Global Information Assurance Certification Paper

SANS Conference Parliament Hill 2000, Securing Windows NT Practical

Written by Kentaro Sato, Office Phone (201) 729-7457

9/24/2000

INSTRUCTION:

For each question, chose the answer that best fit the question within the context of the question. Although avoided as much as possible, some of the answers may be true but not relative to the question being asked.

In section 1, all questions are regarding Windows NT 4.0, unless otherwise stated. Section 2 and 3 both deals with Windows 2000 systems.

SECTION 1
From *Securing NT Step by Step*, 90 questions

Any registered domain name must be registered to the InterNIC. Registration will require the owner of the domain to register key information, which is available and searchable on the Internet. This information will contain:
Answer: B, Page16

A. Type of operating system.
B. Contact information such as phone numbers.
C. IP address of the E-mail server
D. Name of the Internet Service Provider

The purpose of NetBios is similar to:
Answer: A, Page19

A. Purpose of the Port numbers, namely, to identify services running on a system.
B. NetBEUI
C. SMB
D. All of the above.

NBTSTAT utility will list:
Answer: A, Page19

A. NetBios names and services currently in use on a system.
B. NetBios protocol usage statistics
C. IP address of the Interface used.
D. Amount of NetBEUI traffic.

SNMP can be used to change:
Answer: C, Page22

A. Password on NT servers.
B. MAC address
C. IP addresses
D. All of the above.

Firewall is usually not a single piece of hardware. Which of below can be considered a component of the firewall?
Answer: D, Page25

A. Proxy server
B. NAT servers
C. Routers
D. All of the above.

Which of the statement about an Automated Protocol Analyzer is true:
Answer: A, Page27

A. It is a packet sniffer, which can detect attacks.
B. It is always easy to deploy and maintain.
C. Analysis on the packets usually occurs at periodic intervals.

D. All of the above.

From a security perspective which is not recommended.
Answer: A, Page29

A. Implementing WINS server in DMZ.
B. Implementing dual DNS servers.
C. Having a DNS entry for a honey pot server.
D. Having a DNS entry for non-existent host.

Which of this is true ?
Answer: D Page30

A. One should not publish or reveal information to the public unless there is a valid reason to do so.
B. A company website should be periodically reviewed to ensure that it does not promiscuously reveal information which only needs to be available to employees.
C. Private search engines are especially dangerous.
D. All of above.

A hacker who has targeted an administrator for Social Engineering can search that administrator's name and e-mail address in :
Answer: A Page31

A. Usenet
B. His own e-mail inbox.
C. Internet search engine
D. Yellow Pages

A hacker who has targeted an administrator for Social Engineering can search that administrator's name and e-mail address in:
Answer: A Page31

A. Usenet
B. His own e-mail inbox.
C. Internet search engine
D. Yellow Pages

Hackers will discover the phone number of RAS servers by :
Answer: D Page32

A. Searching publicly available information.
B. Social Engineering
C. Wardialers.
D. All of above

One of the ways to detect wardialing is:
Answer: A Page 33

A. To have honeypot RAS.
B. See if your phone rings at home.
C. To ask an operator.
D. To let local police know that you want to be notified when some one is wardialing.

A "Personal Firewall" is
Answer: B Page34

A. A Firewall, which is licensed to an individual.
B. A Firewall, which is runs only on one computer.
C. A Firewall, which is monitoring all computers in one room.
D. A Firewall, which is monitoring computers on one network segment.

Purpose of a DOS attack may be
Answer: D Page 37

A. To just annoy administrators.
B. To cause financial harm.
C. To activate a Trojan Horse.
D. All of the above.

You should suspect an DOS attack on an Internet-accessible server when:
Answer: D Page 39

A. The server suddenly continuously runs at greater than 95 % CPU utilization.
B. Services unexpectedly fail.
C. Bandwidth usage is continuously and abnormally high.
D. All of the above.

It is not unusual for incoming DOS packets to have one or more of the following characteristics:
Answer: D Page 39

A. Packets violate RFC standards.
B. Spoofed source IP address.
C. Fragmented packets whose completing packets never arrive.
D. All of the above.

Which is not an DOS attack.
Answer: C Page 40

A. Ping of Death
B. SYN flood
C. Teletubbies attack
D. WinNuke

When applying Service Packs for NT, which of these is not true:
Answer: A Page 41

A. Service Pack does not contain new utilities or features important to security.
B. After deploying a firewall, installing the latest Service Pack is perhaps the most effective way of defending against DOS attack.
C. Service Packs come in two versions, One for export with weaker encryption and the other for U.S.A. and Canada with stronger encryption.
D. Service Packs must be reinstalled when configuration of the server is change.

