Global Information Assurance Certification Paper

Submitted by Greg Owen, SANS DC 2000

All 90 questions in this section are from book 5.1/5.2/5.3, "Securing Windows NT: Step-By-Step, Parts 1, 2, and 3." The correct answer is marked with emphasized text.

From Page 12

Typical phases of attack include:

- Reconnaissance.
- Acquiring a user account.
- Avoiding detection.
- *All of the above*.
- None of the above.

From Page 14

The Reconnaissance stage of an attack

- Is always followed by either a DoS attack or an attempt at system compromise.
- Must be done before any other type of attack is possible.
- *May be either random or specifically targeted.*
- All of the above.
- None of the above.

From Page 17

Ping and Tracert are tools commonly used by attackers for

- *Reconnaissance*
- Denial of Service
- Port Scanning
- Social Engineering

From Page 17

Port scanning identifies what services are running on a machine, and can also indicate to the attacker

- Which version of a given service is in use.
- *What operating system a server is running*.
- The username of the currently logged in user.
- All of the above
- None of the above

From Page 19

In order to list NetBios services running on a server, the attacker would use:

- Back Orifice
- L0phtCrack
- *NBTSTAT.EXE*
- A 3rd-party Port Scanner

From Page 21

NBTSTAT.EXE can be used to reveal

- Whether a server is running Microsoft Exchange.
- Who is currently logged into a server.
- Who the master browser for a server is.
- *All of the above*.
- None of the above.

From Page 25

The single best defense against all attacks is

- The latest service pack
- Consistently applying hotfixes
- Choosing secure passwords
- *A firewall*

From Page 28

For security purposes, an organization should permit internet access to:

- *DNS servers only.*
- WINS servers only.
- DNS and WINS servers.
- Neither DNS nor WINS servers.

From Page 29

Using DNS forwarding DOES NOT increase security by:

- Simplifying firewall rules.
- Limiting Internet access to Internal servers.
- *Encrypting DNS zone transfers.*
- All of the above.
- None of the above.

From Page 32

Hackers can find RAS servers by

- Searching publicly available information, such as your website.
- Using social engineering against your users.
- *Using wardialers.*
- All of the above.
- None of the above.

From Page 34

A personal firewall

- Is plugged in between a PC and the network switch or hub.
- Is designed to protect information being transmitted by the user.
- *Is designed to protect only the machine it is installed on.*
- Can remove the need for a regular corporate firewall.

From Page 39

DoS attacks are noticeable because

- Hackers use them to post personal or political messages on your website.
- They cause unusual failure modes, like the Blue Screen of Death.
- Windows NT logs any DoS-related activity to the Event Log.

- *Performance degrades below norms without a reasonable internal explanation.*

From Page 42

In order to keep a Windows NT server current,

- *Service Packs must be re-applied whenever the server configuration is changed.*
- Service packs must be re-applied weekly.
- Regular backups must be compared against existing system files.
- All of the above.
- None of the above.

From Page 45

For security, the POSIX subsystem

- Should be upgraded to the OS/2 subsystem.
- *Should be removed if not in use.*
- Should be configured for C2 security.
- Should be configured to use TCP/IP rather than NetBeui.

From Page 46

Microsoft Hotfixes are important because

- They correct stability problems that Service Packs introduce.
- *They are available before fixes are incorporated into Service Packs.*
- They target the important problems that Service Packs ignore.
- All of the above.
- None of the above.

From Page 49

The most effective way to be aware of NT security issues is to

- Subscribe to commercial Windows NT magazines.
- Use search engines on a weekly basis to search for security exploits.
- Spend 2 hours each day on IRC looking for hacker channels.
- *Subscribe to various Windows NT email security bulletins.*

From Page 50

Filling the disks on an NT server may create a DoS if

- *The system runs out of free hard drive space for temporary and paging files.*
- The network connection is slow enough to be choked by the file transfer.
- The system is not using RAID disks.
- The system has more memory than it has hard disk space.

