Global Information Assurance Certification Paper

Shawn Lukaschuk
GCNT

90 Questions from Day 1,2,3

1. Typically, the first phase of a long-term attack against a network is:

Installing a root kit
Reconnaissance
Acquiring a user account

Page 12 Answer B

2. A form of reconnaissance that is possible to detect is:

Public website research
Internic research
Port scanning

Page 16 and 17. Answer C.

3. The following information can not be found in the searchable database at http://www.network.solutions.com:

MX Records for US Military mail servers
Contact information for personnel of the organization who registered a domain
IP addresses of DNS servers which hold the records for one's domain

Page 17 Answer A

4. Netbios:

Is the plural of NetBEUI
Requires TCP/IP
is a high level protocol with a purpose similar to port numbers

Page 19 Answer C

5. SNMP

security is weak
stands for Sans Network Monitorring Protocol
is ideal for unattended batch files

page 23 Answer A

6. Modems on user's desktops represent a potential risk because:

they are firewalled from the network
they automatically circumvent all other host authentication procedures
Are easily discoverable by hackers with wardialers

Page 23 Answer C

7. The information security term for the devious art of tricking users and administrators is:

finangling
Brute force attack
Social Engineering

Page 23 Answer C

8. Firewalls can not typically filter traffic based on:

Source address
Community standards
Direction of travel

Page 26 Answer B

9. DNS servers that are publicly accessible should generally not include records for:

Web servers with E-commerce offerings
A security administrator's workstation
NNTP news servers

Page 28 Answer B

10. Methods of defending against social engineering include:

Holding half day seminars for your users on the topic
Lock all outdoor garbage receptacles
Use strong passwords that include non alphabetic characters

Page 31 Answer A

11. A "Personal" firewall:

is generally more expensive than a traditional firewall
is more important on a dialup internet connection than a cable or DSL connection.
Protects the computer on which it is installed.

Page 34 Answer C

11. Hackers crash systems for several reasons but usually not to:

Force administrators to restart the server and activate a Trojan Horse
Deploy a network firewall
Annoy system administrators.

Page 37 Answer B

12. A symptom of a denial of service attack may be:

Poor system documentation
100% CPU utilization
Positive customer feedback

Page 39 Answer B

13. A service pack from Microsoft:

Is a collection of upgrades and patches.
Should be installed on all production servers immediately.
Is often all the security that is required.

Page 41 Answer A

14. A service pack for Microsoft Windows NT:

Should only be installed once
Should be de-installed before reinstalling
Should be reinstalled whenever the configuration of a server changes

Page 42 Answer C

15. Installing nonessential services and options in NT:

Is often a source of time savings for end users.
Increases one's potential exposure to attack
Allows increased protection of the registry.

Page 43 Answer B

16. An example of a service that is typically non essential and should be removed from all servers is the:

Internet Information Server
Server service
POSIX subsystem

Page 44 Answer C

17. Patches and hotfixes should be tested on a non-production server before deploying on live systems because:

That's what Microsoft pays you for.
They are not as thoroughly tested as service packs
They are generally not compatible with recent NT revisions.

Page 47 Answer B

18. Often, NT patches and hotfixes:

Are included in later ones.
Should be installed in the order described in the NT help (F1)
Are not required to be installed in any particular order.

Page 47 Answer A

19. NT Systems with a low amount of free disk space:

May be vulnerable to a form of DOS.
Are generally safe from most modern trojans
generally perform better but are less secure

Page 50 Answer A

20. Enforcing hard disk space quotas on users via a third party product:

Allows users to more tightly control who has access to their shared folders.
Can save the administrator time during account creation
Is a strategy to combat denial of service attacks

Page 50-51 Answer C

21. Denial of service attacks:

Are not always preventable and measures should be taken to ensure a speedy recovery
Are preventable with vigilant monitoring of security websites and newsgroups and appropriate patches.
Are available for download at ftp://ftp.microsoft.com/pub/nt40/USA_

Page 55 Answer A

22. One strategy for fast recovery of NT servers is:

Large amounts of free disk space and physical RAM to prevent a DOS attack from slowing the system
Multiple installations of NT to allow the transfer of files when an installation is damaged.
A well tested backup strategy with storage of backup tapes at a branch office

Page 56 Answer B

23. The most important reason to protect ERDs is:

if damaged, the server may not be recoverable
because the SAM database is stored upon it
important financial data is often stored on the registry copy

Page 60 Answer B

24. Protecting the SAM on an ERD is important mainly because:

the user passwords are stored in plaintext
the encryption algorithm used to protect user passwords is weak and easily reversible
measures such as account lockout no longer protect provide protection from hackers determining passwords with automated tools.