Disabling non-essential services will reduces potential exposure to attack. Secondary benefit to this is:
Answer: B Page 43

A. Password can be harder to guess.
B. Improvement in performance.
C. Reduces chance of buffer-overflow.
D. Protocol analyzer can be installed.

Exactly what service can be disabled on a particular server can be determined by:
Answer: B Page 44

A. Using a service monitor utility available from the resource kit.
B. Only by trial and error.
C. Watching the performance monitor.
D. Using the "SERVMON" command.

OS/2 or POSIX application support can be removed through:
Answer: A Page 45

A. Registry changes
B. Control Panel
C. Service Patch installation
D. Hot-fix installation

When installing latest patches and hot fixes, which of below is true:
Answer: D Page 47

A. Patches and hot fixes can be installed in any order, as long as the server is rebooted with every install.
B. Patches must always be applied before hot fixes.
C. Hot fixes must always be applied before patches.
D. Patches and hot fixes must be installed in certain order.

Windows NT may crash, if:
Answer: B Page 50

A. Display monitor is turned off.
B. Windows NT runs out of free hard drive space for temporary and paging files
C. Administrator types in the wrong password more than 10 times.
D. RAID device report a recoverable error in one of the hard drive.

Performance of the Windows NT can be improved, if:
Answer: B Page 50

A. The Keyboard is not attached.
B. Multiple Paging files are located on physically separate drives.
C. More than one drive is attached.
D. Services are allocated its own RAM space.

Which of below does not help prevent the Blue Screen of Death:
Answer: A Page 51

A. Have the OS and service use the same partition.
B. Have generous amount of physical RAM.
C. Placing a paging file sized at RAM+11MB in at least one other partition.
D. Using bus-mastering hard drive controllers, instead of Programmed I/O controllers.

You can use _____command to help you determine if SYN flooded.
Answer: D Page 53

A. traceroute
B. intstat
C. ipstats
D. netstat

The number of times Windows NT can be installed on a single hard drive is limited only by:
Answer: A Page 56

A. The free space on that drive
B. The number of partition on that drive.
C. Amount of RAM available at boot.
D. The number of logical drives.

Emergency Repair Disk can be used to :
Answer: C Page 57

A. Re- mount a drive mounted over the network.
B. Repair file and folder permission.
C. Replace and inspect the boot sector.
D. Replace the most recent SAM.

What are the four disks that should be created to boot the computer?
Answer: A Page 58

A. ERD, Emergency boot disk, Setup disks, and MS-DOS boot disk.
B. ERD, Emergency boot disk, resource kit, and MS-DOS boot disk.
C. ERD, Emergency boot disk, Setup disks, and separate SAM backup.
D. ERD, separate SAM backup. Setup disks, and MS-DOS boot disk.

What command or procedure is used to create an ERD?
Answer: C Page 58

A. mkerd
B. From the control panel.
C. rdisk
D. crerd

ERD (Emergency Repair Disk) contains:
Answer: A Page 59

A. SAM of originally created administrator account and guest account.
B. SAM of current administrator account and guest account.
C. Most current SAM.
D. SAM of current administrator account only.

"/s" option to create ERD will
Answer: D Page 59

A. SAM will not be copied.
B. File permissions will be copied.
C. ERD will be made bootable.
D. Current SAM will be copied.

To use the ERD, you must :
Answer: B Page 59

A. "R" key must be pressed down before booting starts.
B. Windows NT must first be booted up with the three Windows setup disks.

C. Windows NT must be booted up from the ERD.
D. Boot up normally and then insert ERD.

Binary drive image are usually used to:
Answer: B Page 61

A. Check the integrity of the files on the hard drive using hash.
B. Restore the hard drive quickly in case of a failure.
C. Create RAID devices.
D. Restore installation of Service Packs.

To analyze DOS attacks protocol analyzer can be used. Windows NT comes with protocol analyzer called:
Answer: C Page 63

A. Network Analyzer
B. Network Sniffer
C. Network Monitor
D. NetXray

Performance Monitor can be used to:
Answer: C Page 65

A. Graph and log performance data.
B. Generate alerts when counters exceed configurable thresholds.
C. Execute custom commands when counters exceed configurable thresholds.
D. All of the above.

If a DOS attack can cause a Blue Screen of Death then crashdump files can be enabled for analysis. Crashdump file contains:
Answer: A Page 68

A. A copy of the entire contents of RAM at the time a BSOD occurs.
B. More detailed error messages than contained in the audit logs.
C. Last 500KB of packets which arrived before BSOD occurred.
D. All of the above.