From Page 51

To prevent a Blue Screen of Death, administrators should:

- Install a generous amount of physical RAM.
- Placing a paging file sized at RAM+11MB on the system.
- Use Performance Monitor to keep tabs on disk usage.
- *All of the above.*
- None of the above.

From Page 53

To identify a SYN attack in progress, you should

- Unplug the network connection to see if performance improves.
- *Run NETSTAT.EXE and study how many connections are in a state of SYN.*
- Run IISSYNC.EXE to clear SYN-only connections.
- Increase the amount of paging space on the system and see if performance improves.

From Page 54

The SynAttackProtect registry value is available as of

- Service Pack 3
- Service Pack 4
- *Service Pack 5*
- Service Pack 6a

From Page 55

In order to completely avoid DoS attacks, an administrator should:

- Remove network connections on mission-critical machines.

- Install both a firewall and a packet-filtering router.
- Stay at the most current Service Pack + Hotfix level
- *Prepare to recover from DoS because they cannot be completely avoided.*

From Page 56

Multiple installations of NT

- Must be installed on distinct partitions.
- Must be installed on RAID arrays.
- *Provide a working system for recovery if the first installation is broken.*
- Provide multiple layers of defense on a single box.

From Page 57

Tape backup systems DO NOT

- *Remove the need for emergency repair disks.*
- Sometimes require an existing OS installation in order to restore.
- Provide high-availability disk storage.
- All of the above
- None of the above.

From Page 57

The Emergency Repair Disk can be used to

- Repair essential registry hives.
- Repair and replace operating system files like BOOT.INI.
- Compare installed files to original copies from the installation CD.
- *All of the above.*
- None of the above.

From Page 58

To use an Emergency Repair Disk, the computer should be booted

- Into an existing NT installation.
- Using the Emergency Repair Disk floppy.
- Using an MS-DOS boot disk.
- *Using the original setup disks.*

From Page 59

An Emergency Repair Disk is created using

- ERD.EXE
- ERDISK.EXE
- *RDISK.EXE*
- RESCUE.EXE

From Page 60

Emergency Repair Disks should be protected
I. Using SYSKEY.EXE
II. Using 3rd-party encryption programs
III. By physically securing them.
IV. They needn't be; they require the Administrator password to be useful.

- I and II
- II and III
- III and IV
- IV and I
- *I and III*

From Page 61

In order to quickly recover a crashed server,

- Backups should be made daily at midnight.
- The Operating System partition should use RAID-5
- *Ready-to-go drives or binary images should be prepared beforehand.*
- Cold spares of complete servers with all installed software should be ready.

From Page 63

The best way to stop an existing DoS attack is to

- Shut down the router interfaces that the attack is coming from.
- *Study the attack using a protocol analyzer to learn how to block it.*
- Install more firewalls between the source of the attack and the target.
- Call your local CIRT and ask for assistance.

From Page 66

The best tool for identifying the effects of a DoS attack is

- A protocol analyzer.
- The Windows Event Viewer.
- *The Windows Performance Monitor*.
- The Windows Task Manager.

From Page 67

The Windows Event Viewer provides access to the logs for

- Only Microsoft Applications.
- All Microsoft Applications.
- *Some Microsoft Applications and some 3rd-party Applications*.
- Only the Windows Operating System.

From Page 68

Windows CrashDump files are typically named

- PAGEFILE.SYS
- CRASH.DMP
- *MEMORY.DMP*
- DUMP.MEM

From Page 69

Windows CrashDump files are enabled using

- *The Control Panel->System applet*.
- The Task Manager.
- The Registry.
- CONFIG.SYS

From Page 71

In order to steal, alter, or destroy data, an attacker generally requires at least the following:

- *A regular user account*

- A local administrator account
- A domain administrator account
- Physical access to the machine.

From Page 73

When attempting to get in using guessed passwords, an attacker will attack the Administrator account because

I. It is the most powerful account on the system.
II. It cannot be renamed.
III. Services access the Administrator account.
IV. It cannot be locked out due to bad login attempts

- I and II
- II and III
- III and IV
- *IV and I*
- IV and II

From Page 73

Password guessing programs

- *Are easily available on the Internet.*
- Are munitions under ITAR and therefore strictly controlled.
- Are only available via Microsoft pay-per-incident support.
- Come as part of the Resource Kit.

