

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 253

Since scheduled backups run as the system account or special service account what else must you do to insure you have an audit of backups if you are auditing the backup application itself?
a) Audit the utility used to schedule backups
b) Audit the AT command

c) Audit system account successful file reads
d) Audit use of user rights

Answer: A
Securing Windows NT: Step by Step Part 1,2 and 3 Page 253

It takes creative combination of accounts, groups, trusts, rights, and permissions to
a) secure NTFS partitions
b) secure FAT shares
c) delegate control safely
d) install NT server

Answer: C
Securing Windows NT: Step by Step Part 1,2 and 3 Page 256

How do you remove the "Add workstations to the domain right" from the account operators group?
a) by removing the account operators from the "Add workstations to the Domain" right in the user rights menu of user manager
b) you can not
c) by selecting show advanced user rights in user manager and than removing the account operators from the "Add workstations to the Domain"
d) By adding account operators to the list of groups under user rights "Can not Add workstations to Domain"

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 257

You and your organization may be liable for invading the privacy of users and perpetrators may avoid successful prosecution if users are not adequately for warned of your monitoring and detail of information you are capable of gathering, therefore _____ are very important.
a) Security Logs
b) Logon Banners
c) Audit Policies
d) Strong Managers

Answer: B
Securing Windows NT: Step by Step Part 1,2 and 3 Page 265-266

30 Questions from Internet Information Server

You can extract the real IP address of the server by using telnet or netcat to "GET /HTTP/1.0" if the file is:
a) static non-ASP
b) ASP
c) IDC
d) HTR

Answer: A
Internet Information Server for Windows 2000, Parts 1 & 2 Page 17

What is the most common threat to IIS?
a) Social Engineering
b) DOS
c) Port Scanning
d) Password Sniffing

Answer: B
Internet Information Server for Windows 2000, Parts 1 & 2 Page 20

What is the most effective way to stay a breast of new developments?
a) Purchase new books as they are published
b) Do frequent searches on the Internet with Alta Vista, etc.
c) Subscribe to e-mail bulletins
d) Attend seminars and conferences

Answer: C
Internet Information Server for Windows 2000, Parts 1 & 2 Page 35

When using host-based packet filtering on an HTTP-only server you should permit only:
a) TCP 80, TCP 443 and IP 6
b) UDP 80, UDP 446, and IP 6
c) TCP 80, TCP 446, and IP 6
d) TCP 80, TCP 443, and IP 4

Answer: A
Internet Information Server for Windows 2000, Parts 1 & 2 Page 37

What is an advantage of moving the root folder off the IIS server?
a) It is more secure because people do not know where the data is located
b) There is a performance increase because it no longer has to compete with the OS for disk access
c) The server becomes generic and can be restored quickly
d) It allows more freedom in domain structure

Answer: C
Internet Information Server for Windows 2000, Parts 1 & 2 Page 49

IIS server should be configured as _____.
a) A Backup Domain Controller
b) A Primary Domain Controller
c) A Stand Alone Server
d) A Member Server

Answer: C
Internet Information Server for Windows 2000, Parts 1 & 2 Page 52

What service on the Option Pack should never be installed because of known security holes?
a) KCC
b) RDS
c) DES
d) NFS

Answer: B
Internet Information Server for Windows 2000, Parts 1 & 2 Page 59

What should be done with \Inetpub\AdminScripts*.*?
a) They should be moved to %systemrrot%\system32\ an assign NTFS so only Administrators and System have Full Control
b) They should be deleted from the system
c) They should be assigned NTFS permissions so only Administrators have Full Control and System has change
d) Nothing the default settings are adequate

Answer: A
Internet Information Server for Windows 2000, Parts 1 & 2 Page 60

Which 2 folders should be deleted to remove sample scripts?
a) \InetPub\scripts\samples*.* and \ProgramFiles\CommonFiles\System\Msadc\Samples*.*
b) \InetPub\IISSamples*.* and \ProgramFiles\CommonFiles\System\Scripts\Samples*.*
c) \InetPub\IISSamples*.* and \ProgramFiles\CommonFiles\System\Msadc\Samples*.*
d) \InetPub\scripts\samples*.* and \ProgramFiles\CommonFiles\System\Scripts\Samples*.*

Answer: C
Internet Information Server for Windows 2000, Parts 1 & 2 Page 60

What should be done about Internet Printing on Windows 2000?
a) Delete the \printers virtual directory and unmap the .printer ISAPI extension
b) Audit access to the \printers virtual directory
c) Restrict access to the \printers virtual directory to authenticated users
d) Register the .printer ISAPI extension

