Global Information Assurance Certification Paper

Securing Unix Systems GIAC Practical for Harley Sanders

6.1 Unix Basics for the Security Professional

1) Modern Unix kernels utilize loadable modules which means that kernel code for a device is loaded:

   a) Each time the system is booted
   b) when the device is accessed
   c) if the kernel detects that the device is connected to the system
   d) manually upon request of the superuser

The correct answer is c
Ref: Page 2-12

2) On SYSV Unix machines, "normal" multi-user run level is:

   a) S
   b) 2
   c) 3
   d) 6

The correct answer is c
Ref: Page 2-15

3) What is the longest filename that can be specified on Solaris?

   a) 8
   b) 11
   c) 255
   d) 1024

The correct answer is c
Ref: Page 2-25

4) On a BSD Unix system, what is the result of removing the /boot file before rebooting?

   a) The system will boot from an alternate /root file
   b) The administer must boot off the OS media and restore the /boot program manually
   c) The system will boot into single user mode
   d) There will be no noticeable effect

The correct answer is b
Ref: Page 2-29

5) You have a cron job the runs the "du" command against the /dev directory on a regular basis. You notice that the size of the directory has recently changed. How can you interpret this change?

   a) A larger number of users than normal are signed onto on the system, increasing resource load
   b) An attacker may have gained access to your system, and has tried to hide some files on your system
   c) New users have been added, creating additional home directories
   d) The cable to your printer has gone bad

The correct answer is b

Ref: Page 2-30

6) The fifth column shown by an "ls" command is a date. This date indicates:

   a) The date the file was last modified
   b) The date the file was created
   c) The date access to the file expires
   d) The date the file was added to the directory

The correct answer is a
Ref: Page 2-33, 2-44

7) If the setuid permission flag is set on a file, it means:

   a) Only the owner can change permissions on the file
   b) The file is not executable
   c) Anyone in the owner's primary group has full access to the file
   d) The program runs as the owner of the file, instead of as the person who executes the program

The correct answer is d
Ref: Page 2-36,37

8) Permissions on file Unix.lst are "-rwxr-sr--". If you are not in the same primary group as the owner of the file, what permissions do you have for that file?

   a) Read, write, and execute
   b) Read only
   c) Read and execute
   d) None

The correct answer is a
Ref: Page 2-36,37

9) myfile.tst has permissions set as "-rw-r--r--". Which of the following permission modes will change the access to myfile.tst to allow all users to execute the file?

   a) chmod +x myfile.tst
   b) chmod 755 myfile.tst
   c) umask 022 myfile.tst
   d) a, b, and c

The correct answer is d
Ref: Page 2-38,39,40

10) The overlap partition on a disk:

   a) Is used to hold temporary files during file copy and move activities
   b) Is used to hold buffer overflows that occur during kernel processes
   c) Represents the entire disk geometry
   d) Is a special read-only partition used by internal kernel functions

The correct answer is c
Ref: Page 2-42

11) You run the "df –k" command against your local FFS file system. You notice that the (bytes used) and (bytes available) numbers don't equal the total size of the partition. Is this a cause for concern?

a) Yes. It indicates a bug in the kernel process that requires a complete rebuild of the system.
b) Yes. It indicates that an attacker has compromised your system.
c) No. There are other entries in the command listing that make up the difference.
d) No. The file system reserves 10% of the total partition because performance suffers if the partition gets too full, and shows 100% usage when the partition is actually only 90% full.

The correct answer is d
Ref: Page 2-43

12) You run an ls –l command against a directory. There are no subdirectories shown, and the link count is 5. This indicates:

a) You are at the bottom of a directory tree, and can't go any deeper.
b) Your ls command may have been compromised, and the attacker has hidden files on your system.
c) There are special files in some directories that are not displayed using ls -l. You must use the ls -al command to see them.
d) The directory had subdirectories, but the link count hasn't been updated using a "refresh" command yet.

The correct answer is b
Ref: Page 2-51

13) John complains to you that Mary can read his files, even though he set permissions to only allow him to read them. Mary swears she hasn't cracked John's password. The first thing you should do is:

a) Log Mary's activity on the system to make sure she is telling the truth.
b) Check John and Mary's UIDs to make sure they aren't the same
c) Check the permissions on John's files to make sure he has set them correctly.
d) Change John's password to lock Mary out of his files.

The correct answer is b
Ref: Page 2-69

14) In a BSD system, the command "ps –auxww" will display a detailed listing for processes for all users, including system processes not tied to any particular user login session, and the entire command line that was executed, no matter how long the command line was. How can you duplicate this command on a Solaris system?

a) ps -ef
b) ps -efww
c) ps –auxww
d) You can't. Solaris only will display the first 80 characters of the command line.

The correct answer is d
Ref: Page 2-77, 78

15) In order to shut down a running process and create a core dump file, what command needs to be executed?

a) kill -HUP <pid>
b) kill -3 <pid>
c) kill -9 <pid>
d) kill <pid>

The correct answer is b

Ref: Page 2-80

16) On a SYSV system, the "fuser" command can be useful by:

a) Showing which files are open by which processes
b) Showing which processes were started by which users
c) Showing which users are currently accessing the system
d) Showing users that have attempted to access files they don't have permissions for

The correct answer is a
Ref: Page 2-84

17) You know you have one network card on your system, on interface le0. When you run the "netstat –in" command, you see entries for le0 and lo0. The lo0 interface has an IP address of 127.0.0.1. What does this indicate?

a) A hacker has gained physical access to your system and installed another network card in order to monitor your network traffic.
b) An alias has been set up on the le0 interface.
c) The le0 interface is for incoming traffic, and the lo0 interface is for outgoing traffic. This is a normal condition.
d) The lo0 interface is the "loopback" interface, used for internal communications on the system. This is a normal condition.