To steal an NT account, an attacker requires:
Answer: B Page 72

A. Username and password.
B. Username, password, and domain name.
C. Username, password and hash.
D. Username, password, and IP address.

Windows NT server has two built-in account, guest and administrator, they can:
Answer: A Page 73

A. Be renamed, but not deleted.
B. Only be left alone, as is.
C. Be deleted and renamed, but administrator can not be deleted.
D. None of the above.

Administrator account is most attractive to a hacker because:
Answer: C Page 73

A. It cannot be locked out.

B. It is the most powerful account.
C. Both A and B.
D. None of the above.

When Windows NT users log on, transmission of:
Answer: C page 74

A. All authentications are done using hash.
B. All authentications are encrypted.
C. Only username and domain name is clear text.
D. Only domain name is clear text.

Microsoft Security Configuration Editor (SCE) can be used to:
Answer: D Page 76

A. Define a template of security configuration settings.
B. Compare the local machine's settings against a template.
C. Configure the local machine's settings to match a template.
D. All of the above.

SCE can also be:
Answer: C Page 78

A. Used to configure the setting over the network.
B. Used to execute SCE tasks from the command line using the SECEDIT.EXE utility.
C. Used to audit file permissions.
D. Used to Audit Share permissions.

"Null Sessions" is:
Answer: C Page 80

A. Same as anonymous user account for IIS (IUSR_*computername*).
B. Automatic Guest logons when one's username is completely unknown.
C. When null character is entered for both username and password.
D. "Null" is entered for both username and password.

When registry change has been made to block username listing to a null session,:
Answer: A Page 86

A. A user may not be able to list users and groups from trusted domain, if multiple domains are used.
B. A user may not be able to list users and groups at all.
C. A user may not be able to list users and groups at all, unless when he is on PDC or BDC.
D. All of the above.

An excellent way to get a very strong password is to:
Answer: C Page 87

A. Use combination of your personal data such as birthday, SSN, and names.
B. Use passwords creation programs to make password consisting of alphabets.
C. Include extended ASCII characters
D. Easy to remember words, but spelled backwards.

Service Pack 3 or later will allow use of PASSPROP.EXE. This utility will enable lock out for administrator account. This will lock out administrator account:
Answer: D Page 88

A. Completely, only to allow access with another password created before hand.
B. Only from telnet service.
C. For predetermined time.
D. Only for over-the-network authentications.

Guest account is special in that remote user will be automatically logged on as Guest if:
Answer: D Page 90

A. The guest account is enabled.
B. The password for the Guest account is blank.
C. The supplied username does not exist in any accounts database to which the server has access.
D. All of the above.

Shared accounts should generally be avoided. Exception may be, if the rights and permissions of a shared account is limited and when special-purpose users who occupy a functional role in an organization and their ranks frequently turn over. The account such as this is referred to as:
Answer: A page 92

A. Role account
B. Specific account
C. Duty account
D. Working account

When no domain name is provided during the logon, as with older and/or non-Microsoft clients, then supplied username is matched against:
Answer: D Page 97

A. Local database then databases of trusted domains then local domain database.
B. Local domain database then local database then databases of trusted domains.
C. Databases of trusted domains then local database then local domain database.
D. Local database then local domain database then databases of trusted domains.

All process on Windows NT:
Answer: A Page 98

A. Must run under the context of some account.
B. Run under the context of some account, but network related process run under null account.
C. Run with full access privileges, but network related process run under null account.
D. All run under local account.

User manger can enforce:
Answer C Page 101

A. Minimum password length and complex passwords.
B. Only complex passwords.
C. Minimum password lengths, but not complex passwords.
D. None of the above.

User manager can be used to set account and password policies:
Answer: B Page 104

A. This policy applies to all but administrator account.
B. This policy applies to all user accounts.
C. This policy applies to all but administrator and guest account.
D. This policy applies to those specified.

Password uniqueness will:
Answer: B Page 105

A. Ensure that each user account has a unique password.
B. Ensure that a user account does not reuse previously used passwords. (Up to 24 previous passwords.)
C. Ensure that user account does not reuse the most recent password.
D. None of the above.

SAM can be encrypted using:
Answer: A Page 109

A. syskey.exe
B. encsam.exe
C. option in the registry.
D. On Windows NT in a single domain.

If SAM is encrypted the system key cn be made available to Windows NT via:
Answer: D Page 110

A. A copy in hard drive.
B. A copy in a floppy disk.
C. Manual entry at boot up.
D. All of the above.

If a system key is lost when SAM is encrypted:
Answer: C Page 110

A. Use a Windows Install CD to recover.
B. Use an ERD made after SAM encryption to recover.
C. Use a backup or ERD made prior to SAM encryption to recover.
D. Login as an administrator and recover through the provided utility.