Page 60 Answer C

25. To create Windows NT Setup disks:

Run RDISK /s from the command prompt
Run WINNT /ox from the installation CD-ROM
Run WINNT /s- from the NT system directory

Page 59 Answer B

26. Which is true about the Administrator account?

It cant be deleted.
It cant be renamed or deleted.
It cant be renamed

Page 73 Answer A

27. What information can be found in the following NBTSTAT output?

```
Name               Type         Status
---------------------------------------------
MB12244-049782 <00>  UNIQUE      Registered
MANITOBA       <00>  GROUP       Registered
MB12244-049782 <03>  UNIQUE      Registered
MB12244-049782 <20>  UNIQUE      Registered
SLUKASCHUK     <03>  UNIQUE      Registered
MB12244-049782 <01>  UNIQUE      Registered
```

SLUKASCHUK is logged onto the machine.
SLUKASCHUK is the name of the domain that the machine is a member of.
The administrator account has been renamed.

Page 72 Answer A

27. Which of the following is false:

NBTSTAT shows a list of netbios names.
NBTSTAT only shows the currently logged in user when the messenger service is running.
NBTSTAT is not installed by default on NT Workstation

Answer C Page 72

28. The administrator account is often targetted by password guessing programs because:

It has complete system access to the ERD and SAM.
By default, the account can not be locked out due to bad logon attempts.
It can not be renamed.

Page 73 Answer B

29. The L0phtCrack utility:

Can sniff password hashes off the network.
Can crack all passwords using only a limited dictionary based attack.
Can be discovered on a system by installing Option Pack 4.

Page 74 Answer A

30. When RDISK /S- is run,

An ERD is stored on floppy disk.
A copy of the SAM is stored in the %SystemRoot%/Repair folder.
Cleartext passwords are revealed from password hashes for all user accounts.

Page 75 Answer B

31. What can't the Microsoft Security Configuration Editor do?

Define a template of security configuration settings.
Compare a remote machine's settings against a template.
Reconfigure the local machine's settings to match a template.

Page 76 Answer B

32. The password for a null sessions user is:

A space.
Enter.
The null character.

Page 80 Answer C

33. Null sessions users are members of the:

Network group
Backup Operators group
Authenticated Users group

Page 80 Answer A

34. The null user:

Is the same as the user account for IIS (IUSR_computername)
Uses the Guest account if enabled.
Always has a Security ID (SID) of S-1-5-7

Page 80 Answer C

35. Null user sessions are not:

Used by the local system account to connect to remote machines.
Used by any known applications and can safely be disabled.
Identical to automatic guest logons.

Page 81 Answer C

36. To prevent null sessions from listing users and groups from a domain:

A registry change is required.
Disable the NULL account in USER MANAGER Advanced.
Encrypt the local user database with SYSKEY

Page 85 Answer A

37. An excellent way to get a very strong password:

Is to combine multiple words with no relation to each other
Set the password expiry limit as low as possible, optimally 30 days or less.
Include extended characters in the password.

Page 87 Answer C

38. By default, the Administrator account locks out:

After 3 failed login attempts
After 5 failed login attempts
Never

Page 88 Answer C

39. To recover from a locked out administrator account:

Logon at a domain controller
Use your ERD to reload the SAM
Login with the Guest account and reset the Administrator password

Page 88 Answer A

40. A honeypot or decoy Administrator account:

Should trigger an event when accesed.
Have unlimited rights to the filesystem
Be members of the Domain Admins group.

Page 89 Answer A

41. The "automatic" guest logon applies when:

The password for the guest account is set to a Null character.
The password for the guest account is blank AND the guest account is not disabled
A user correctly supplies his username but incorrectly enters his password.