The correct answer is c
Ref: Page 2-86

18) Even though your system has access to a DNS server, using the /etc/hosts file can be useful in order to:

a) Guarantee accurate resolution of IP addresses and hostnames
b) Improve hostname resolution performance for often-accessed systems
c) Decrease required administration for the DNS servers
d) Control which users can access which network hosts

The correct answer is b
Ref: Page 2-91

19) The standard port for a telnet server is:

a) 23
b) 25
c) 80
d) 514

The correct answer is a
Ref: Page 2-96

20) The ARP protocol is used to:

a) Resolve host names to IP addresses
b) Determine owners of internet domains
c) Determine which user owns which active process
d) Resolve IP addresses to hardware addresses

The correct answer is d
Ref: Page 2-102

21) "Ping" is a simple command used to:

a) test whether your system can communicate with the network
b) determine if your hostname can be resolved by DNS
c) determine whether a network host is up and responding on the network
d) a and c

The correct answer is d
Ref: Page 2-105

22) Sending a "ping" to the local LAN broadcast network address will cause all machines on the local network to respond. This will fill the machine's ARP cache with the hardware addresses for all machines on the LAN. Why is this useful?

a) It allows the administrator to identify machines that are sending out malformed packets over the network
b) It allows the administrator to identify machines that have been added to the network without his knowledge
c) It overwrites obsolete ARP information in the cache, improving network communications.
d) a and b

The correct answer is d
Ref: Page 2-108

23) You should never edit a crontab file directly in the cron directory because:

a) You may change the permissions on the file, rendering it non-executable
b) Your changes may be overwritten by other administrators using the crontab –e command
c) The system monitoring software may interpret this as an attack on your system
d) The cron process may try to execute a cron command, with unforseeable results

The correct answer is b
Ref: Page 2-118

24) If there is an entry in the syslog.conf file for auth.warn, what message levels will be logged to syslog

a) Authentication messages at warning level
b) Authentication messages at warning level and above
c) Authentication messages at warning level and below
d) None. Warning level messages are sent to a different log file.

The correct answer is b
Ref: Page 2-121 – 2-124

25) After changing the syslog.conf file, what must be done in order to have the new configuration become active?

a) Reboot the system
b) renice –n <syslogd pid>
c) kill -HUP <syslogd pid>
d) /etc/init.d/syslog stop, then /etc/init.d/syslog start

The correct answer is c
Ref: Page 2-126

6.2 Common Issues and Vulnerabilities in Unix Security

1) Reusable passwords are a security vulnerability. Why?

   a) They can be stolen by someone watching you type your password
   b) They are relatively easy to crack using brute force methods
   c) They are often written down and kept near the computer they are used on
   d) All of the above

The correct answer is d
Ref: Page 7-15

2) The safest passwords:

   a) Contain upper and lower case characters
   b) Contain upper case, lower case, and numeric characters
   c) Contain upper and lower case, numeric, and special characters
   d) Are not reusable

The correct answer is d
Ref: Page 8

3) How many characters in the 13 character encrypted password string are used as the "salt"?

   a) 1
   b) 2
   c) 3
   d) 4

The correct answer is b
Ref: Page 18

4) The arguments to the crypt() function are:

   a) The salt and the cleartext password
   b) The salt, the cleartext password, the time and date
   c) The cleartext password
   d) The cleartext password, the spice, and the username

The correct answer is a
Ref: Page 19

5) Core dump files are dangerous because:

   a) They can overwrite other important files on the partition
   b) They can overwrite each other, cause wasted time trying to debug process problems
   c) They are world readable, and contain whatever was in memory at the time the process aborted
   d) All of the above

The correct answer is c
Ref: Page 27-29

6) A buffer overflow attack:

a) Attempts to lock up the processor by sending an extremely long string as input to an application
b) Attempts to exploit the time lag between two operations in an application
c) Attempts to write past the end of an allocated string buffer in an attempt to overwrite the return execution address, causing the program to jump instead to a malicious instruction
d) None of the above

The correct answer is c
Ref: Page 39

7) The best way to stop buffer overflow attacks is to:

a) Fix the programs that contain the exploitable string buffers
b) Teach programmers to check the length of the strings they accept as input
c) Run the stringchk() function to make sure that all string buffers are of acceptable length
d) Modify the kernel so that executing an instruction in the stack causes the program to abort

The correct answer is d
Ref: Page 44-45

8) Which of the following is not a used as an attack against a set-UID script?

a) Symlink tricks
b) Brute force attack
c) Environment attacks
d) Race conditions

The correct answer is b
Ref: Page 51

9) A set-UID environment attack:

a) Exploits the time lag between two commands in the script to gain a root shell prompt
b) Attempts to write past the end of an allocated string buffer in an attempt to overwrite the return execution address, causing the program to jump instead to a malicious instruction
c) Exploits scripts that don't set variables such as PATH and IFS from within the script
d) None of the above

The correct answer is c
Ref: Page 55

10) set-UID problems can only be avoided by:

a) Fixing the underlying operating system
b) Writing the script correctly
c) Not using set-UID scripts
d) a and b

The correct answer is c
Ref: Page 56-57

11) When a process is chroot()ed, it is:

a) Wrapped in a "safe" C program
b) Able to only access files in the specified chroot()ed directory and below
c) Changed from an interpreted process to a compiled process
d) None of the above

The correct answer is b
Ref: Page 60

12) Which of the following is not a use for chroot()?

a) Running networked services in captive environments so security holes n these services can't be exploited against the entire machine
b) Testing new services when you are not sure how secure the service may be
c) Creating safe environments from which to run set-UID processes
d) Creating captive shell accounts for users

The correct answer is c
Ref: Page 61

13) One way to detect backdoor trojan horse programs is to:

a) Run the "strings" command against binaries such as login, ssh, ftp, and rlogin
b) Run the "ls -al" command to check the last modified date for binaries such as login, ssh, ftp, and rlogin
c) Check the /etc/shadow file to see if any system usernames have been assigned valid passwords
d) All of the above

The correct answer is a
Ref: Page 74

14) A rootkit is:

a) A trojan horse program designed to allow an attacker to gain root on a system
b) A bundle of compromised programs that are packaged together to enable the attacker to avoid detection for an extended period of time
c) A collection of security programs written on read only media used to detect compromised programs
d) A program designed to make the superuser account impregnable to exploitation by a hacker

The correct answer is b
Ref: Page 75

15) The problem with writing undetectable rootkits is:

a) There are too many binaries to replace all of the ones that could cause the rootkit to be detected
b) Checksumming (like the process used by Tripwire) allow for easy detection of compromised binaries
c) The more complex a rootkit becomes, the greater the chance of detection by a careful system administrator
d) All of the above

The correct answer is d
Ref: Page 80

16) The .rhosts file is a target for attackers because:

a) Security on the .rhosts file is difficult to configure
b) The .rhosts file contains a list of accounts and machines that are implicitly trusted to connect to the system without giving a password
c) a and b
d) none of the above

The correct answer is b
Ref: Page 84

17) The most effective way to protect against .rhost exploits is:

a) Write a script that automatically removes any .rhosts files found on the system
b) Replace the .rhosts files in user's directories with a .sshhosts file
c) Disable the "r-commands" (rlogin, rsh, etc) in /etc/inetd.conf and use ssh instead
d) Replace the .rhosts file in user's directories with the hosts.equiv file