Answer: A
Internet Information Server for Windows 2000, Parts 1 & 2 Page 61

You should never use _____ authentication because it is possible to extract the IIS server's real IP address if no realm is defined.
a) Digest
b) Windows Integrated
c) Basic
d) Anonymous

Answer: C
Internet Information Server for Windows 2000, Parts 1 & 2 Page 66

_____ represents anonymous users to the OS.
a) Guest
b) IUSR_Computername
c) IWAM_Computername
d) E-mail address

Answer: B
Internet Information Server for Windows 2000, Parts 1 & 2 Page 71

When using Digest Authentication _____ is used to encrypt the password.
a) MD5
b) Base64
c) Kerberos
d) DES

Answer: A
Internet Information Server for Windows 2000, Parts 1 & 2 Page 78

If using IE 4 as your browser which type of authentication can not be used?
a) Basic
b) Digest
c) Fortezza
d) Integrated Windows (NTLM + Kerberosv5)

Answer: B
Internet Information Server for Windows 2000, Parts 1 & 2 Page 78

What is the order of precedence of the different authentication methods?
a) Certificate, Anonymous, Integrated Windows, Basic, Digest
b) Anonymous, Integrated Windows, Basic, Digest, Certificate
c) Anonymous, Integrated Windows, Digest, Certificate, Basic
d) Certificate, Anonymous, Integrated Windows, Digest, Basic

Answer: A
Internet Information Server for Windows 2000, Parts 1 & 2 Page 89

If you do not install a certificate trust list on the IIS server to let it know which CA's to trust:
a) it will not trust any CA's
b) it will trust all CA's
c) it will display an error that you must add a trust list
d) it will only trust certificates from Verisign

Answer: B
Internet Information Server for Windows 2000, Parts 1 & 2 Page 102

IIS permissions are enforced by _____ when a user accesses the machine over HTTP or FTP.
a) Inetinfo.exe
b) IISserv.exe
c) LSA.exe
d) IISAdmin.exe

Answer: A
Internet Information Server for Windows 2000, Parts 1 & 2 Page 117

What danger exists if both the script source access and read permissions are enabled?
a) You could upload to a file to the scripts directory and execute it
b) You could download script files to reveal the source code
c) You could modify the source code of the script remotely
d) You could append a virus to the end of the script file

Answer: B
Internet Information Server for Windows 2000, Parts 1 & 2 Page 119

_____ should be disabled by default unless specifically enabled for some purpose because it allows one to see a list of files and subdirectories in a given folder when there is no default HTML file in that folder.
a) Scripts Only
b) Directory Browsing
c) Script Source Access
d) Execute

Answer: B
Internet Information Server for Windows 2000, Parts 1 & 2 Page 120

What is the deadliest combination of permissions on an IIS folder?
a) Write and Execute
b) Script source access and read
c) Read and Execute
d) Scripts Only and script source access

Answer: A
Internet Information Server for Windows 2000, Parts 1 & 2 Page 121

What is the effective permissions of combining NTFS and IIS permissions?
a) Least Restrictive
b) Cumulative
c) Most Restrictive
d) Additive

Answer: C
Internet Information Server for Windows 2000, Parts 1 & 2 Page 124

On Intranet IIS servers you should use _____ to prevent access from outside your organization as an extra security piece.
a) Host Based IDS
b) Personal firewalls
c) IP address blocking rules
d) Port Blocking

Answer: C
Internet Information Server for Windows 2000, Parts 1 & 2 Page 125-126

For stability a good strategy is to run inetinfo.exe?
a) Alone
b) With mission critical Applications
c) With all other web applications
d) On a separate partition

Answer: A
Internet Information Server for Windows 2000, Parts 1 & 2 Page 144

Unmapping unused ISAPI extensions is the equivalent of:
a) Disabling unused services
b) Locking down executables
c) Securing who can submit jobs to the schedule service
d) Restricting remote access to the registry

Answer: A
Internet Information Server for Windows 2000, Parts 1 & 2 Page 148

If you are not running Site Server you should unregister?
a) scrrun.dll
b) scrrun.ocx
c) scrrun.tlb
d) scrrun.exe

Answer: A
Internet Information Server for Windows 2000, Parts 1 & 2 Page 150

The utility used to copy metabase data from the local server to one or more servers over the network is called?
a) Metaedit.exe
b) Lissync.exe
c) Regedit.exe
d) Adsutil.vbs

Answer: B
Internet Information Server for Windows 2000, Parts 1 & 2 Page 159

Which registry value controls whether or not "# exec cmd" will function?
a) SSIExecDisable
b) SSIDisableCmdDirective
c) SSIExecEnable
d) SSIEnableCmdDirective