Page 90 Answer B

42. A role or shared account can actually increase security IF:

It is used as a general purpose account.
It is strictly limited in functionality.
It satisfies the needs of a large group of people.

Page 91 Answer B

43. Windows NT standalone systems which are not members of a domain have access to:

Local Accounts
Global Accounts
Standalone Accounts

Page 96 Answer A

44. A problem with using a domain account for a service account:

The domain account can not have their access controlled.
The password is stored in the registry.
Trojan horses can be started in login scripts

Page 99 Answer B

45. Third party password filters:

Generally don't provide as much functionality as Microsoft's PASSFILT.
Can not enforce the use of non-alphanumberic symbols
May contain password snatching trojans.

Page 101 Answer C

46. With a null user session, an attacker can:

List the account and password policies in force on your domain controller.
Change the account and password policies in force on your backup domain controller.
Enforce different policies for different users.

Page 104 Answer A

47. The SYSKEY.EXE utility:

Strongly encrypts the entire SAM.
Strongly encrypts password information sent over the network during network logons.
Is available with service pack 3 and later.

Page 109 Answer C

48. NTLM v2 authentication:

Is not available by default for Windows 95 clients.
Is the default authentication mechanism.
Strongly encrypts the password hashes in the SAM.

Page 112 Answer A

49. When supporting users over the phone:

They should provide their password to administrators.
It is better to issue new passwords than reveal the current one (if known).
Granting them administrator access temporarily is a good way to resolve a problem.

Page 128 Answer B

50. Good practice for groups, rights and permissions includes:

Organizing users into Global groups based on common needs and roles.
Organizing users into Local groups based on common needs and roles.
Granting rights to individual users for easy administration.

Page 134 Answer A

51. NTFS volumes:

Allow permissions to be enforced on FAT volumes.
Do not support file and folder inheritable permissions.
Allow permissions to be enforced over the network.

Page 136 Answer C

52. NTFS and Share permissions:

Combine to give the cumulative permissions.
Combine to give the most restrictive of these two permissions.
Combine to form new permissions only on IIS servers.

Page 137 Answer B

53. The default NTFS and share permission for Everyone is:

Full Control but should be Change.
Generally pre-applies the principal of least privilege.
Do not allow anyone to modify executable files

Page 140 Answer A

54. One of the differences between the Change and the Full Control permission:

Is the ability to modify attributes of files.
Is the Change Permissions permission.
The ability to read data or execute programs.

Page 140 Answer B

55. The Everyone group:

does not include users from untrusted domains.
does not appear in user manager.
Has full control of Shares by default.

Page 142 Answer C

56. Null users can be prevented from listing Share names by:

Modifying the properties of the %SYSTEMROOT% folder.
Modifying a registry value.
Changing Null user's permissions in User manager.

Page 149 Answer B

57. Administrative shares on NT Systems:

Are installed by default and may not be removed.
Are installed by default and the permissions to them should be changed according to the principles of least required.
Are hidden and named for the volume.

Page 150 answer C

58. Within the registry of a Windows NT workstation:

The everyone group has read access to certain portions.
The everyone group has full control to certain portions.
The everyone group has no access to the registry.

Page 152 Answer A

59. The Named Pipe File System:

Is only accessible through registry modifications.
Is meant for file storage as an alternative to NTFS
Can be accessed with SMB.

Page 158 Answer C

60. RAS server phone numbers:

Should be located on a company's internet web server.
Are susceptible to port scans.
Are discoverable by wardialing.

Page 161 Answer C

61. A security feature of RAS is:

User definable callback number.
Data encryption.
v.90 modem support.

Page 162 Answer B

62. The default packet filtering of Windows NT:

Is upgradeable for free with Routing and Remote Access Service from Microsoft.
Is generally sufficient for use as a corporate security measure.
Rivals the features available in commercial products.

Page 164 Answer A

63. Network monitor agents:

Provide features generally not found in commercial products.

Are best left uninstalled if access to them is not limited.
Are Microsofts automated but limited intrusion detection systems.

Page 165 Answer B

64. By default SMB sessions are not digitally signed. This makes them susceptible to:

Trojan horse programs.
Packet replay attacks.
Denial of service attacks.