From Page 74

Password-sniffing programs work well because

- Passwords are transmitted in the clear across the network.
- *The challenge-response protocol used for transmitting passwords* can be broken using reasonably small resources.
- The encrypted password is all that is required for some forms of access.
- All of the above.
- None of the above.

From Page 75

Hackers can acquire the full database of encrypted passwords by gaining access to

- Emergency Repair Disks
- Tape Backups
- %SystemRoot%\Repair\Sam._
- *All of the above*.
- None of the above.

From Page 76

The Security Configuration Editor can NOT be used to:

- Configure the local machine's settings to match a template.
- Compare the local machine's settings against a template.
- Define a template of security configuration settings.
- All of the above.
- *None of the above*.

From Page 78

Security Configuration Editor tasks can be executed from the command line using which utility?

- SCEEDIT.EXE
- *SECEDIT.EXE*
- REGEDT32.EXE
- MSSCE.EXE

From Page 80

A "Null Session" is best described as:

- A NETLOGON connection where no data is passed.
- An IIS connection using "Anonymous Authentication."
- *A logon to an NT server where both the username and password are a null character*.
- A logon to an NT server by a user whose password is blank.

From Page 81

Null sessions are NOT used

- For administrative purposes when one's user account is unavailable.
- For cross-network communication by the System account.
- Between two NT domains.
- *By IIS "Anonymous Authentication."*

From Page 85

To prevent null sessions from listing users and groups from one's domain, a registry change must be made

- On the domain's PDC.
- *On all the domain's Domain Controllers.*
- On all the NT Servers in the domain.
- On all the NT Servers and NT Workstations in the domain.

From Page 86

If null session access is restricted using the RestrictAnonymous key, the following is NOT a workaround in a multidomain environment:

- Creating a second account in the trusted domain that is a member of Local Administrators for each system in the trusting domain.
- Manually entering TRUSTEDDOMAIN\username or TRUSTEDDOMAIN\groupname rather than listing users and groups from TRUSTEDDOMAIN.
- *Configuring the Administrator and Service accounts in each domain with the exact same usernames and passwords.*
- Creating a two-way trust between domains.

From Page 88

Using extended ASCII characters in a password can cause problems when:

- *Using the password for a web-based application.*
- Using a laptop which doesn't have a numeric keypad.
- Configuring the passwords for service accounts.
- Marking a password as expired.

From Page 88

The Administrator account can be locked out locally when

- The PASSPROP.EXE program has been used.

- The Administrator account is used outside of configured logon hours.
- On any system with Service Pack 5 or greater.
- *Never*.

From Page 90

The Guest account is disabled by default

- On NT Workstation.
- *On NT Server*.
- On NT Workstation and NT Server.
- On any system with Service Pack 5 or greater.

From Page 96

The following systems DO NOT accept logins from both Local and (Domain) Global account databases:

- PDCs
- BDCs
- Exchange Servers
- All of the above
- *None of the above*

From Page 99

For Service accounts, the order of preference is to use:

- First local account, then domain account, then system account.
- First local account, then system account, then domain account.
- First domain account, then system account, then local account.
- *First system account, then local account, then domain account*.

From Page 101

To filter out weak passwords, Administrators should use

- FPNWCLNT.DLL
- PASSPROP.DLL
- *PASSFILT.DLL*
- L0phtCrack

From Page 102

Custom password filters can be created

- By Microsoft on a pay-per-incident basis.
- *By any administrator with access to the Win32 SDK or MS TechNet.*
- By any user of the system with the "Modify password properties" right.
- All of the above.
- None of the above.