Answer: D
Internet Information Server for Windows 2000, Parts 1 & 2 Page 160

A website operator can:
a) throttle bandwidth
b) enable logging
c) create virtual directories
d) change the identification of websites

Answer: B
Internet Information Server for Windows 2000, Parts 1 & 2 Page 164

Setting HKLM\System\CurrentControlSet\Control\Security\Providers\Schannel\Eventlogging value to 4 logs:
a) errors
b) errors and warnings
c) informational an success events
d) everything

Answer: C
Internet Information Server for Windows 2000, Parts 1 & 2 Page 172

What types of authentication are available for FTP?
a) Digest, Integrated Windows, Certificate, Anonymous and Basic
b) Integrated Windows, Certificate, Anonymous, and Basic
c) Integrated Windows, Anonymous, and Basic
d) Anonymous and Basic

Answer: D
Internet Information Server for Windows 2000, Parts 1 & 2 Page 180

30 Questions from Active Directory for Windows 2000 in a Nutshell

The Database that contains information about the users and computers on the network, replacing the SAM database of NT 4 is called:
a) Dynamic DNS
b) Active Directory
c) Schema
d) Group Policy

Answer: B
Active Directory for Windows 2000 in a Nutshell Page 9

What is the central security feature of Active Directory that replaces and enhances NT 4 System Policy ?
a) Security Configuration Editor

b) Security Configuration Manager
c) System Editor
d) Group Policy

Answer: D
Active Directory for Windows 2000 in a Nutshell Page 11

When does active directory services get installed?
a) During setup of Windows 2000
b) During promotion to a domain controller
c) When you go into Network>Properties>Services>Add>Active Directory Services
d) When you double click on the actdirsv.exe on the Windows 2000 CD

Answer: B
Active Directory for Windows 2000 in a Nutshell Page 12

What must you do before demoting a Windows 2000 domain controller?
a) Nothing you can not demote a domain controller you must reinstall Windows 2000
b) You must promote a Backup Domain Controller
c) You must decrypt your e-mail and encrypting file system files
d) You must remove it from the schema of the Global Catalog server

Answer: C
Active Directory for Windows 2000 in a Nutshell Page 13

What is the implication of the everyone group having read access to accounts in AD?
a) Anonymous users on the Internet can download a list of all your usernames
b) All users on the network will be able to read group policies
c) All users on the network will be able to view security settings on the directories on the NTFS volumes
d) The guest account will be able to view passwords for all the user accounts.

Answer: A
Active Directory for Windows 2000 in a Nutshell Page 16

What is the default location for the Active Directory database file?
a) %systemroot%\NTDS\ntds.dit
b) %systemroot%\NTDS\ntds.edb
c) %systemroot%\NTDS\ntads.dit
d) %systemroot%\NTDS\ntads.edb

Answer: A
Active Directory for Windows 2000 in a Nutshell Page 21

What is the name of the shared folder containing scripts and policy files used by members of the domain including a scripts folder for backwards compatibility with Windows NT 4?
a) Netlogon
b) Sysvol
c) Ntpol
d) ADScript

Answer: B
Active Directory for Windows 2000 in a Nutshell Page 22

Why is it important to realize that because of Multimaster replication AD changes on one domain controller are automatically replicated to all other domain controllers?
a) So as you do not waste time making changes on all your DC's

b) So as you realize that the strength of AD security is determined by your "weakest link"
c) So as you do not manually replicate your changes from site to site
d) So as you make changes late at night to have better access to remote servers

Answer: B
Active Directory for Windows 2000 in a Nutshell Page 23

At a minimum DC must be physically secured (locked room, etc.) and the NTFS permissions on the \NTDS folder and contents set to:
a) Administrators: full control, system: full control, everyone: no access
b) Administrators: full control, system: full control, everyone: list
c) Administrators: full control, system: full control, everyone: read
d) Administrators: full control, everyone: list

Answer: C
Active Directory for Windows 2000 in a Nutshell Page 23

What must be done before the Schema Manager snap-in can be installed?
a) regserv.exe schmmgmt.dll
b) regsrv32.exe schmmgmt.dll
c) regserv.exe schmmgr.dll
d) regsrv32.exe schmmgr.dll

Answer: B
Active Directory for Windows 2000 in a Nutshell Page 27

What port does LDAP listen on by default?
a) 349
b) 369
c) 389
d) 493

Answer: C
Active Directory for Windows 2000 in a Nutshell Page 28

What is Microsoft's preferred language for scripting?
a) PerlScript
b) JScript
c) VBScript
d) KixStart

Answer: C
Active Directory for Windows 2000 in a Nutshell Page 28

What two windows script host engines are provided by default?
a) VBScript and PerlScript
b) PerlScript and Jscript
c) PerlScript and VBScript
d) VBScript and Jscript