Page 166 Answer B

65. A tip for securing Internet Information Server is:

Ensure that the IUSER_computername account is granted NO ACCESS to all NTFS volumes.
Install all features currently available (ie: FTP, NNTP, etc)
Delete all sample files and scripts.

Page 169 Answer C

66. An audited event typically does not record the:

Date and time of the event.
User's name.
Digital signature of the user

Page 175 Answer C

67. NT's audit log can be viewed remotely with:

Control Panel
Event Viewer
REGEDT32

Page 177 Answer B

68. A good source of legal advice on the use of honey pots, marked files, or other network defenses is:

The NT online help
NT Security step-by-step text book
A lawyer

Page 184 Answer C

69. The right to view and clear the security log is called:

Managed Auditing and Security Log (SeSecurityPrivelege)
Inbox Repair tool
Diagnostics logging

Page 186 Answer A

70. If the system log is set to overwrite events older than 7 days:

The security log is vulnerable to being flushed by hackers.
Events related to operating system performance may be overwritten in 7 days.
The log must be cleared manually

Page 187 Answer B

71. Enabling the CrashOnAuditFail option:

Allows a server to continue operating when no logging is occuring
May be desirable in high security environments
Prevents a hacker from using audit logging as a denial of service attack.

Page 190 Answer B

72. Automated event log analysis:

Is configured through the Control Panel applet
Solves the problem of too much data and the need for realtime alerts.
Allows multiple administrators to delegate granular authority within a domain

Page 196 Answer B

73. A prioritized list of those who should be contacted when a security incident occurs is part of a:

User list exported from User Manager for Domains.
Financial risk assessment
Incident response plan.

Page 200 Answer C

74. A 1996 FBI study found that what percentage of security breaches are carried out by legitimate users?

75
25
.75

Page 203 Answer A

75. It is often easier to launch an attack from a workstation inside the organization's network than from the internet because:

They do not have to worry about physical security measures like security officers.
There is often no firewall separating internal users from internal servers.
Servers may not have the most recent service pack installed.

Page 204 Answer B

76. System Policy in NT 4.0:

Is a way of defining registry changes for users, groups and computers.
Forms part of the license agreement presented when installing NT.
Replaces the limited tool User Manager for Domains

Page 207 Answer A

77. Resolution of differences in system policy applied to two groups to which a user belongs:

Is done on a most restrictive basis like NTFS and File Share access permissions.
Is performed directly through modifications to the user's registry.
Is done according to the ranking of groups assigned by the administrator

Page 208 Answer C

78. POLEDIT.EXE:

Is a registry editting tool that is not as powerful as REGEDT32.
Is a third party tool that replaces Microsoft's System Policy Editor.
Is bundled with Windows 9x by default.

Page 208 Answer A

79. Windows systems automatically look for a policy file in:

The %systemroot%\policy folder
The NETLOGON share
The %systemroot% folder

Page 210 Answer B

80. Windows 95 users attempt to download system policy settings from the domain controller in a file called:

Config.pol
95config.pol
%username%config.pol

Page 210 Answer A

81. System policy template files:

Are available only in the NT Option Pack.
Allow end users to modify who has access to their file system.
Are designed to be modifiable by hand

Page 211 Answer C

82. System policy template files:

Can affect settings of Microsoft applications and operating systems only.
Can affect settings of almost any registry value.
Are in a binary executable format.

Page 212 Answer B

83. System policy is:

Not available to improve the security of Windows 9x desktops
Available to evaluate how close to C2 security a workstation is.
Not enforced in MS-DOS mode.

Page 215 Answer C

84. One problem with using system policy to change the registry is:

That system policy can not set registry permissions
Most users are familiar with how to change system policy
It can not prevent users from undoing changes with regedt32.exe.

Page 216 Answer A

85. A hyperlink to a REG file is a way to make changes to a user's registry but:

It requires the installation of expensive third party software.
Users should never import registry files from anywhere but trusted web sites.
Its more complicated than setting up unattended script files

Page 216 Answer B

86. When automatic logon is enabled in the registry.

The user's password is stored in the registry in cleartext.
The user's password is stored in the SAM in cleartext
A user is required to enter their username and password only once per day.

Page 218 answer A

87. Cached credentials:

Allow internet explorer 5.x to finish typing your email address in a web page

html form.
Are used when a user attempts to log on, but no domain controller is available for authentication.
Are disabled by default.