The correct answer is c
Ref: Page 87

18) Modern Unix systems protect against the most vulnerable aspects of tftp by:

a) Requiring a password in order to gain access to the system
b) Only allowing a user to get files, but not to write them
c) Not allowing tftp to be executed from X terminals and diskless workstations
d) Chroot()ing the tfpt server at start-up

The correct answer is d
Ref: Page 97

19) The most effective defense against session hijacking attacks is:

a) A firewall to monitor source IP addresses
b) Encryption such as ssh or IPSEC
c) Re-prompting the user for their password at random intervals
d) a and c

The correct answer is b
Ref: Page 100

20) The major problem(s) with Remote Procedure Calls is:

a) It doesn't have an authentication scheme
b) Many vendors have reverse-engineered their own buggy and divergent RPC implementations
c) a and b
d) none of the above

The correct answer is b
Ref: Page 102

21) The automounter should be run on client workstations whenever possible because:

a) The automounter rechecks the NFS security configuration on a regular basis
b) Attackers may attempt to spoof the IP address of legitimate client workstations
c) The automounter will automatically unmount file systems that haven't been accessed in some period of time
d) The automounter will periodically refresh the NFS export parameters

The correct answer is c
Ref: Page 117

22) If you must use NFS despite all it's vulnerabilities, you should:

a) Block access to portmapper, nfsd, and lockd at your firewall
b) Monitor NFS mounted directories using Tripwire
c) Set up mounted home directories in a chroot()ed environment
d) All of the above

The correct answer is a
Ref: Page 121

23) Sun Microsystems quit shipping Sparc workstations with small optional microphones because

a) An incorrectly attached microphone can cause static electricity, which can cause disk and memory problems
b) Users were able to record sound files, interfering with their productivity
c) No one used them, so it was more economically sound to not ship them
d) A user with root access to the machine can read the data from the microphone device and play the data on the audio device (speakers), effectively "bugging" the location where the machine was located

The correct answer is d
Ref: Page 124

24) A backup isn't a backup:

a) If the backup media is stored at the same location as the machine from which it was taken
b) If an attacker is able to get a physical copy of it
c) Until you do a restore from it
d) If the backup job is run unencrypted over the network

The correct answer is c
Ref: Page 125

25) A common mistake in setting up redundant network links is to:

a) Using cable shielding that is susceptible to environmental damage
b) Forgetting to set the pressure alarm for the two-layered pressurized conduit
c) Not testing the failover process to the secondary link
d) Have the redundant links travel through the same physical conduit

The correct answer is d
Ref: Page 132

6.3 Unix Security Tools and Their Uses

1) Why is it important to not use security tools that have dynamically loaded libraries?

a) It's difficult to guarantee the libraries are for the current release of the tool.
b) It's possible to an attacker to modify the load path environment, resulting in a corrupted or exploited library being loaded.
c) Dynamically loaded security tools take longer to run, resulting in delays during time sensitive investigations.
d) T's difficult to reproduce the execution of the tool at a later time in the investigation, because the library might have been changed.

The correct answer is b
Ref: Slide 14

2) Which is *not* a valid use for the COPS tool?

a) Examining the root environment and system setup
b) Execute commands and detect extreme or unusual behavior
c) Examine group and password files
d) Examine user home directories

The correct answer is b
Ref: Slide 20

3) What is the negative aspect of running Tiger with Tiger_Collect_CRACK=Y in the Tiger configuration file?

a) Tiger will check only local passwords
b) Tiger will not email the results of the check
c) Tiger will wait until Crack has completed and add the results to Tiger's mail, which may take a very long time
d) Tiger will run it's own password guessing tool instead of Crack

The correct answer is c
Ref: Slide 74

4) Setting Tiger_Check_PATH will report if:

a) Root's path contains a "."
b) Root's path has non-standard directories included
c) A script has been written in such a way that it's PATH environment variable can be altered before being executed
d) None of the above

The correct answer is a
Ref: Slide 86

5) One of the major problems with Tiger is that it:

a) Has been compromised with trojans on some sites, so be careful where you get it from
b) Doesn't really check important file and path information thoroughly by default
c) Is very difficult to configure and use
d) Produces a lot of spurious warning and doesn't have a filtering mechanism

The correct answer is d
Ref: Slide 113

6) Tripwire is a security tool for**:**

a) Checking the integrity of selected file and directories
b) Analyzing log output and extracting relevant entries
c) Restricting the set of commands that a user can run from a privileged shell
d) Enforcing creation of strong passwords by users

The correct answer is a

Ref: Slide 116

7) In order to skip a directory and it's subtree, precede the directory name with which character?

a) #
b) !
c) \
d) ~

The correct answer is b
Ref: Slide 118

8) A security hole in the configuration and use of Tripwire is:

a) It's open source software, and therefore hackers can read the code looking for ways around it
b) It's very old, and hasn't been updated for newer systems
c) If the database and config files aren't on read only media, the output cannot be trusted
d) There is only one algorithm for producing the checksums, and it is showing it's age

The correct answer is c
Ref: Slide 133, 137

9) Which of the following is *not* a goal of using Swatch?

a) To analyze logs, extracting relevant entries
b) To read log entries as they are added to a file
c) To protect the logs files from being corrupted by log cleaning programs
d) To execute commands based on log entries

The correct answer is c
Ref: Slide 139

10) lsof is a program that:

a) lists which files are in use by which processes, and who is connecting to your server
b) executes an ls command from a directory other than /usr/bin in order to have an uncorrupted listing program in case of a hack
c) checks files for valid permissions, including alerting for set-UID scripts
d) none of the above

The correct answer is a
Ref: Slide 167

11) The -i flag allows lsof to report who is connecting to your sever based on:

a) host
b) port
c) protocol
d) any of the above

The correct answer is d
Ref: Slide 174

12) Which of the following network analysis tools logs and controls access from remote clients?

a) ISS
b) courtney
c) nmap
d) tcp_wrappers

The correct answer is d
Ref: Slide 197

13) Which flag causes ISS to scan a host or hosts for open ports?

a) -f
b) -o
c) -p
d) -e

The correct answer is c
Ref: Slide 212

14) courtney is a network analysis too that was created to:

a) detect network scanners, particularly SATAN
b) checks network packets for proper formatting based on the port and protocol
c) checks for known bugs in various NFS implementations
d) checks for malformed tcp packets

The correct answer is a
Ref: Slide 248

15) Which of the following commands will perform a stealth scan on host tester?

a) #nmap –sT tester
b) #nmap –sF tester
c) #nmap –sS tester
d) #nmap –sX tester

The correct answer is b
Ref: Slide 262, 263

16) Which of the following timing options is *not* valid for nmap?

a) Paranoid
b) Polite
c) Insane
d) Psychotic

The correct answer is d
Ref: Slide 278

17) Other than scanning for open ports, nmap can also perform other interesting options, such as

a) Checking the umask on important host files
b) Running brute force password attacks against a host
c) Checks to see what users are currently logged on
d) Guesses the OS type and reports how hard it was to guess

The correct answer is d
Ref: Slide 276

18) In order to run nessus you must also get and install:

a) Crack and yps
b) Gimp and nmap
c) Tcp_wrapper
d) SATAN

The correct answer is b
Ref: Slide 284

19) Nessus can be a better choice to run than SATAN because:

a) It has a more complete set of tests
b) If there is no response from a host via ping, it assumes the host is dead
c) It produces fewer false positives
d) All of the above

The correct answer is a
Ref: Slide 292

20) The default syslog logging level for tcp_wrapper is:

a) mail.crit
b) auth.warn
c) mail.info
d) user.alert

The correct answer is c
Ref: Slide 302

21) With tcp_wrapper, having the same daemon name and client host pair in both the hosts.allow and hosts.deny files will result in:

a) The host being allowed access to the daemon
b) The host being denied access to the daemon
c) A warning message will be produced, and access will be allowed
d) A warning message will be produced, and access will be denied

The correct answer is a
Ref: Slide 304, 308

22) When a user attempts to execute a command through sudo, sudo will:

a) Check to see if the user is authorized to run the command
b) Prompt the user for their password before running the command
c) Prompt the user for a password every few minutes
d) All of the above

The correct answer is d
Ref: Slide 329

23) sudo –l <command> will:

a) log all of the user's keystokes for the duration of the command
b) lock the user's access tot he command for a specified period of time
c) list the allowed and forbidden commands for the user
d) none of the above

The correct answer is c
Ref: Slide 334

24) PGP was designed to:

a) Provide C functions to automatically configure the use of system(3) and popen(3) functions
b) Force users to choose strong password
c) Provide enciphered, authenticated and integrity-checked electronic mail, as well as providing digital signatures for signing files
d) Execute commands, and detect extreme and unusual behavior

The correct answer is c
Ref: Slide 373

25) Which of the following password tools is useful in guessing a user's password?

a) S/key
b) crack
c) passwd+
d) lsof

The correct answer is b
Ref: Slide 394

6.4 – Running UNIX Applications Securely

1) When configuring WU-FTP, you should use the /etc/passwd file, suitably modified to not block legitimate users, to populate :

a) ftpaccess
b) ftpusers
c) ftpgroups
d) ftpservers

The correct answer is b
Ref: Page 12

2) Configuring WU-FTP in /etc/inetd.conf to run in standalone mode will bypass access control with TCP wrappers, but this is alright because:

a) WU-FTP can provides effective access control using the /ect/ftpaccess configuration file
b) WU-FTP can be run to log sessions in syslog
c) a globally accessible anonymous ftp site doesn't have much use for TCP wrappers anyway
d) all of the above

The correct answer is d
Ref: Page 13

3) File downloads and uploads are logged:

a) in the xferlog file, usually found in /var/log
b) in the location specified in syslog for the LOG_FTP facility
c) in the location specified in syslog for the LOG_USER facility
d) in the location specified in syslog for the LOG_AUTH facility

The correct answer is a
Ref: Page 18

4) In order to control the format of uploaded file names in WU-FTP, you should configure:

a) ftpaccess
b) ftpnames
c) ftpconversions
d) ftpservers

The correct answer is a
Ref: Page 21-23

5) Files that are uploaded to your WU-FTP site should:

a) require authentication, blocking uploads from anonymous or guest clients
b) be set up as read/write, so the user can update the information if they need to
c) have permissions set so that clients can't see what is in the directory
d) all of the above

The correct answer is c
Ref: Page 21-23

6) In an Apache web server configuration file, what does the mod_auth module handle?

a) basic allow/deny access control
b) HTTP Basic Authentication
c) anonymous FTP style username/password authentication
d) HTTP/1.1 Digest Authentication

The correct answer is b
Ref: Page 31

7) The order mutual-failure access control option for an Apache web server implies:

a) the host is allowed if it appears under allow, whether it is in deny or not
b) the host is denied if it appears under deny, whether it is in allow or not
c) the host is allowed only if it appears in allow, and not in deny
d) none of the above

The correct answer is c
Ref: Page 40-41

8) Since setting the FollowSymLinks option to none adversely effects performance, you may want to consider specifying the:

a) VerifySymLinks option
b) FollowSymLinks verify option

c) FollowSymLinks root option
d) SymLinksIfOwnerMatch option

The correct answer is d
Ref: Page 40

9) It is important to have a default index page for every directory in order to:

a) avoid exposing a directory listing of files and subdirectories to casual users
b) help users more successfully navigate your site
c) avoid sending users the 404 Page Not Found message
d) improve page loading performance

The correct answer is a
Ref: Page 42

10) You can override directory settings on an Apache web server setting directives in:

a) .htoverride
b) .htoptions
c) .htaccess
d) none of the above

The correct answer is c
Ref: Page 43

11) Although Apache supports MD5 hash Digest Authentication, it is also requires:

a) a cryptographically strong random number generator
b) that the client also supports digest authentication
c) the client to have an entry in /etc/passwd
d) a and b

The correct answer is d
Ref: Page 30-31, 45

12) In order to install a fully functional Apache web server on a development workstation that is only accessible by the workstation, you must:

a) set the DenyAllExceptLocalhost in .htaccess
b) set Listen 127.0.0.1:80 in conf/httpd.conf
c) set the default route on the workstation to 127.0.0.1
d) disconnect the workstation from the network

The correct answer is b
Ref: Page 48-49

13) the most common means of having your Apache web server compromised is:

a) not checking for IP spoofing
b) installing a trojanized version of the software
c) not allowing indexing without having default index.html pages
d) allowing improperly inspected CGI input

The correct answer is d
Ref: Page 51-55

14) In order to limit CGI's disk access you should

a) chroot() the CGI script to run under a dedicated UID/GID
b) use third party CGI scripts
c) confine the character set to known "safe" values
d) run the CGI script as "nobody"

The correct answer is a
Ref: Page 54

15) DNS is used to:

a) Resolve IP addresses to MAC addresses
b) Resolve hostnames to IP addresses
c) encrypt web traffic
d) none of the above

The correct answer is b
Ref: Page 64-65

16) There are security issues that result running BIND, including:

a) Giving away too much information
b) Buffer overflows
c) Cache poisoning
d) all of the above

The correct answer is d
Ref: Page 67

17) The best and simplest defense against the numerous buffer overflow problems that have been historically experienced in BIND is:

a) run BIND in a chroot()ed environment
b) run BIND as a Split Horizon DNS
c) stay up to date on the version of BIND you are running
d) block unauthorized zone transfers

The correct answer is c
Ref: Page 67

18) Running BIND as a Split Horizon DNS helps prevent

a) exposing too much information about your internal network to the Internet
b) exposing too much information about your BIND version
c) IP spoofing
d) a and b

The correct answer is d
Ref: Page 73-75

19) When configuring a bastion host, it is important to:

a) restrict access to specific IP address ranges
b) remove any unneeded services
c) have only one network interface defined
d) b and c

The correct answer is b
Ref: Page 77

20) DESTETC tells BIND:

a) where to look for it's configuration file
b) where to drop the named.pid file
c) what the name of the default directory is
d) what the OS version is

The correct answer is a
Ref: Page 82

21) You can hide your BIND version from outsiders by:

a) using the allow-transfer option
b) restricting port 53 traffic with your firewall
c) using the query-source option
d) changing the text in the version option to something meaningless or misleading

The correct answer is d
Ref: Page 84

22) Running BIND in a chroot()ed environment:

a) limits the files an attacker can access, even if they subvert your name server daemon
b) improves performance
c) is required to be able to use a split horizon configuration
d) none of the above

The correct answer is a
Ref: Page 96-104

23) By default, SMTP traffic is sent over port

a) 23
b) 25
c) 53
d) 80

The correct answer is b
Ref: Page 109

24) Although aggressive anti-spam controls result in a higher percentage of false positives, you should always:

a) maintain your own blacklist
b) check email addresses for embedded shell commands
c) disallow relaying
d) query a third party spammer list in realtime

The correct answer is c
Ref: Page 117-121

25) Since most machines are *not* mailservers, they should:

a) be configured as a nullclient
b) not run the Sendmail daemon
c) invoke Sendmail periodically from a cron job to flush queued messages
d) all of the above

The correct answer is d
Ref: Page 125

6.5 – Linux Practicum

1) The default runlevel for Linux is set in what parameter in /etc/inittab?

a) runlevel
b) id
c) ca
d) si

The correct answer is b
Ref: Page 17

2) To disable ctrl+alt+del reboots, specify what parameter in /etc/inittab?

a) runlevel
b) id
c) ca
d) si

The correct answer is c
Ref: Page 18

3) Using Pluggable Authentication Modules means that without changing login programs you can impose access limits, impose resource limits, and:

a) change password encryption type
b) impose session limits
c) open or close service ports
d) redirect log file destinations

The correct answer is a
Ref: Page 22

4) Which of the following is *not* PAM configuration file module type?

a) auth
b) account
c) session
d) host

The correct answer is d
Ref: Page 23

5) Which of the following is *not* a PAM module config file?

a) access.conf
b) resource.conf
c) limits.conf
d) time.conf

The correct answer is b
Ref: Page 24

6) If you specify type as "hard" for a item in the limits.conf file:

a) the kernal enforces the limit and it cannot be increased
b) you can still adjust limits within the "hard range" by specifying the same item with type "soft"
c) a and b
d) none of the above

The correct answer is c
Ref: Page 26

7) Syslog messages are prioritized based on:

a) facility and level
b) facility and privilege
c) privilege and level
d) facility and priority

The correct answer is a
Ref: Page 30

8) When configuring logfile rotation, you should always:

a) uncomment the compress option to compress the logfile into gzip format after rotation
b) change the rotation period parameter from weekly to monthly
c) change the rotate parameter to increase the number of back logs you keep
d) all of the above

The correct answer is d
Ref: Page 32-33

9) A central log server can be extremely useful for:

a) ease of logged information retrieval
b) relieving load on the remote server
c) analyzing compromised systems
d) limiting access to system logs

The correct answer is c
Ref: Page 36

10) Compiling a kernel:

a) requires detailed knowledge of the system hardware
b) isn't usually required since most modern distributions include a module that contains almost every possible drive
c) a and b
d) none of the above

The correct answer is b
Ref: Page 41

11) If a compiled kernel is too big even after being gzipped, you should:

a) remove unnecessary modules, and re-compile
b) increase the memory in your machine
c) run "make clean" against the gzipped kernel
d) execute "make bzlilo" instead of "make zlilo"

The correct answer is d
Ref: Page 46

12) When using RPM to install updated packages, specifying –F <update directory> will:

a) force all packages to be installed, even if the dates match
b) only install packages that already exist and have an earlier version number
c) install packages that you hadn't installed previously
d) leave the previous version of the kernel intact, in case you need to boot with the old kernel

The correct answer is b
Ref: Page 49

13) When running the up2date Update Agent for Red Hat, after configuring it for the correct ftp site, username, and password, you must still:

a) establish an encrypted session to the server
b) make sure Perl is installed
c) respond to interactive dialog
d) click on the "connect" button

The correct answer is d
Ref: Page 52

14) To disable services in /etc/inetd.conf, you should edit the fiel and comment out any unneeded services. You must then:

a) run killall –HUP inetd
b) reboot the system
c) run /etc/inetd stop and /etc/inetd start
d) run kill –9 inetd

The correct answer is a
Ref: Page 60

15) If a connection source is not defined in /etc/hosts.allow or /etc/hosts.deny, the connection will be:

a) allowed
b) denied

c) prompted for authentication
d) dropped with no response

The correct answer is a
Ref: Page 63

16) Best practice when using TCP wrappers is to:

a) drop any unauthorized access attempts without sending a deny message
b) deny all access by defualt, and selectively allow required hosts
c) a and b
d) none of the above

The correct answer is b
Ref: Page 64

17) When running the netstat command, which flag is required to display which process is listening to which port?

a) -l
b) -r
c) -p
d) -n

The correct answer is c
Ref: Page 66

18) Which of the following is not a valid mount option for NFS?

a) rw
b) nosuid
c) noguid
d) noexec

The correct answer is c
Ref: Page 72

19) Because RPC uses UDP packets to communicate, you must:

a) enable reverse DNS lookups
b) specify the hosts allowed to access the portmapper by IP address
c) open all UDP ports above 1023 on your firewall
d) none of the above

The correct answer is b
Ref: Page 73

20) If you do not specify a hostname when defining exported directories in /etc/exports:

a) no one will be able to export the directory
b) the directory will be world exportable
c) the directory can be exported, but permissions will be read-only
d) The directory will be world-writable

The correct answer is b
Ref: Page 74

21) When specifying which hosts are allowed to submit print jobs in Red Hat, you should put the list in:

a) /etc/hosts.lpd
b) /etc/hosts.equiv
c) /etc/hosts.allow
d) /etc/hostslp.conf

The correct answer is a
Ref: Page 75

22) Samba makes a Unix server:

a) able to run Microsoft applications
b) communicate using the NetBIOS protocol
c) look like an NT server in the network neighborhood
d) b and c

The correct answer is c
Ref: Page 78

23) In order to stop shares on a Linux server from being accessible by anyone, you must configure:

a) /etc/smb.allow and /etc/smb.deny
b) /etc/hosts.allow and /etc/hosts.deny
c) /etc/hosts.equiv
d) /etc/smb.conf

The correct answer is d
Ref: Page 80

24) The three basic ipchains for Linux are:

a) accept, deny, reject
b) accept, reject, redirect
c) input, output, redirect
d) input, output, forward

The correct answer is d
Ref: Page 86

25) Before scanning your network:

a) test the scan on an isolated network
b) get a signed piece of paper authorizing you to perform the scan
c) post notice that the scan is going to happen
d) all of the above

The correct answer is d
Ref: Page 105

6.6 – Solaris Practicum

1) When installing the Solaris Core System Support cluster, you need to add what package in order to enable remote administration?

   a) SUNWsprot
   b) SUNWarc
   c) SUNWnptr
   d) SUNWter

The correct answer is d
Ref: Page 1-16

2) Since the default umask for system daemons is 000, files created by these daemons:

   a) Are world writeable
   b) Are only accessible by root
   c) Have securely set permissions
   d) Cannot be read by anyone

The correct answer is a
Ref: Page 1-30

3) Removing the line "Sc:234:respawn:/usr/lib/saf/sac –t 300" from /etc/inittab will

   a) Disable the listener on parallel ports
   b) Still allow the login: prompt to be displayed on the /dev/tty/a (console) device
   c) Disable the listener on serial ports
   d) a and b

The correct answer is d
Ref: Page 1-36

4) The fourth column in the /etc/vfstab file defines:

   a) What device will be mounted
   b) Where the device will be mounted
   c) What file system format is to be expected
   d) Whether the system should automatically mount at boot

The correct answer is c
Ref: Page 1-43

5) Since nosuid also implies nodev:

   a) Devices can't operate in a nosuid environment
   b) The root directory can't be mounted nosuid
   c) Chroot()ed environments can't be mounted nosuid
   d) All of the above

The correct answer is d
Ref: Page 1-45

6) Installing ssh, besides enabling secure remote access and administration:

   a) Enables X Windows and most other IP protocols to run over encrypted tunnels
   b) Enforces strong passwords
   c) Automatically configures all machines on the network as secure clients

d) a and b

The correct answer is a
Ref: Page 1-49

7) When configuring TCP wrappers access controls:

a) The hosts.deny file should be set to deny all by default
b) The hosts.allow file should be set to allow all by default
c) You can leave both files empty to lock out all remote access
d) You can allow access by UID

The correct answer is a
Ref: Page 1-56

8) Make sure root is in /etc/ftpusers:

a) To allow root to ftp into the system
b) To stop root from ftp'ing into the system
c) To allow root to own the ftp environment
d) To make sure the ftp environment blocks anonymous access

The correct answer is b
Ref: Page 1-64

9) When you configure syslog to log messages of certain priority:

a) You also automatically log all messages for each higher level priority
b) You also automatically log all messages for each lower level priority
c) You can log the same message to more than one destination
d) a and c

The correct answer is d
Ref: Page 1-66

10) In order to be able to write to a logfile:

a) The administrator must create (touch) the file
b) The file must be world writeable
c) The file must be world readable
d) a and c

The correct answer is a
Ref: Page 1-67

11) After rotating a log file:

a) The syslogd daemon needs to be reinitialized with a HUP signal
b) The syslogd daemon should be killed and restarted
c) The new file is created with mode 755 by default and needs to be reassigned to 644
d) No log information has been missed

The correct answer is b
Ref: Page 1-68

12) The main advantage of syslog-ng is:

a) It allows syslog to be sent over tcp instead of udp, allowing ssh tunneling
b) It uses gzip compression for remote syslogging, improving network performance
c) a and b
d) none of the above

The correct answer is a
Ref: Page 1-69

13) Which utility will produce graphs from sar data?

a) SarTek
b) /var/sadm/sa
c) perf
d) sag

The correct answer is d
Ref: Page 1-73

14) In order to enable process accounting, run:

a) accton
b) paccton
c) accton /var/adm/pacct
d) paccton /var/adm/pacct

The correct answer is c
Ref: Page 1-75

15) In order to disable process accounting, run:

e) accton
f) paccton
g) accton /var/adm/pacct
h) paccton /var/adm/pacct

The correct answer is a
Ref: Page 1-75

16) You should modify the banner files for various services:

a) To warn users and attackers that they are being monitored and could be prosecuted for improper use
b) To mislead attackers as to which OS and version of the service they are seeing
c) a and b
d) none of the above

The correct answer is c
Ref: Page 1-78-79

17) In order to disable Stop-A you must modify:

a) /etc/default/login
b) /etc/default/su
c) /etc/default/kbd
d) /etc/default/profile

The correct answer is c
Ref: Page 1-80

18) In order to force a password to be entered whenever any EEPROM command is issued (other than a normal reboot), set:

a) eeprom security-mode=none
b) eeprom security-mode=command
c) eeprom security-mode=full
d) eeprom security-mode=password

The correct answer is b
Ref: Page 1-82

19) To prevent set-UID programs from being brought in on removable media, edit:

a) /etc/rmmount.conf
b) /etc/nosuid.conf
c) /etc/system
d) none of the above

The correct answer is a
Ref: Page 1-84

20) In order to stop attackers from seeing world readable core dump files that may contain important information like the /etc/shadow file, set core dump size to 0 in::

a) /etc/core.conf
b) /etc/system
c) /etc/inetd.conf
d) /usr/sbin

The correct answer is a
Ref: Page 1-85

21) Creating an empty read only /.rhosts file:

a) Will allow only the superuser to use rlogin, rsh, and rcp
b) Will thwart attacks that attempt to drop a /.rhosts file containing +
c) Enables the "r" commands to be re-enabled quickly if ssh stops working
d) a and c

The correct answer is b
Ref: Page 1-86

22) Backups are only useful if:

a) They're current
b) The media is still readable
c) You can find the media
d) All of the above

The correct answer is d
Ref: Page 1-98

23) If you configured /etc/hosts.deny to email the administrator when failed ssh connections are attempted,

but you don't receive the mail:

a) The hosts.allow file may be too permissive
b) Securehost may have an invalid sendmail.cf file
c) You may not be running the Sendmail daemon
d) All of the above

The correct answer is b
Ref: Page 1-91

24) YASSP is a tool for:

a) Modifying file permissions
b) Running BIND securely
c) Automatically hardening a Solaris system
d) All of the above

The correct answer is c
Ref: Page 1-105-110

25) Which of the following is another Solaris hardening tool?

a) TITAN
b) FISH
c) SYASSP
d) PARC

The correct answer is a
Ref: Page 1-111

Unix@Night – Network Time Protocol

1) The accuracy standard for NTP is:

a) Within 5 seconds
b) Within 3 minutes
c) Within 1 tenth of second
d) Within hundredths of a second

The correct answer is d
Ref: Page 4

2) Time synchronization is important organization because:

a) Effective prosecution of security incidents requires accurate matching timestamps on all log files
b) Many security products require accurate time information in order to work properly
c) Correct time information is necessary when using a parallel/distributed make product
d) All of the above

The correct answer is d
Ref: Page 5

3) Burst mode NTP was implemented in v4 , but:

a) Is too buggy to use in a critical production environment
b) Has been back-ported into NTP v3 distribution
c) Requires additional hardware expenditures
d) Has not caught on as a Internet time standard

The correct answer is b
Ref: Page 7

4) An NTP primary server:

a) Is the clock against which all other servers in a distributed environment are set
b) Runs a process that contacts the other servers in the network, and pushes down the correct time
c) Sets it's clock against a highly accurate external time source
d) Requires an extremely powerful processor

The correct answer is c
Ref: Page 9

5) The stratum of a server is:

a) Equal to the highest level server that it is in communication with
b) Equal to the lowest level server that it is in communication with
c) Equal to one plus the highest level server that it is in communication with
d) Equal to one plus the lowest level server that it is in communication with

The correct answer is d
Ref: Page 11

6) Clients who take time information from a server without notifying the server's administrator are known as:

a) Clock suckers
b) Dependents
c) Slaves
d) Time thieves

The correct answer is a
Ref: Page 12

7) It is important to have your server in communication with more than one external clock source:

a) In case you lose contact with a clock source
b) In case your clock source experiences drift
c) To make proper use of the built in algorithms for detecting and ignoring bogus time information attacks
d) To make use of average time algorithms that enable sub-second accuracy

The correct answer is c
Ref: Page 13

8) Without a pseudo clock, when your internet gateway or other WAN link goes down all of your local time servers will suddenly become stratum:

a) 0
b) 1
c) 8

d) 16

The correct answer is d
Ref: Page 19

9) When you configure a pseudo clock in your NTP environment, you should:

a) Set the stratum of pseudo clock a couple of points higher than the stratum of the regular clock server
b) Make sure it is not accessible from the internet
c) First run ntpdate to get to the approximate real time
d) Make sure the server is configured as a peer

The correct answer is a
Ref: Page 19

10) The NTP startup script first calls ntpdate:

a) To verify connectivity to the internet clock sources
b) To jump your server time close enough to true time to allow NTP to synchronize
c) To verify proper licensing of the software
d) To verify the settings in the /etc/ntp.conf file

The correct answer is b
Ref: Page 27

Unix@Night – One Time Passwords

1) What is required for every One Time Password (OTP) system?

a) A radius server
b) Dial-up access to the system
c) A software or hardware cryptographic hash calculator
d) An encrypted session with the system you are accessing

The correct answer is c
Ref: Page 5

2) A synchronous two-factor OTP device:

a) Requires the user's secret in order to compute the response
b) Continuously produces new passwords
c) Generates a public/private key pair
d) None of the above

The correct answer is b
Ref: Page 8

3) Other than the inevitable technical difficulties, what is one of the biggest problems you will face when implementing an OTP system?

a) The expense of the software
b) Choosing the correct token for your environment
c) Identifying the users that need the tkens

d) Educating users and overcoming their initial resistance

The correct answer is d
Ref: Page 13

4) If a user trying to access an OPIE OTP system does not have an entry in the /etc/opieaccess file on that server, what will be the result.

a) The user will not be able to access the system
b) The user will be able to access the system without authentication
c) The system will fall back to the /etc/passwd process for authentication of the user
d) The user will be dynamically added to the /etc/opieaccess file

The correct answer is c
Ref: Page 18

5) One very important step in the install for OPIE is to:

a) Have an open root shell, and don't give it up until you verify that OPIE is working properly
b) Make the permissions for /etc/opiekeys mode 755
c) Make sure to use the make install process from the OPIE source directory
d) Use Tripwire to create digital signatures of the OPIE binaries as a baseline

The correct answer is a
Ref: Page 20, 21

6) The /etc/opiekeys file should be considered to be equivalent to:

a) /etc/hosts
b) /etc/passwd
c) /etc/shadow
d) /etc/resolv.conf

The correct answer is c
Ref: Page 21

7) In order to be able to type in the OPIE secret password directly on the console, which flag should be specified on the opiekeys command?

a) -a
b) -c
c) -n
d) -x

The correct answer is b
Ref: Page 21

8) After cut and pasting the challenge string into an OPIE calculator window and entering his OPIE secret, the opiekey program returns:

a) A 13 character hexadecimal string
b) A six word response
c) A 1024 bit public key
d) A request to re-enter the OPIE secret for verification

The correct answer is b

Ref: Page 23

9) In contrast to OPIE, commercial OTP solutions generally employ

   a) A large staff of administrators to keep the system available at all times
   b) Small, handheld secret key calculators
   c) An extra security server device to maintain the user/token database
   d) None of the above

The correct answer is c
Ref: Page 26

10) At a minimum, a commercial OTP system should:

   a) Support Radius for communicating with network devices
   b) Provide replacement replacement login, ftpd, and su programs, plus an application library which allows you to hack OTP support into your own local apps
   c) Be able to quickly lock out a lost or stolen token
   d) All of the above

The correct answer is d
Ref: Page 35

Unix@Night – Secure Shell (SSH)

1) Ssh is a secure replacement for:

   e) login, cp, and ftp
   f) rlogin, rcp, and rsh
   g) telnet and ftp
   h) ksh, csh, and sh

The correct answer is b
Ref: Page 5

2) Which of the following is not an ssh authentication method?

   a) Host based trust files
   b) Rhosts combined with RSA-based authentication
   c) .Xauthority trust files
   d) RSA-based user authentication

The correct answer is c
Ref: Page 8-11

3) When using RSA-based user authentication, the user's public key must be copied to the remote host and:

   a) Run through a keygen process to create a private key
   b) Placed in the user's home/.ssh/authorized_keys file
   c) Verified using a hand held authentication token
   d) Placed in the /etc/hosts.allow file

The correct answer is b

Ref: Page 10

4) Other ssh capabilities include

   a) Secure X11 connections
   b) Secure port forwarding
   c) a and b
   d) none of the above

The correct answer is c
Ref: Page 13-15

5) During the ssh connection process, the server sends the client a 64 bit cookie:

   a) For IP spoofing prevention
   b) To enable secure tunnel configuration
   c) For session key generation
   d) For protocol version verification

The correct answer is a
Ref: Page 19

6) If ssh is configured on a client to transparently replace rsh, rlogin, and rcp, and the remote host doesn't support ssh:

   a) The login process will fall back to /etc/passwd authentication
   b) ssh will automatically run the moved rsh, rlogin, or rcp command
   c) the user can't connect until the system admin installs ssh on the server
   d) rsh, rlogin, and rcp must be re-enabled in order to connect to the server, and the user must use ssh to non-transparently connect to ssh-configured servers

The correct answer is b
Ref: Page 22

7) Using the "with-login" option in./configure:

   a) Will cause ssh to fall back to the /bin/login program if it can't connect to the server securely
   b) Will replace the /bin/login program with a secure version so an attacker can't bypass the ssh authentication process
   c) Will cause ssh to invoke /bin/login after user authentication
   d) None of the above

The correct answer is c
Ref: Page 27

8) Although ssh can be configured using the "with-kerberos" option to enable support of Kerberos v5:

   a) It is not recommended due to OS specific xomplications
   b) Kerberos will be installed in a non-standard configuration
   c) There are process problems that can result in the ssh session hanging or disconnecting unexpectedly
   d) There is no documentation with the ssh distribution to set up Kerberos, so previous Kerberos experience is recommended

The correct answer is d
Ref: Page 28

9) ssh has many run time options, which are evaluated in the following order

   a) command line, system config file, user config file
   b) command line, user config file, system config file
   c) user config file, command line, system config file
   d) system config file, command line, user config file

The correct answer is a
Ref: Page 31

10) Connection and authentication options in the configuration of sshd does *not* include:

   a) AllowHosts/DenyHosts to determine which hosts are allowed to connect
   b) AllowUsers/DenyUsers to determine which users are allowed to login
   c) AllowGroups/DenyGroups to determine which primary groups can login
   d) AllowPorts/DenyPorts to determine which ports ssh can connect over

The correct answer is d
Ref: Page 33

Unix@Night – Unix Forensics

1) When an intrusion is detected, there is an immense amount of pressure to investigate and recover from the compromise. This makes it difficult or impossible to:

   a) Collect evidence in a thorough manner
   b) Make sure the evidence collected is admissible in court
   c) Record the scene of the incident without altering the state of the computer
   d) All of the above

The correct answer is d
Ref: Page 10

2) Which of the following is not necessary in order to be a good Unix forensics investigator?

   a) A certification from a well respected security organization
   b) A broad base of experience in system administration, networking, intrusion detection techniques, and advanced incident handling
   c) A plan to deal with an intrusion
   d) A toolkit of "clean" commands and tools

The correct answer is a
Ref: Page 21-23

3) In order to be secure, an incident response toolkit:

   a) Must be commercially available and supported by a reputable company
   b) Must include a complete copy of the compromised OS
   c) Must be in read-only format, preferably CD-ROM
   d) Must include dynamically linked binaries

The correct answer is c
Ref: Page 23

4) If you can't use statically linked executables on your incident response toolkit:

   a) You will not be able to guarantee your results
   b) You should ensure that any dynamic library links are done against the libraries on the CD
   c) You should link to libraries on a remotely mounted NFS system
   d) You need to compare all link library sizes on the compromised system to a clean system to ensure they haven't been replaced

The correct answer is b
Ref: Page 26

5) When collecting evidence, it is extremely important to:

   a) Collect the most volatile evidence first
   b) Take a snapshot of the compromised system(s) by using the script command
   c) Maintain a verifiable chain of evidence
   d) All of the above

The correct answer is d
Ref: Page 35-39, 50

6) When running commands like netstat and lsof on a compromised machine that has been removed from the network, make sure you:

   a) Use the clean version from your CD
   b) Use the -n option to avoid trying to do network name resolution
   c) Have a tape drive mounted on the system
   d) Have a root session on the console

The correct answer is b
Ref: Page 42

7) The lsof command is an important tool in forensics because:

   a) It isn't part of the original OS install, and therefore is seldom a part of a rootkit
   b) It shows the same information as netstat, but in a more easily readable format
   c) It displays the network state, the process state, and the file state
   d) All of the above

The correct answer is c
Ref: Page 41, 45

8) The dd utility is excellent for obtaining file system information because:

   a) It copies the input files block by block, including blocks of data marked "deleted"
   b) It's faster than tar or dump
   c) It is a difficult binary to compromise
   d) It is simple to run, and most administrators are very familiar with it

The correct answer is a
Ref: Page 49

9) File Integrity Assessment tools such as Tripwire and L5 are only useful if:

   a) You can verify the integrity of the integrity assessment tools
   b) They were installed before the compromise occurred, and up to date baseline files were kept

c) Someone or some process regularly monitors the output files
d) All of the above

The correct answer is b
Ref: Page 56-57

10) Even if a machine has been highly compromised, it is often possible to find useful evidence:

a) On system backup tapes
b) By interviewing the administrator of the machine, and looking for inconsistancies between his knowledge and the current state of the machine
c) By identifying the rootkit that was installed, and working backwards
d) By investigating logs from remote machines, including syslog servers, IDS systems, firewalls, and routers

The correct answer is d
Ref: Page 60-61

Last Updated: July 24th, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**