Windows NT support multiple authentication methods:
Answer: D Page 112

A. LanManager
B. Windows NT
C. NTLMv2
D. All of the above.

Which of below is true about NTLMv1 (LanManger):
Answer B page 113

A. It is case sensitive
B. Passwords longer than 14 characters are truncated.
C. Two identical passwords will have different hash through use of salts.
D. 14 byte passwords are used to encrypt the magic string as a whole.

Which of below about NTLMv2 support is untrue:
Answer: A Page 117

A. Even when NTLMv2 is enabled on a server, a backwards compatibility with all other authentication methods can be maintained through LMCompatibilitylevel setting, except Windows NT authentication.
B. Even when NTLMv2 is enabled on a server, a backwards compatibility with all other authentication methods can be maintained through LMCompatibilitylevel setting.
C. Windows 95 can support NTLMv2.
D. Windows 95 can support NTLMv2.

NetLogon is channels used for:
Answer: C Page 118

A. Process and service log on.
B. Logon for services initiated on local servers. (i.e. telnet)
C. Pass-through authentication and accounts synchronization.
D. For all log on initiated through the network and or modems.

Social engineering is:
Answer A Page 121

A. Art of tricking users into revealing information.
B. Using social security numbers to obtain passwords.
C. Using "Social" process on a PDC to sniff passwords.
D. Using "Social" utility tool to guess and/or sniff passwords.

Reverse social engineering involves:
Answer: D Page 125

A. Making the hacker aware that he is available to help.
B. Causing or waiting for problems to occur.
C. Extracting information by assisting targets.
D. All of the above.

Statistically, the majority of one's intruders are:
Answer: B Page 131

A. From the Internet.
B. Legitimate internal users.
C. From remote access services.
D. Consultants hired at that company.

Best practice for account creation are:
Answer: C Page 134

A. To manually customize each according to the business needs imposed.
B. To manually customize groups, and assign permissions to global groups as needed.
C. To use templates which gives standardized groups for accounts or use batch scripts with the same standards.
D. Create global groups and assign standard rights to them and create accounts that belongs to local accounts.

It is recommended to use:
Answer: B Page 136

A. Combination of FAT and NTFS file system.
B. NTFS only.

C. FAT only.
D. Any files systems.

Combination of NTFS and share permissions is:
Answer: C Page 137

A. More lenient of the NTFS or share permission.
B. Always NTFS
C. More restrictive of the NTFS or share permission.
D. Always share permission.

NTFS permission is:
Answer: B Page 137

A. Most restrictive of all permissions assigned to that user and his groups.
B. Combined sum total of all permissions assigned to that user and his groups.
C. The permission of his group, unless the user is does not have any access.
D. The permission of the user, unless his group does not have any access.

Share permission is:
Answer: A Page 138

A. Cumulative and does not apply to console users.
B. Most restrictive of the user and group permission and applies to console users.
C. Most restrictive of the user and group permission and does not applies to console users.
D. None of the above.

Leslie is a member of three groups: SALES, ADMINS and MANGERS. Her permissions are as below. Her final effective permission is:
Answer: C Page 138

	NTFS Permissions	Share Permissions
Sales	Change	Read
Admins	Change	Full Control
Managers	Read	Change

A. Read
B. Full Control
C. Change
D. No access

On previous question, if the share permission on sales group was "No access", her final effective permission is:
Answer: D Page 139

A. Read
B. Full Control
C. Change
D. No access

Default NTFS permission is:
Answer: D page 140

A. No access

B. Change
C. Read
D. Full access

Everyone group includes:
Answer: B Page 142

A. Only authenticated users.
B. Users from untrusted domains, users who have no Windows NT domain, anonymous Internet users and null session users.
C. Only users from local area network.
D. Only users logged on locally.

Named pipe is:
Answer: D Page 157

A. Used to pipe (or redirect) command output to another command.
B. A special IP packet used to communicate between process on different machines.
C. A special program that names all the Windows NT pipes being used.
D. A file system in the memory address space which desire to communicate with each other.

On RAS CHAPv2 can be used after Service Pack 4. CHAPv2 has an advantage in that
Answer: E page 162

A. Use of the NT method of response during challenge/response authentication.
B. Stronger encryption keys.
C. Different encryption keys for the send and receive paths.
D. Mutual authentication of client and server.
E. All of the above.
F. Just A and C

When a user on the LAN remains connected even after his or her logon hours have expired:
Answer: A Page 163

A. Session will stay connected.
B. Session will be disconnected when time expires.
C. Session will be connected until screen saver is turned on.
D. Window box will come up for a soft shutdown.