Page 221 Answer B.

88. Logging off and locking a workstation are different because logging off:

Closes all open files and running applications.
Allows hackers access to domain controllers.
Is faster.

Page 222 Answer A

89. One way to protect workstations that users leave logged in and unattended is:

Restricting users to select passwords which meet complexity requirements.
Shorter keyboard cables.
Requiring password protected screen savers.

Page 223 Answer C

90. Passwords should be shared with:

Very close coworkers only.
Telephone help desk personnel who call.
No one.

Page 224 Answer C

91. It is important to protect passwords because:

NT's password encryption algorithm is easily crackable.
They are commonly the only secret information required for authentication to the network.
They are impossible to replace if lost.

Page 224 Answer B

92. Workstations with unauthorized modems installed:

Are usually the work of sophisticated hackers.
Are usually installed by employees who are doing everything they can to compromise network security.
Are usually installed by well meaning employees who believe that security through obscurity protects the access point.

Page 225 Answer C

30 Questions from IIS

1. CGI scripts and Active Server Pages (ASP):

Contain scripting that is executed within a client's browser.
Contain scripting that is excuted on the webserver.
Do not contain scripting that can be executed.

Page 18 Answer B

2. Allowing clients to see the code in CGI or ASP files is:

Dangerous because it allows the client to analyze the script for exploitable security holes.
Necessary in order to execute the scripts.
Dangerous because users may change contents of the scripts to execute unauthorized code.

Page 18 Answer A

3. Access to restricted files is protected by:

Properly configured permissions.
Poorly written scripts.
Cookies placed on the client's workstation.

Page 24 Answer A

4. An attack which uses a dictionary of passwords and a list of usernames is a:

Denial of service attack.
Reverse social engineering ploy.
Brute force attack

Page 25 Answer C

5. Vulnerability to buffer overflow attacks is caused by:

Incorrectly set permissions.
Programming flaws.
Lack of available drive space.

Page 27 Answer B

6. An example of misconfigured permissions is a folder:

With both the Read and Execute permissions.
With both the Write and Execute permissions.
Used for storage of executable code.

Page 27 Answer B

7. A connection interception program can be installed to successfully accept incoming requests in place of the installed web server because:

Most TCP/IP stacks will give preference to a program listening on a particular IP address over those listening for any address.
IIS includes functionality for installation of connection interception programs by default.
The full SMS version of Network Monitor must be used to capture packets not originating from or sent to one's own machine.

Page 30 Answer A

8. The following is not a method for maintaining state in web based applications.

Cookies on a client's hard drive with a session ID number.
Additional information in the URL path which the server knows how to process.
Modification of the host name records on a registered DNS server.

Page 31 Answer C

9. An advantage to moving the root folder off the IIS server is:

The IIS server will be able to serve the pages from this folder more quickly.
That if the IIS server were damaged by hackers, the content could still remain safe behind the firewall.
That one more single point of failure is introduced.

Page 49 Answer B

10. An advantage to making an IIS server a stand-alone server is that:

The NETLOGON channel does not have to be shared to the internal LAN.
It uses domain accounts which can reduce the number of passwords a user must remember.
A one way trust relationship is easier to establish.

Page 52 Answer A

11. The following service is generally not required on a IIS web server:

Protect storage (pstores.exe)
Simple TCP/IP services

World Wide Web publishing service (inetinfo.exe)

Page 54 Answer B

12. Which of these is not a IIS authentication method?

Digest
Complex
NTLM

Page 67 Answer B

13. Where can authentication be required?

A referring web site's link.
An individual folder within a website
An individual field within a web form.

Page 68 Answer B

14. The Anonymous Account is:

Equal to the System account
Equal to the null session user account
Transparent to the user and compatible with all clients.

Page 71 Answer C

15. The IUSR_*computername* account should be disabled because:

It uses weak passwords.
It's access permissions can not be controlled.
Its account name is well known to hackers.

Page 73 Answer C

16. One problem with the Basic authentication method is that:

It does not strongly encrypt the username and password.
It is not supported by most browsers.
It is too slow to be used in most situations.