From Page 105

Minimum Password Length can be any number between

- 0 and 8
- *0 and 14*
- 1 and 14
- 1 and 16

From Page 109

The Security Accounts Manager contains user passwords hashed with

I. LanManager
II. MD4
III. NTLM
IV. DES

- *I and II*
- II and III
- III and IV
- IV and I
- IV and II

From Page 113

NTLMv2 was introduced to Windows NT starting with

- Service Pack 3
- *Service Pack 4*
- Service Pack 5
- Service Pack 6a

From Page 117

Directory Services Client for Windows 95/98 upgrades

- SECURE32.DLL
- VNETSUP.VXD
- VREDIR.VXD
- *All of the above*
- None of the above

From Page 118

NetLogon channels can be established

- On a stand-alone NT computer
- Using a Windows 95/98 computer
- *Between member machines of two different domains with a one-way trust*
- All of the above
- None of the above

From Page 120

The ability to secure the NetLogon channel was added with

- *Service pack 4*
- Service pack 5
- Service pack 6a
- It wasn't added; it is part of an unpatched Windows NT installation.

From Page 122

Social engineering targets Network Administrators because

- They lack the required social skills to fend off such an attack.
- They are required to be helpful as part of their job.
- *They are most likely to possess useful information.*
- They aren't targeted; company executives are preferred targets.

From Page 124

Reverse Social Engineering refers to

- Administrators attempts to deflect attackers.
- The testing "White Hat" hackers do to help Administrators.
- *Maneuvering a user or administrator to initiate contact with a hacker.*
- What hackers do to confuse their trail after a penetration of security.

From Page 131

A 1996 FBI report estimated that what percent of security breaches are perpetrated by legitimate internal users?

- 10%
- 25%
- *75%*
- 90%

From Page 132

The default NTFS and share permissions are

- *Excessively lax*
- As strong as they can be without inconveniencing users
- Strong enough to require loosening for many users
- Specified by the Network Administrator at system install time.

From Page 134

Local and Global groups are used as follows:

- Global groups for assigning rights, Local groups for grouping users.
- *Local groups for assigning rights, Global groups for grouping users.*
- Local groups within a single domain, Global groups across trusting domains.
- Local groups on non-Domain NT installations, Global groups in an NT Domain.

From Page 136

The most secure filesystem is

- FAT
- FAT32
- *NTFS*
- SMBFS

From Page 141

As a rule of thumb, only the following account(s) should have Full Control permission as their final, effective permission:

- Administrators
- The System account
- Creator Owners
- *All of the above*
- None of the above.

From Page 142

The Everyone group does NOT contain

- Users from untrusted domains
- Users who have no NT Domain
- Anonymous Internet users
- All of the above
- *None of the above*

From Page 146

Members of which group can use DACL/SACL tools to assign ownership of a file?

- Domain Administrators
- Local Administrators
- *Backup Operators*
- Printer Operators

From Page 151

To disable Administrative shares on an NT Workstation,

- log in as Administrator and unshare them using Windows Explorer.
- Manually share the appropriate filesystems with explicit "No Access" for everyone.
- Create the AutoShareServer registry key.
- *Create the AutoShareWks registry key.*

From Page 152

The HKLM\System portion of the registry is shared by default on

- *NT Workstation only*.
- NT Server only.
- NT Workstation and NT Server.
- Neither NT Workstation nor NT Server.

From Page 156

The NullSessionShares registry key has no effect when

- The "Everyone" group has no permissions to a share.
- RestrictNullSessAccess is set to 0
- *Both 1 and 2*.
- Neither 1 nor 2.

From Page 157

Which of the following is NOT a filesystem:

- FAT
- NTFS
- *FSMO*
- NPFS

From Page 165

The Network Monitor Console can be detected by looking for

- The registered NetBios name "computername[BE]"
- *The registered NetBios name "computername[BF]"*
- Lack of response to PING
- Excessive response to PING

From Page 166

SMB sessions send the User ID number in cleartext

- *Always*
- With EnableSecuritySignature set to 1

- With RequireSecuritySignature set to 1
- Never

From Page 175

IIS logging information can be written to

- Windows Event Log
- ASCII text files
- An SQL database
- *All of the above*
- None of the above

From Page 178

Auditing is most effective when

- No events are logged.
- Only failure events are logged.
- *Some success and some failure events are logged.*
- All events are logged.

From Page 179

The following tool(s) can be used to manage auditing:

- Windows Explorer
- REGEDT32.EXE
- Security Configuration Manager
- *All of the above*
- None of the above

From Page 180

Custom events cannot use the following severity:

- Success
- Information
- Failure
- *Debug*

From Page 181

Event logs are stored

- In the HKEY_LOCAL_MACHINE registry hive
- *In the %SystemRoot%\System32\Config folder*
- In the %SystemRoot%\System32\Logs folder
- In the %SystemRoot%\Repair folder

From Page 187

The maximum size an event log can be configured for is

- 512K
- 32,768K
- 1,048,576K
- *4,194,240K*

From Page 193

Which of the following cannot be used to archive event logs?

- The Windows Event Viewer
- DUMPEL.EXE from the Resource Kit
- SomarSoft DUMPEVT.EXE
- *The Unix SNMP tools*

From Page 195

Automated Event Log Analyzers are also known as

- LIDS (Log Intrusion Detection Systems)
- *HIDS (Host-based Intrusion Detection Systems)*
- NIDS (Network-based Intrusion Detection System
- AELA (Automated Event Log Analyzers)

From Page 197

If you suspect a system compromise, you should

- Immediately format the disk, reinstall the OS, and restore data from tape.

- *Re-install the latest service packs and hotfixes.*
- Install Netcat to try and track the intruder.
- All of the above.
- None of the above.

From Page 201

An Incident Response Plan

- Should be developed during a security incident, since each incident is different
- Should not be reviewed by management, who might leak it via Social Engineering
- *Should be reviewed my management, who should authorize action in an emergency.*
- Should be stored only in paper, which is not available to remote hackers.

From Page 203

In NT 4.0, registry changes can be made to many machines automatically using

- REGEDIT.EXE
- REGEDT32.EXE
- Group Policy
- *System Policy*

From Page 210

A System Policy file can contain the settings for

- Users
- Groups
- Computers
- *All of the above*
- None of the above

From Page 215

Disabling registry editing tools via System Policy does NOT effect

- .reg file merges
- REGEDIT.EXE
- REGEDT32.EXE
- *POLEDIT.EXE*

From Page 218

The Resource Kit utility AUTOLOG.EXE stores passwords

- *In cleartext.*
- Using a LanManager hash.
- Using an NTLM hash.
- It doesn't store passwords.

From Page 219

The GetAdmin, SecHole, and SecHoleD system compromise programs are not functional

- If Service Pack 4 is installed.
- *If Service Pack 6a is installed.*
- If Null Session access is disabled.
- When a user is logged on locally.

From Page 222

System Policy changes are applied

- Hourly.
- Daily.
- *When a user logs on.*
- When a user logs off.

From Page 225

Protocol Analyzers can be rendered less useful by

- *a fully switched network*
- NTLM authentication
- Packet-filtering routers
- All of the above
- None of the above

From Page 230

The threat posed by computer viruses

- Is small and shrinking
- *Is enormous and growing*
- Is negated by packet-filtering routers
- Should only be blocked on incoming traffic

From Page 233

Printer drivers run

- As System users
- With Administrative privileges
- *In kernel mode*
- Under DllHost.exe

From Page 236

Floppy drives can be disabled

- By nothing short of physically removing them from the system.
- Using the FloppyLock registry key
- *Using the system BIOS*
- All of the above.
- None of the above.

All 30 questions in this section are from book 5.4, "Internet Information Server." The correct answer is marked with emphasized text.

From Page 15

In order to map a web site, an attacker might:

- Use the diagrams returned by popular search engines.
- *Download the entire website for offline study.*
- Download the sites search engine index.
- All of the above.

From Page 16

Error messages that IIS returns to the browser:

- Discourage the attacker from exploring the web site.
- Indicate a DoS attack in progress.
- *Educate the attacker about the way the site works.*
- Warn administrators that someone is probing their defenses.

From Page 18

Attackers try to obtain source code to web site scripts because:

- The source code may reveal existing security holes.
- The scripts may contain useful usernames or passwords.
- The scripts may help map out the target network.
- *All of the above.*
  e) None of the above

From Page 23

Brute force attack tools like Xavior and WebCracker work by:

- Causing repeated requests to computationally-expensive SSL-encrypted links.
- Sending malformed packets which the operating system can't handle.
- Encrypting a large dictionary of words and comparing them to the encrypted text retrieved from the web server.
- *Sending an enormous number of possible usernames and passwords to a server that requires authentication.*

From Page 25

Buffer overflows can compromise a server by:

- *Corrupting the running code on the server.*
- Using up all the memory on the server.
- Reserving network resources on a server.
- Exploiting script engines carelessly left in accessible directories.

From Page 27

IIS secures data in transit using:

- Base64 encoding
- NTLM authentication
- *SSL encryption*
- NTFS permissions

From Page 28

Session hijacking occurs when:

- Browser sessions are not SSL-encrypted.
- *The server stores session tokens in hidden form values.*
- The server stores session tokens in an unencrypted database.
- The client stores tokens on shared filesystems.

From Page 47

Static IIS web pages should be stored

- On the system partition.
- On a read-only tape.
- On an encrypted filesystem.
- *On a read-only share on another machine.*

From Page 54

IIS communications can be made more secure by using:

- NetBeui
- IPX/SPX
- *Both of the above*
- None of the above

From Page 57

The sample pages and scripts that come with IIS

- Enhance security by providing "best practices" examples.
- Enhance security by ensuring consistent installations.
- Damage security by lessening free space on the data partition.
- *Damage security by providing exploitable scripts to attackers.*

From Page 57

Users can change their passwords using IIS

- *Under IIS 4.0, but not IIS 5.0.*
- Under IIS 5.0, but not IIS 4.0.
- Only when the connection is SSL-encrypted.
- Only when connected via Local Area Network.

From Page 61

"401 Access Denied" can indicate

- The user's browser doesn't support Integrated authentication.
- The user's browser is not allowing cookies.
- The server will never allow access to the requested file.
- *The server requires further authentication before accessing the requested file.*

From Page 61

The WWW-Authenticate header

- Is how the client requests the server switch to SSL.
- Is how the server requests the client switch to SSL.
- Is how the client indicates what forms of authentication may be used.
- *Is how the server indicates what forms of authentication may be used.*

From Page 62

Anonymous authentication using HTTP

- Is an oxymoron
- Requires the user's email address as the password.
- *Is transparent to the user.*
- Requires a null user connection to the server

From Page 65

Basic authentication uses

- SSL

- SMB
- *Base64*
- NTLMv1

From Page 68

Digest authentication is used

- For broad support by RFC-compatible clients.
- When transferring a large number of files.
- Instead of Basic Authentication whenever both are offered.
- *Only with IIS 5.0 and Windows 2000.*

From Page 77

Certificate authentication is not stronger than

- Integrated Windows authentication.
- Digest authentication.
- NTLM + Kerberos authentication.
- *All of the above*.
  e) None of the above.

From Page 77

The complexity of Certificate authentication

- *Decreases security by complicating management*.
- Increases security when used to protect Win98 clients.
- Decreases security because of its weak encryption.
- All of the above.
  e) None of the above.

From Page 78

Fortezza authentication was developed by

- The Mafia
- *The NSA*
- The CIA
- The Open Source movement

From Page 80

Digest authentication uses

- *MD5 encoding*
- Base64 encoding
- ROT13 encoding
- SSL encryption

From Page 81

SSL certificates adhere to which standard?

- X.400
- X.443
- X.500
- *X.509*

From Page 81

In order to have two-way encryption, you must have

- A public key and a private key.
- A Certificate Authority like Verisign.
- *One key that works for both encoding and decoding.*
- All of the above.
  e) None of the above.

From Page 100

SSL is an acronym for:

- Server Side Locking
- *Secure Sockets Layer*
- Secure Scripting Language
- Secure Server Logging

From Page 100

You can identify an SSL document because:

- *The URL begins with "https://"*
- The URL begins with "shttp://"
- The URL ends with ".shtml"
- The URL ends with ".ssl"

From Page 105

Best practices for implementing SSL include:

- Using a trusted Certificate Authority
- SSL-encrypting both an HTML form and the form submission URL.
- Not using SSL except where really necessary.
- *All of the above*.
  e) None of the above.

From Page 107

IIS permissions can control the following:

- CPU throttling
- IP address blocking
- Script Source Access
- *All of the above*
  e) None of the above

From Page 111

The deadliest combination of IIS permissions is:

- Read and Write
- *Script Source Access and Scripts Only*
- Write and Execute
- Directory Browsing and IP Address Blocking

From Page 115

IP address restrictions

- Remove the need for SSL
- Protect IIS from DoS attacks
- Require DNS lookups to function properly
- All of the above

e) None of the above

From Page 140

ISAPI extensions allow IIS to

- Be used as by ASPs (Application Service Providers)
- Run CGI programs written for other operating systems
- Run scripts in an isolated 'sandbox' for security reasons.
- *Trigger the execution of a program on the server by accessing a file*.

From Page 144

IIS 5.0 is to DllHost.exe as IIS 4.0 is to

- cacls.exe
- mts.exe
- *mtx.exe*
- wsh.exe

From Page 150

The following extensions are associated with Index Server:

- *.idq*
- .idc
- .stm
- All of the above
- None of the above

All the questions in this file are from book 5.5, "Active Directory for Win2000 in a Nutshell." The correct answer is marked with emphasized text.

<

From Page 108

The 'Computer Configuration->Administrative Templates' section of a GPO is used to modify:

- HKEY_Current_User
- *HKEY_Local_Machine*
- The Metabase
- The Global Catalog

From Page 108

The 'User Configuration->Administrative Templates' section of a GPO

is used to modify:

- *HKEY_Current_User*
- HKEY_Local_Machine
- The Metabase
- The Global Catalog

From Page 104

Local Policies allow you to

I. Audit the access of global system objects.
II. Block access to all but the listed TCP/IP ports.
III. Restrict floppy access to locally logged-on user only.
IV. Tag suspicious use of the network in the Domain Controller's event log.

- I and II
- II and III
- III and IV
- *I and IV*

e) II and IV f) III and I

From Page 102

GPO scripts can be run

- In the order they are listed in the directory.
- All at the same time.
- Hidden from the user.
- *All of the above*.

e) None of the above.

From Page 98

Group Policy cannot be used to

- Install applications
- Repair applications
- Remove applications
- *Search for applications*

From Page 97

In order to place restrictions on one member of a group, you should

- Create a sub-group with the appropriate restrictions.
- *Deny that member Read and Apply Group Policy permissions.*
- Disable that member's user account.
- Assign the group member to a GPO Delegation.

From Page 91

A GPO uses loopback mode

- To keep sensitive traffic off the network.
- To emulate network traffic when off the LAN.
- *Allow one GPO to override all other GPOs.*
- For internal verification purposes.

From Page 89

4LSDOU

- Is the first virus released that targeted Windows 2000 specifically.
- *Describes the order of precedence for GPOs.*
- Is the database technology Active Directory is based on.
- Describes the Active Directory Object Hierarchy.

From Page 86

GPO Links

- *Bind GPOs to containers.*
- Allow GPOs to inherit properties from other GPOs.
- Enable GPOs to be manipulated over the web.

- Allow client workstations to reference AD-based GPOs.

From Page 84

Group Policies can be linked to

I. Sites
II. Local Groups
III. Global Groups
IV. Organizational Units

- I and II
- II and III
- III and IV
- *IV and I*

e) IV and II f) I and III

From Page 83

The scripts referred to by Group Policy are stored in:

- Active Directory
- LDAP
- *SYSVOL folder*
- NETLOGON share

From Page 81

Group Policy allows you to set policies for:

- Kerberos
- IPSec
- PKI
- *All of the above*

e) None of the above

From Page 80

The Delegation Wizard is most useful

- *As a learning tool*
- Because it removes the need to work with raw permissions
- Because it makes repairing permissions simpler

- All of the above
  e) None of the above

From Page 77

The precision of delegation is limited only by:

- The free space remaining in the Active Directory.
- The security-consciousness of the organization.
- *The flexibility and granularity of Active Directory permissions.*
- The backwards-compatibility required by downlevel networks.

From Page 75

You can get SU.EXE and RUNAS.EXE

- Both as part of Windows 2000.
- *SU.EXE from the Resource Kit, RUNAS.EXE as part of Windows 2000.*
- RUNAS.EXE from the Resource Kit, SU.EXE as part of Windows 2000.
- From Pedestal Software, a third-party vendor.

From Page 75

Null user access to Active Directory

- Can be limited using the HKEY_LOCAL_MACHINE\System\CurrentControlSet \Control\SecurePipeServers\Winreg key.
- Can be achieved using the CACLS.EXE program
- *Is dangerous when "Pre-Windows 2000 Compatible Access" is enabled.*
- Cannot be scripted using WSH.

From Page 72

Active Directory containers and objects should use inherited permissions because

- It reduces the processor overhead of checking permissions.
- Most containers and objects don't need customized permissions.
- Orphaned, or non-inheriting, objects don't participate in security.
- *Orphaned, or non-inheriting, objects make it hard to scan permissions for security holes.*

From Page 72

The determining factor in configuring Organization Units is:

- Adherence to the company Organizational chart.
- *To make the process of assigning permissions more efficient.*
- The number of domains that exist in the tree.
- To apply security policies to objects from more than one domain.

From Page 68

The DSACLS.EXE utility from the Resource Kit

- Can edit permissions on an item without overwriting the item's other permissions.
- Can reset permissions back to defaults define in the schema.
- Uses the RFC1779 naming convention.
- *All of the above.*
- None of the above.

From Page 62

When an account is trusted for delegation,

- It is eligible to be granted authority for Active Directory administration.
- *It can take on the identity of a remote user and perform actions on their behalf.*
- It can be used across two different Domains.
- All of the above.
- None of the above.

From Page 60

User passwords may be changed

- By Windows Scripting Host scripts.
- With the NET USER command.
- Using the "AD Users and Computers" snap-in.
- *All of the above.*
- None of the above.

From Page 57

Universal groups, whether for Distribution or Security,

- Are the Windows 2000 version of NT 4.0 Global Groups.
- Can contain Users, Global Groups, and Local Groups.
- Are equally available in Native and Mixed mode domains.
- All of the above.
- *None of the above*.

From Page 52

Windows NT 4 domains are the equivalent of Windows 2000

- *Organizational Units*
- Sites
- Domains
- Trees
- Forests

From Page 51

A "Forest" consists of

- A root domain and a set of subdomains.
- Two or more subdomains which do not trust each other.
- Two or more domains which are not subdomains of each other, and which do not trust each other.
- *Two or more domains which are not subdomains of each other, but which do trust each other*.

From Page 48

A Windows 2000 domain might be named

- FOSSEN
- FOSSEN-NET
- *fossen.net*
- fossen_net

From Page 46

ADSI can bind to directories using the following ProgIDs:

I. LDAP://
II. IIS://
III. HTTP://
IV. NETLOGON://

- *I and II*
- II and III
- III and IV
- IV and I
- I and III

From Page 41

Schema changes are most dangerous when

- They are reversed after having been replicated to all controllers.
- They are reversed during replication to all controllers.
- *They are used to mark any item "mandatory."*
- They are implemented without executing "regsvr32 schmmgmt.dll" first.

From Page 38

In a Mixed-mode Windows 2000 domain,

- Each domain controller acts as a BDC for NT 4.0 machines.
- Each domain controller acts as a PDC for NT 4.0 machines.
- *One and only one domain controller acts as a PDS for NT 4.0 machines.*
- All of the above.
- None of the above.

From Page 35

How much of the Active Directory is replicated is determined by

- Organizational Units
- Sites
- *Domains*
- Trees
- Forests

From Page 33

If you want to modify the replication transport link between two physical locations that are in the same domain,

- You must put each location in a different Site.
- You must modify the AD Schema.

- You must enable a high-bandwidth link between the two locations.
- All of the above.
- *None of the above*