Answer: D
Active Directory for Windows 2000 in a Nutshell Page 30

Intersite replication is manually configured and conveys data between DC's in different sites using _____ or _____.
a) SMB, SMTP

b) SMB, TFTP
c) RPC-Over-IP, SMB
d) RPC-over-IP, SMTP

Answer: D
Active Directory for Windows 2000 in a Nutshell Page 32

The sysvol share and shares you create with the Distributed File System snap-in are replicated by:
a) DFS
b) KCC
c) FRS
d) SMB

Answer: C
Active Directory for Windows 2000 in a Nutshell Page 34

Special DC's called _____ Servers contain the most often needed data from the AD of all the domains in the enterprise.
a) FSMO
b) Global Catalog
c) RID Master
d) Schema Master

Answer: B
Active Directory for Windows 2000 in a Nutshell Page 35

Windows 2000 domains have _____ trusts.
a) non-transitive
b) transitive
c) one way
d) bi-directional

Answer: B
Active Directory for Windows 2000 in a Nutshell Page 49

A _____ is two or more domains where one domain is not a DNS sub-domain of the other(s) but they still trust each other.
a) tree
b) forest
c) bush
d) branch

Answer: B
Active Directory for Windows 2000 in a Nutshell Page 51

For the ease of location, the assignment of permissions/policies and the delegation of authority _____ are used.
a) domains
b) global groups
c) universal groups
d) organizational units

Answer: D
Active Directory for Windows 2000 in a Nutshell Page 53

Which types of groups can not be created in mixed mode?

a) security groups
b) global groups
c) universal security groups
d) universal distribution groups

Answer: C
Active Directory for Windows 2000 in a Nutshell Page 57

Because universal groups are part of the GC frequent changes to them will cause high amounts of replication traffic between domains therefore universal groups should not contain _____.
a) individual user accounts
b) global groups
c) local groups
d) other universal groups

Answer: A
Active Directory for Windows 2000 in a Nutshell Page 57

Password policies for the domain are no longer set with user manager instead they are set with:
a) group policy
b) system policy
c) ADSI client
d) Ldp.exe

Answer: A
Active Directory for Windows 2000 in a Nutshell Page 60

Every property of every object in the AD database can have its own separate set of permissions this provides complete flexibility for:
a) creating groups
b) securing directories
c) delegating control
d) automating processes

Answer: C
Active Directory for Windows 2000 in a Nutshell Page 65

What two utilities allow you to launch programs under the security of a different user?
a) su.exe and runas.exe
b) connectas.exe and switchusr.exe
c) switchusr.exe and runas.exe
d) su.exe and connect.exe

Answer: A
Active Directory for Windows 2000 in a Nutshell Page 75

Which three times can group policies be applied?
a) Bootup, logon, and scheduled intervals
b) Logon, logoff, and scheduled intervals
c) Bootup, during connections, and scheduled intervals
d) Logon, during connections, and scheduled intervals

Answer: A
Active Directory for Windows 2000 in a Nutshell Page 83

What order are GPO's and NT 4 System policies applied?

a) Local GPO's, site GPO's, domain GPO's, organizational GPO's, NT 4 system policies
b) organizational GPO's, Local GPO's, site GPO's, domain GPO's, NT 4 system policies
c) NT 4 system policies, Local GPO's, site GPO's, domain GPO's, organizational GPO's
d) NT 4 system policies, organizational GPO's, domain GPO's, site GPO's, local GPO's

Answer: C
Active Directory for Windows 2000 in a Nutshell Page 89

If you wish to set the GPO on a container and block the inheritance from any parent containers:
a) you would check the "loop back" box
b) you would check the "no override" box
c) you would check the "block policy inheritance" box
d) you would check the "no policy blocking" box

Answer: C
Active Directory for Windows 2000 in a Nutshell Page 90

If you wish to force a parent containers settings down to all sub-containers then use:
a) "loop back" checkbox
b) "no override" checkbox
c) "block policy inheritance" checkbox
d) "no policy blocking" checkbox

Answer: B
Active Directory for Windows 2000 in a Nutshell Page 90

What two permissions must a user have at minimum to have a GPO applied to their desktop?
a) Read and apply group policy
b) Change and apply group policy
c) List and apply group policy
d) Write and apply group policy

Answer: A
Active Directory for Windows 2000 in a Nutshell Page 95

Logon/logoff scripts run as the _____, and startup/shutdown scripts run as the _____.
a) user, user
b) user, system
c) system, user
d) system, system

Answer: B
Active Directory for Windows 2000 in a Nutshell Page 101