Page 75 answer A

17. One problem with the Digest authentication method is that:

It does not strongly encrypt the username and password.
It is not supported by most browsers.
It is too slow to be used in most situations.

Page 78 answer B

18. One problem with the Kerberos authentication method is that:

It does not strongly encrypt the username and password.
It is not supported by most browsers.
It is too slow to be used in most situations.

Page 81 answer B

19. If IIS manages the password for the IUSR account, that account:

May need to be renamed to reflect a different computer name.
May need the Log On Locally right.
May occasionally not have a password at all.

Page 90 Answer B

20. A feature of one way or public key cryptography is:

That it is faster at encrypting data than two way or private key cryptography.
That the algorithms are simple enough to perform with pen and paper.
That you may share one key with the world to encrypt messages with and yet no one with this key may decrypt information.

Page 94 Answer C

21. A digital certificate:

binds one's credentials to one's public key.
Is printed with photocopy resistant inks and methods.
Can only be read by someone who knows the private key.

Page 95 answer A

22. A digital certificate for use by IIS must be:

Obtained from Verisign or Entrust.
Installed on the clients.
Obtained from a Certifying Authority (CA).

Page 96 Answer C

23. An advantage to using a certificate from Entrust on your server instead of a certificate issued by a Windows 2000 CA is that:

Most clients have a copy of Entrust's certificate preinstalled.
They are generally cheaper to obtain.
Have an expiry date further in the future.

Page 97 Answer A

24. With the default behavior of trusting all CA's when a certificate trust list is not entered,

It is very important to ensure a certificate trust list is entered.
IIS defaults to a DENY ALL security level.
Certificates signed by Netscape enterprise server will be rejected.

Page 102 Answer A

25. When a client browser uses certificate authentication, the client's certificate must be:

Signed by the Primary Domain Controller.
Protected as it contains the client's private key.
Mapped to a user account.

Page 104 Answer C

26. SSL is incapable of:

Verification that data has not been altered in transit.
Encryption of user account info in the SAM.
Verification of the identity of the webserver to the client

Page 110 Answer B

27. SSL with 128 bit session encryption keys is how many times more stronger than with 40 bit session encryption keys?

Approximately 3 times
Approximately 4 thousand times
Approximately 5 million times

Page 113 Answer B

28. When SSL is enabled with the "Requires 128 bit encryption" option and the client's browser does not support it,:

The client is given a link to www.microsoft.com to download the security upgrade.
The server downgrades the requirement to 40 bit and tries again.
The client receives an error message.

Page 113 Answer C

29. Running applications in the High (isolated) Application protection mode:

Gives the best performance
Puts IIS in danger of being damaged.
Prevents other applications from crashing them.

Page 144 Answer C

30. The IWAM_*computername* account:

Can be a target for hackers as it sometimes must be an administrator
Is an acronym for the Internet Will Always MakeMoney.
Is functionally equivalent to IUSR_*computername*

Page 145 Answer A

30 Questions from Active Directory

1. Active Directory:

Augments but does not replace the SAM database.
Contains information about the users and computers on the network.
Is available on most non Microsoft platforms.

Page 9 Answer B

2. The switch from mixed mode to native mode:

Can be done, and undone, without reinstalling the OS.
Will require Kerberos authentication.
Can not be done on NT 4.0 without service pack 6a or better.

Page 17 Answer B

3. The database used by Active Directory is:

Functionally very similar to that used by Exchange.
Able to use circular or space based logging.
Stored in the root of C: by default.

Page 21 Answer A

4. The schema manager snap in cannot be installed until:

Its filespace is formatted with the NTFS file system.
All domain controllers are in Native mode.
Its DLL has been registered with the operating system.

Page 27 Answer C

5. A “site” is a:
Set of computers belonging to the same Domain.
Set of well connected computers on IP subnets.
Similar to an organization unit.

Page 31 Answer B

6. Access to a global catalog (GC) server at logon time is important because:

A user’s universal group membership must be checked against the GC.
A GC is the only type of server that can perform authentication.
It will greatly speed up login time.

Page 35 Answer A

7. The following is not a Flexible Single Master Operation (FSMO) Master role:

Global Catalog Master
PDC Emulator Master
Schema Master

Page 37 Answer A

8. The Schema master:

Is responsible for all Site replication optimization.
Is responsible for all FSMO elections.
Is responsible for all changes to the structure of the objects and attributes in the AD database.