SMB is used to:
Answer: B Page 166

A. Send message broadcasts to communicate between multiple processes.
B. Access shared folders, printers, and named pipes.
C. Send memory broadcasts.
D. Send monitor broadcasts to collect stat data.

"Mange Auditing and Security Logs" rights in user manager gives:
Answer: E Page 186

A. Configure ASCL on folders, files, registry keys, and printers.
B. View and clear the Security log.
C. Give ""Mange Auditing and Security Logs" rights to other accounts.
D. All of the above
E. Just A and B

In most cases, recommended setting security in regards to NT logs are:
Answer: C page 188

A. Use wrapping option to overwrite events as needed.
B. Use "Do not Overwrite events"
C. Use option o "Overwrite Events Older than X days".
D. None of the above.

Windows 9x and Windows NT computer automatically attempt to download System Policy settings from the domain controller, which authenticated their logon. This is done by storing System Policy from a single file named:
Answer: B page 210

A. syspol.ini
B. ntconfig.pol
C. syspol.txt
D. config.ini

When domain controller is not available:
Answer: C Page 221

A. Windows will refuse any logon.
B. Windows will log you on if you were the last one to logon to that machine.
C. Windows will log you on if you were one of the last ten to logon to that machine.
D. Windows will ask for an local administrator password.

You can look for Protocol Analyzers on the network by:
Answer: D Page 226

A. Use a utility in the Network Monitor itself to discover other network monitor.
B. Use EMS to look for popular Protocol Analyzers' file name.
C. Use utility such as "Antisniff"
D. All of the above.
E. Just B and C

One way to minimize the threat of protocol analyzers is to:
Answer: B Page 227

A. Use routers to segment networks.
B. Use switches.
C. Configure all machines to only transmit packets to destination.
D. All of the above.

You can scan for viruses at:
Answer: D Page 231

A. Tape backup procedures.
B. E-mail gateways.
C. Firewalls and proxy servers
D. All of the above.

In Windows NT, printer drivers run:
Answer: A Page 233

A. In kernel mode.
B. As a user that is currently logged on.

C. Same as services.
D. None of the above.

When Schedule service launches a job, that job:
Answer: B Page 234

A. As the user that scheduled the job.
B. As a Systems account.
C. Same as services.
D. None of the above.

Default setting on Windows NT is to:
Answer: A Page 240

A. Have two names for every folder and file, a long file name and short name.
B. Use only a long file name.
C. Use only a short name.

Which of below is not recommended:
Answer: B Page 247

A. Computer cases should be cabled to their cabinets or racks.
B. Install automatic overhead sprinklers.
C. Computer cases should be elevated off the floor.
D. Install UPS systems.

The Audit Policy defined in User Manger includes the option to audit Use of User Rights. However, even when this option is enabled, the following user rights are not audited:
Answer: H Page 252

A. Backup Files and Directories.
B. Restore Files and Directories.
C. Bypass Traverse Checking
D. Debug programs.
E. Create A Token Object
F. Replace A Process Level Token.
G. Generate Security Audits.
H. All of the above.
I. Only A, B, C, and G

Local accounts:
Answer: B Page 256

A. Can only be used to log onto the computer where it was created.
B. Can only be used to log onto the computer where it was created, except if it was created on the domain controller which is replicated to other domain controllers.
C. Can log onto any computer on the domain.

SECTION 2

From *Active Directory for Windows 2000 in a Nutshell*,

(And supplemental handout sheets, Indicated by "S" before page numbers)

30 questions

Active Directory replaces:
Answer: A Page 9

A. SAM database
B. DNS service
C. NTFS permissions
D. Share permissions

Windows 2000 is first installed without Active Directory, and then it is installed when the machine is:
Answer: C Page 12

A. It participates in a domain.
B. When it boots up the second time.
C. When it is promoted to become a domain controller.
D. None of the above.

Windows 2000 can run in either "Mixed mode" or "Native mode". Native mode is available only when:
Answer B: Page 16

A. All servers and clients are patched for 2000 compatibility.
B. All domain controllers are Win 2000 and all else are patched for Win 2000 compatibility.
C. All servers and clients are Win 2000.
D. None of the above.

After switching to native mode:
Answer: B Page 18

A. Win 2000 does not use SMB, so it does not use Netbios by default.
B. It is possible to turn off Netbios over TCP/IP. But default will still use it.
C. Netbios over TCP/IP is turned off by default.
D. None of the above.

When Active Directory (AD) database is modified on one server, then:
Answer: D Page: 23

A. All other domain controllers will compare the AD database with their own and replace it with the correct AD database.
B. It will be replaced with the primary AD database copy, unless it is the primary copy.
C. It will stay on that server until manual command to replicate on all other servers is executed.
D. The changes will automatically replicated to all other DCs.

Windows 2000, including Active Directory:
Answer: B page 29

A. Can be managed entirely only through GUI.
B. Can be managed entirely through scripts.
C. Is controlled by Bill Gates through the network.
D. Can be managed entirely through scripts, which must be written by windows 2000 script language.

"Site" is a concept of:
Answer: B Page 31

A. Any IP reachable sets of machines.
B. Set of well-connected computers on IP subnets.
C. Any IP reachable sets of machines on a network segment.
D. None of the above.

Replication between sites is manually configured; this can be done over:
Answer: B Page 32

A. RPC-over-IP
B. RPC-over-IP or SMTP
C. SMTP
D. SNMP

Global Catalog servers contains:
Answer: A Page 35

A. The most often needed data from the AD database of all domains in the enterprise.
B. The most often needed data from the AD database of its domain.
C. Backup copy of the AD database.
D. Full copy of the entire AD database in all domains in the enterprise.

FSMO stands for:
Answer: D Page 37

A. Full single message operation
B. Finite source master operation
C. Flexible source main operation
D. Flexible single master operation

Schema in the Active Directory database:
Answer: B Page 40

A. Only defines the structure in AD
B. Defines the structure and data types of the objects and properties in AD.
C. Is a utility to help you plan out the structure of the AD.
D. Is a data attribute in a AD which controls how the database is used.

Major "Naming contexts" in AD database is called.
Answer: D Page 43

A. Domain naming context
B. Schema naming context
C. Configuration naming context
D. All of the above.

Domains in Windows 2000:
Answer: D Page 48

A. Can be nested.
B. Can be named following DNS standards using dotted notations.
C. And its sub-domains all have two-way transitive trusts.
D. All of the above.

Universal group in Windows 2000 is:
Answer: A Page 56

A. Enterprise-wide groups, which can contain users and global groups from any domain in the forest, except local groups.
B. Enterprise-wide groups, which can contain users and groups from any domain in the forest.
C. Enterprise-wide groups, which contain user from local groups only.
D. Enterprise-wide groups, which contain other global groups.

_____in the AD database can have it's own separate sets of permissions.
Answer: B Page 65

A. Only the chosen objects.
B. Every property of every object.
C. Only the chosen property of every object.
D. Only the chosen group of objects.

Recommended methods of reducing the complexity of the AD permissions are:
Answer: D Page 72

A. Using inheritance as much as possible.
B. Leveraging organizational units to control inheritance.
C. Use generic permissions instead of specific.
D. All of the above.

In windows 2000 it is possible to give user a degree of administrative powers because:
Answer: B Page 77

A. It has specific administrative groups in the user manager utility.
B. It is possible to delegate administrative power and precisely limit the scope of this power.
C. NTFS permissions are very granular.
D. All of the above.

Group policy can be applied to:
Answer: D Page 83

A. Sites
B. Domains
C. Organizational units.
D. All of the above.
E. Just A and B

Group policy is applied when:
Answer: D Page 83

A. Computer boots up.
B. User logs on
C. Scheduled intervals.
D. All of the above.
E. Just A and B

Group Policy Objects are applied in the following order:
Answer: C Page 89

A. Local GPO, Site GPO, NT4.0 policy, Domain GPS, and then organizational unit GPO.

B. Site GPO, NT4.0 policy, Local GPO, Domain GPS, and then organizational unit GPO.
C. NT4.0 policy, Local GPO, Site GPO, Domain GPS, and then organizational unit GPO.
D. Local GPO, Site GPO, Domain GPS, NT4.0 policy and then organizational unit GPO.

User must have at least _____ in order to have a GPO applied to his or her desktop.
Answer: C Page 95

A. Create Group Policy permissions in order to have a GPO applied to his or her desktop.
B. Read Group Policy permissions in order to have a GPO applied to his or her desktop.
C. Read and Apply Group Policy permissions in order to have a GPO applied to his or her desktop.
D. Apply Group Policy permissions in order to have a GPO applied to his or her desktop.

To create or edit a GPO, a user requires at least:
Answer: B Page 96

A. Read permissions on that GPO.
B. Read and Write permissions on that GPO.
C. Write permissions on that GPO.
D. Create permissions on that GPO.

Group Policy can be used to install, update repair and remove applications. However, these applications:
Answer: C Page 98

A. Must exist on the Windows OS with Active DNS with native support.
B. Must be managed only locally.
C. Must support the new Microsoft Installer Service by including a special installation script with the .MSI filename extension.
D. Must be located on the Domain Controller.

Group Policy can be used to launch scripts on computers when:
Answer: E Page 101

A. Computer starts up.
B. Computer shuts down.
C. User logs on.
D. User logs off.
E. All of the above.
F. Only A and B.
G. Only C and D.

Windows 2000 domain controllers and clients:
Answer: B Page S1

A. Does not need DNS.
B. Require DNS.
C. Need DNS to execute certain advanced features.
D. Need DNS or Active Directory.

DNS zone data can be stored:
Answer: A Page S4

A. Either in text files or in Active Directory.
B. In a text file.
C. In Active Directory.
D. In a special encrypted DNS zone file.

SRV records identify:
Answer: B Page S7

A. IP address of the servers available.
B. Available services, the protocol available, port numbers, FQDN of the system, and load-balancing information.
C. Services and passwords to manage them.
D. Servers' passwords to manage them.

When DNS record are stored in AD:
Answer: A Page S9

A. A separate access control list of permissions can be applied to each record.
B. An access control list of permissions can be applied to the whole record.
C. A separate access control list of permissions can be applied according to each server's record.
D. A separate access control list of permissions can be applied according to each domain's record.

Cache poisoning is:
Answer: C page S18

A. Memory cache of DNS server is manipulated by an executable.
B. Disk Cache of DNS server is manipulated by an executable.
C. A type of attack in which incorrect or a huge number of bogus query responses are sent to a DNS server.
D. A Cache record of a DNS is replaced with another file.

DNSCMD.EXE utility in the resource kit can:
Answer: E Page S20

A. Be used to list/create/delete resource records.
B. Clear DNS cache.
C. Be used to set IP addresses for recursive queries.
D. Create/delete zones
E. All of the above.

SECTION 3
From *IIS for Windows 2000*, 30 questions

An attacker may use different forms of reconnaissance to gather information about the servers , which of below is not true:
Answer: B Page 11,12,

A. HTTP uses port 80 and FTP uses ports 21 and 20.
B. Hidden and non-public servers cannot be located if they are not advertised.
C. Attacker can determine that Webserver is running IIS – as opposed to Lotus Domino or Apache.
D. URL scanner can be used to identify well-known CGI and ISAPI scripts.

It is dangerous to allow clients to see the code in CGI and ASP files because:
Answer: D Page 18

A. This permits the client to analyze the script for exploitable security holes.
B. Scripts may contain the names or IP addresses of other servers.
C. Some scripts contain user names and passwords.
D. All of the above.

A hacker will be able to run arbitrary commands on the webserver:
Answer: D Page 27

A. If a folder is given both the Write and execute permission, then a file can be downloaded and executed by accessing it on the browser using http://www.domain.com/program.exe.
B. If script engines are placed in the same folder as the scripts, then that engine can be accessed directly with command sent directly to them.
C. If the user is given execute right in any folder, the local executable can be executed by http://www.domain.com/~yourcomputer.domain.com/program.exe.
D. A and B

HTTP and FTP transmit data in:
Answer: A Page 28

A. Clear text.
B. Encrypted form when certificate is installed on the server.
C. Clear text with hash to ensure integrity.
D. Always encrypted.

HTTP is a:
Answer: B Page 31

A. Statefull connection.
B. Stateless connection.
C. Secure connection.
D. None of the above.

To maintain state in web based application,
Answer: D Page 31

A. Cookie can be used.
B. A “Folder” in the URL path may be used as an ID number.
C. Forms with “Hidden” values may be used as an ID number.
D. All of the above.

An advantage of moving the root folder off the IIS server is that:
Answer: C Page 49

A. Is that hacker will have a harder time accessing those files in that folder.
B. Is that it saves hard disk space on the IIS server itself.
C. IIS box becomes generic to accommodate quick restoration.
D. All of the above.

IIS should not be installed:
Answer: A Page 51

A. On a domain controller.
B. On any computer participating in the domain.
C. On any stand-alone servers.
D. All of the above.

When domain controller IIS server is in the DMZ:
Answer: A Page 51

A. Port 138 and 139 must be opened between DMZ and internal networks.
B. Port 21 and 20 must be opened between DMZ and internal networks.
C. Port 80 and 443 must be opened between DMZ and internal networks.
D. All of the above.

In general, when installing IIS,
Answer: B Page 59

A. Install all optional components of the Option Pack you can find.
B. Do not install any of the components of the Option Pack unless it is specifically needed.
C. It should be done before all service packs are installed.
D. All of the above.

To hide an IP address of the server when serving an static page:
Answer: D Page 63

A. An option should be turned on in the registry.
B. Rename all static webpages with the .asp extension.
C. Disable "GET" command on the server.
D. Just A and B.

If multiple authentication methods are used,
Answer: B Page 68

A. Authentication must be retried at random until it succeeds.
B. IIS will inform the browser which methods are available.
C. IIS automatically re-initiate an authentication with the method proffered.
D. Depends up on the options specified in the authentication option sent by the browser.

When anonymous users access web pages or FTP files, the operating system will represent the users internally as:
Answer: A Page 71

A. IIS anonymous account
B. Null user
C. Non-authenticated users

D. Depends up on the options.

When using Basic authentication, in a default setting, user must have this right:
Answer: C page 76

A. Access this computer from the network.
B. Log on as a batch file.
C. Logon locally.
D. Logon as anonymous

Digest authentication can be used on IIS 5.0 that is a member of a Windows 2000 domain. This authentication method will use:
Answer: B Page 78

A. Encrypt the authentication session with SSL.
B. MD5 to hash the username, password, domain-realm, server's random challenge, the HTTP method use, and the requested URL.
C. MD5 to hash the username and password.
D. MD5 to hash the password.

Fortezza is a:
Answer: D Page 88

A. Type of a hash algorithm.
B. Type of a file integrity method.
C. Type of encryption algorithm.
D. Type of Certificate authentication and SSL encryption technology.

When multiple all authentication methods are enabled for a single resource:
Answer: A Page 89

A. Certificate authentication takes precedence over all other authentication method.
B. Basic authentication is requested first for backward compatibility.
C. Digest authentication will be requested first.
D. None of the above.

"What if Tool" can be utilized to:
Answer: B Page 92

A. Try out actual authentication process to see if the authentication works.
B. Allows you to quickly see the web application and authentication ramifications of using any combination of the Browser, client OS, scenario, web server, and authentication method.
C. Give you the list of resources accessible using certain username and password.
D. All of the above.

To enable certificate authentication:
Answer: D Page 97

A. A digital certificate must be installed.
B. A personal digital certificate must be installed in the browsers.
C. Both server and browsers must have the certificate of the certifying authorities which both sides trust and which issued the certificates to the server and the browser.
D. All of the above.

To control access via client certificates, authentication can be:
Answer: E Page 104

A. Via the Directory Service.
B. Many to one
C. One to one
D. Any trusted certificate accepted.
E. All of the above.
F. Just A, B and C.

Which of below is untrue regarding the SSL:
Answer: C page 110

A. SSL will encrypt data transmitted between webserver and browser.
B. SSL will verify that data has not been altered.
C. FTP is supported with SSL.
D. SSL will optionally verify the identity of the client to the server.

In addition to NTFS permission:
Answer: B Page 117

A. No permission can be assigned to an IIS service user.
B. IIS permission can be assigned to an IIS service user.
C. IIS permission and HTML permission can be assigned to an IIS service user.
D. Just B and C.

Application permission in the pull-down menus are:
Answer: D Page 118

A. None
B. Scripts only
C. Scripts and executables.
D. All of the above.
E. Just B and C.

When scripts and executables are run on the IIS, it is run with:
Answer: A Page 121

A. System level privileges.
B. Rights that user logged on with.
C. Rights that IIS service has.
D. Anonymous

When NTFS and other IIS enabled permissions are combined:
Answer: B Page 124

A. It is the more lenient of the two.
B. It is the more restrictive of the two.
C. It is the cumulative of the two.
D. None of the above.

Throttling IIS can be done via:
Answer: D page 127

A. Limiting number of connections.
B. Limiting bandwidth utilization.
C. Limiting CPU usage.
D. All of the above.

Web Distributed Access and Development (WebDAV) will allow:
Answer: B Page 135

A. Installation of IIS over the network.
B. Allows authors to create, edit, and mange files in folders on remote HTTP servers.
C. Remote configuration of IIS.
D. Remote shutdown and execution of IIS.

When IIS is acting as an application server, application runs on:
Answer: B Page 142

A. The main memory space with the Operating System.
B. Runs on separate memory pool within the single instance of DLLHost.exe.
C. Runs on separate memory pool allocated on the client.
D. All of the above.

Unregistering OLE controls and COM components will:
Answer: A Page 150

A. Make it unavailable to the web application.
B. Make it unavailable to the web application without knowing its full path.
C. Make it unavailable to the web application, if it is located on a folder other than the root folder.
D. Only B and C.

Single IIS box can:
Answer: B page 163

A. Can only host one website.
B. Can host multiple website.
C. Can host multiple website, as long as the are in the same domain.

Last Updated: May 25th, 2017

Upcoming Training

SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 06, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**