Page 38 Answer C

9. Information normally associated with Active Directory such as Domains and OUs is held in which context?

Schema Naming
Configuration Naming
Domain Naming

Page 45 Answer C

10. Objects on hard drives and objects in AD are similar in that:

Both can be formatted with NTFS.
They can be referenced with path names.
Both are physical structures.

Page 46 Answer B

11. Trust Relationships in Windows 2000 Domains are:

Easier to setup than in Windows NT.
Not necessary to setup. They exist from startup.
Are one way trusts only unless specified exclusively in the trust management wizard.

Page 49 Answer B

12. Domains within a single forest do not:

Exist as a single tree.
Trust each other.
Share a common schema.

Page 51 Answer A

13. Organizational units:

Are sub divisions of domains.
Can include multiple domains.
May not include other OUs.

Page 52 Answer A

14. A distribution group:

Is a way to apply policy to users with common requirements.
Is an email list.
Can not contain members from multiple domains.

Page 57 Answer B

15. Universal groups should only contain global groups:

As they are limited to how large they can grow.
As individual users get their security policy applied only at the local level.
To minimize replication between GC Servers.

Page 58 Answer C

16. A container or object that does not inherit from its parent container is called:

A widow.
A twig.
An orphan

Page 65 Answer C

17. OUs should be setup the same as the departments, committees, and divisions

of an organization because:

It must mirror the organization's structure.
It allows for easy verification of organization charts.
Users in the same area often require the same permissions.

Page 73 Answer C

18. Group policy may not be applied to:

Sites and Domains
Organization Units
Users

Page 84 Answer C

19. A group policy:

Exists only as a property of an OU, site, or domain.
Can be modified by going to the property of an OU.
Is deleted when the OU to which it is attached is deleted.

Page 86 Answer B

20. NT 4.0 system policy is supported in mixed mode:

By placing the NTCONFIG.POL file in the NETLOGON share on the Windows 2000 DC.
By maintaining at least one NT4.0 BDC.
By a registry setting on the workstation.

Page 89 Answer A

21. Usually at least two group policy objects (GPOs) would be applied to an OU:

,One for user settings and another for machine settings so that roaming users would maintain their settings regardless of which machine they use.
Because GPOs are processed in a random order.
Because one provides a backup in case the other becomes corrupt.

Page 91 Answer A

22. A way to make a user or group exempt from an existing GPO to which they would normally be part of is:

To change the user's widow orphanage setting to False.
Remove the user from that domain.
To assign the Deny Read and Deny Apply permission.

Page 95 Answer C

23. Which of the following is false?

Group policy can be used to install applications.
A user may be given permission to modify a GPO but not have permission to link it to any OU.
Users generally have permission to modify GPOs that affect them.

Page 96 Answer C

24. GPO assigned scripts can:

Be set to start at computer shutdown.
Not be set to run at computer startup as no user context is available.
Be written in Vbscript or DOS style commands only.

Page 101 Answer A

25. Windows 2000 GPO administrative templates are not:

Used to control registry values.
The same as NT 4.0 system policy templates.
Editable by hand like NT 4.0 system policy templates.

Page 108 Answer B

26. Group policy:

Depends on Active directory.
Is available on Windows 2000 servers that do not have Active Directory installed.
Is available only as a third party add on.

Page 7 Answer A

27. The DCPROMO utility:

Can promote a server to a domain controller.
Allows for the permission of individual directory items to be set from the command line.
Saves any encryption keys that you may currently be using.

Page 12 Answer A

28. One of the main reasons for installing Windows 2000 with the backwards compatibility option is:

To improve upon the security found in NT 4.0
To allow some older applications to continue to function on Windows 2000.
Jason Fossen recommends it.

Page 16 Answer B

29. One thing that Windows 2000 still must use is:

Netbios over TCP/IP
Wins servers.
SMB.

Page 18 Answer C

30. The main tool for managing Windows 2000 and Active directory is:

Dcpromo.exe
Ldp.exe
MMC

Page 24 Answer C

Last Updated: July 25th, 2017

Upcoming Training

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 13, 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 Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced