Global Information Assurance Certification Paper

SANS Network Security 2000

Monterey

UNIX Track 6 Certification Practical Exam

by

Marlene Lane

Phoenix, Arizona

November, 2000

6.1 UNIX Basics for the Security Professional

1. Why may it be unwise for the privileged user, root, to execute the following command, where 3791 is the process ID of a large database query?

renice –n –19 3791

A. This may effectively lock up the system.
B. This may open process ID 3791 for undetected intrusion.
C. This may provide the individual actually running the query enough time to bring up another instance of the database.
D. None of these.

CA A, page 2-83

2. The programs **truss**, **trace**, and **ktrace** are most useful for

A. setting the termcap.
B. examining the content of core files.
C. cracking the /etc/shadow file.
D. debugging.

CA D, page 2-84

3. NFS originated at

A. the Department of Defense.
B. Digital Equipment Corporation.
C. Microsoft.
D. Sun Microsystems.

CA D, page 2-7, 2-22

4. In which sequence does Unix boot?

A. Boot loader, kernel initialization, initialization of system processes, run of start up scripts
B. Kernel initialization, initialization of system processes, boot loader, run of start up scripts
C. Kernel initialization, boot loader, initialization of system processes, run of start up scripts
D. Run of start up scripts, kernel initialization, boot loader, initialization of system processes

CA A, page 2-10

5. _____ is/are usually found in ROM or NVRAM.

   A. Start up scripts
   B. Device and other special configuration files
   C. The kernel
   D. The boot loader

CA D, page 2-11

6. Unix SYSV start-up scripts are typically stored in the _____ directory.

   A. /etc/init.d
   B. /var/sadm/install
   C. /etc/rcf
   D. /etc/adm

CA A, page 2-16

7. The server process **named**, known as **in.named**, on some systems, is part of

   A. the portmapper.
   B. NFS.
   C. DNS.
   D. ftp and other network services.

CA C, page 2-21

8. The key advantage to running **automounter** is

   A. It can resolve name-to-IP-address lookups.
   B. It can dynamically reallocate NVRAM at startup.
   C. It administers and logs *cron*.
   D. It can shutdown idle NFS-mounted file systems.

CA D, page 2-22

9. Which of the following describes Unix's file naming convention?

   A. File names can be up to 1024 bytes in length.
   B. File names may contain any characters except "/" and null (ASCII 0).
   C. File names may contain embedded directory names.
   D. File names may not contain escape sequences, such as *control M* (^*M*).

CA B, page 2-25

10. On SYSV systems, _____ shows file names with non-printing characters represented by their octal ASCII value.

    A. ls –b
    B. ls –f
    C. ls –ll
    D. ls –latr

CA A, page 2-27

11. Given the following listing of a Unix directory and assuming one is currently working from within that directory, what would the following command accomplish?

touch hostinfo

```
total 23368
-rw-------   1 marlene  sysadmin 3514870 Mar 17  2000   broker.sav
-rw-------   1 marlene  sysadmin   123648 Mar 20  2000   broker_fw_scripts
-rw-------   1 marlene  sysadmin    30571 Apr 27  2000   broker_fw_vx
-rw-------   1 marlene  sysadmin 3659504 Mar 20  2000   broker_scripts
-rw-------   1 marlene  sysadmin   290024 Apr 27  2000   broker_vx
-rw-------   1 marlene  sysadmin 3502909 Jun 15 07:12   dev_server
-rw-------   1 marlene  sysadmin     1758 Apr  3  2000   domain_status
-rw-------   1 marlene  sysadmin     1136 Apr  3  2000   domain_switch
-rw-------   1 marlene  sysadmin    13855 May  5 14:08  hostinfo
-rw-------   1 marlene  sysadmin    31663 May  9 14:06  ssp
-rw-------   1 marlene  sysadmin    32177 May 19 14:06 sundevil_20000509
-rw-------   1 marlene  sysadmin     5073 Apr  3  2000   sys_id
-rw-------   1 marlene  sysadmin   677926 Jun 15 07:12   tx_sun
```

    A. A "No such file or directory" error would occur.
    B. Two new files, *touch* and *hostinfo*, would be created.
    C. The time stamp of files beginning with "t" and files beginning with "h" would be updated to the current system time.
    D. None of these.

CA D, page 2-26

12. Although one could put individual user log-in directories virtually anywhere in a Unix file system, which of the following directories is the **least** likely place for user's home directories?

    A. /users
    B. /usr
    C. /u1
    D. /home

CA B, page 2-28

13. Although one could store configuration files just about anywhere on a Unix system, which of the following is the most common location of configuration files?

    A. /
    B. /config
    C. /etc
    D. /usr/local/share

CA C, page 2-29

14. What files exist within the **/var/spool/cron/crontabs** or, on some systems, within the **/var/cron/tabs** directory?

    A. disk quota files
    B. print spooler files
    C. mail files if sendmail is configured and activated
    D. user files containing automated jobs

CA D, page 2-32

15. Which type of file is the following?

lrwxrwxrwx 1 root other 13 Aug 27 1999 vxva -> /opt/VRTSvxva

    A. An AF_UNIX address family socket
    B. A symbolic link
    C. A fifo or named pipe special file
    D. A special Unix block or device file

CA B, page 2-33

16. Which of the following is **true** in regard to Unix file permissions?

    A. A user may run a file if he has execute permissions on it, although he may not have "read" permissions.
    B. The sticky bit is usually found on the world-accessible /etc directory.
    C. Changing ownership to world read-write-execute where possible enhances system security.
    D. None of these.

CA A, pages 2-35 and 2-37

17. When the **sticky bit** is set on a directory,

A. then only the owner of a given file may remove that file from the directory
B. the sticky bit overrides other settings, making the directory world read-write-execute.
C. users can run programs within that directory, but the **ls** command will not list the file names within that directory.
D. Both B & C.

CA A, page 2-37

18. For the security-minded Unix systems administrator, which of the following is the preferred **umask** setting?

A. 000
B. 022
C. 026
D. 077

CA D, page 2-39

19. The following is an excerpt of the output returned after issuing the command **df –k –F ufs** on a Solaris 2.6 server:

/dev/dsk/c3t0d0s0	482824	346037	136305	72%	/
/dev/dsk/c3t0d0s6	1986439	884956	1094862	45%	/usr
/dev/dsk/c3t0d0s4	963869	580975	381288	61%	/var
/dev/dsk/c3t0d0s5	5173094	1674748	1446616	33%	/opt
/dev/vx/dsk/qmgrs	1919976	256	1917801	1%	/var/mqm/qmgrs
/dev/vx/dsk/mqlogs	2006247	196771	807470	10%	/var/mqm/log
/dev/vx/dsk/opt2	3927264	2846313	1077024	73%	/opt2

The first column shows…

A. disk devices
B. file systems
C. NFS partitions
D. High Sierra partitions

CA A, page 2-43

20. **Termcap** and the **vi** editor originated in

A. Programmer's Workbench
B. 4BSD
C. AT&T versions of DEC Unix
D. Xenix

CA B, page 2-6

21. Which of the following is a **true** statement?

A. The **umakefs** command is used to dynamically generate more inodes when a file system is running low on inodes.
B. After using a file system for years, one can freely add inodes without worrying that the file system may be destroyed.
C. USENET news hierarchies are known for their efficient conservation of inodes.
D. The **df –i** command can be used to display the number of free inodes.

CA D, page 2-44

22. Which of the following is a **true** statement?

A. When used to rename a file, **mv** simply changes the file's name in the parent directory.
B. The **cp** command is preferred over the **mv** command when rotating files, to which data are being currently written.
C. One may use the **mv –R** command to move files recursively between file systems.
D. The use of **cp** decreases inode consumption.

CA A, page 2-46

23. Which of the following is a **true** statement?

A. Symlinks increment the link count.
B. **ln –s** is used to create a symlink.
C. **ln –h** is used to create a hard link.
D. A symlink must always point to an existing file.

CA B, page 2-49

24. What is the result of issuing the following command?

find /usr/sbin –mtime –1 –type –f –print

A. All objects in the /usr/sbin directory older than one day will be listed.
B. All objects of type file system one day old will be listed.
C. All objects of type file that have been accessed less than one day ago will be listed.
D. All objects of type file that have been modified less than one day ago will be listed.

CA D, page 2-63

25. To reduce the risk of attackers from cracking users' passwords and impersonating them, most Unix implementations now put encrypted passwords in…

    A. /etc/shells
    B. /etc/passwd
    C. /etc/shadow
    D. /etc/group

CA C, page 2-66

6.2 Common Issues and Vulnerabilities in UNIX Security

1. Tools available which can be used in place of standard re-usable passwords include

    A. IRC links and lsof
    B. Kerberos and one-time passwords
    C. NIS and NIS+
    D. NFS and AFS

CA B, page 8

2. Which of the following was **not** discussed in the SANS Unix security track at Monterey as a vulnerability with passwords?

    A. Biometrics
    B. Shoulder Surfing
    C. Social Engineering
    D. Exhaustive Guessing

CA A, page 7

3. Which of the following does **not** carry passwords over the network in clear text?

    A. telnet
    B. rlogin
    C. rsh
    D. ssh

CA D, page 10

4. According to the course materials, which of the following is a **false** statement?

    A. Never keep the passwords in an electronic file longer than you need for generating the password sheets.

B. The least likely place to find hand-written passwords is on shared-use types of PCs and terminals.
C. In a switched Ethernet network, each machine only sees the traffic on its leg of the switch.
D. True security from password sniffers is achieved only with strong encryption.

CA B, pages 11-13

5. In regard to password protection, which of the following is a **false** statement?

A. Use a permulation "algorithm."
B. Choose a password that's quick to type.
C. Choose password themes.
D. Choose a small font when printing a password sheet.

CA C, page 14

6. Which of the following is a **false** statement?

A. Most modern versions of Unix place encrypted passwords in the /etc/passwd file.
B. It is wise to train and encourage users to report suspicious email.
C. Where accounts are locked after a set number of failed login attempts, an attacker may practice denial of service attacks on user accounts.
D. Most systems tend to log login failures.

CA A, pages 15-17

7. Which of the following is a **false** statement?

A. Every Unix implementation allows the users to use any printable character(s) in their passwords.
B. Only the first eight characters of Unix passwords are significant.
C. The correct way for a system administrator to lock a user's account is to use an empty password string for that account in the password file.
D. A common method of cracking passwords involves "dictionary attacks."

CA C, pages 18, 21, 22

8. The file **/etc/passwd** in modern Unix implementations

A. contains login logs per user.
B. contains encrypted passwords.
C. is used for DNS primary server authentication.
D. is world-readable by default.

CA D, page 23

9. To prevent the user from changing his password and then immediately changing it back to his original password, implement

   A. password aging/history
   B. password expiration algorithms
   C. minimum password lengths and numeric/alphanumeric requirements
   D. none of these.

CA A, page 24

10. Which of the following is a **true** statement?

   A. OpenBSD provides no password hashing/encyption schemes and is considered a security nightmare.
   B. Commercial Unix variants, such as Solaris, provide adequate password hashing schemes, such as DES56.
   C. The **strings** command is useful in re-encrypting a cracked password file.
   D. A conscientious security administrator would prevent users from creating core (dump) files and/or periodically scan for and remove such files.

CA D, pages 25 and 27

11. Putting **ulimit** at the top of boot scripts

   A. is used to decrease the number of world-writable directories on a Unix server.
   B. is used to activate TCPWrappers.
   C. will prevent software developers from dumping core.
   D. may be used in preventing system daemons from dumping core.

CA D, pages 30-31

12. Which of the following would be of **least** priority when securing a system?

   A. removing /etc/hosts.equiv and removing .rhosts files from users' directories
   B. reducing the number of world-writable directories on a system
   C. reducing the volume of data the user may write to the system by establishing disk quotas
   D. maintaining 0-byte-length files per user (accessible only by that user) in world-writable mail directories

CA C, pages 31-32

13. Race conditions occur when an attacker

   A. exploits the improper use of symbolic links.

B. performs a recursive removal of files from world-writable directories.
C. creates a buffer overflow.
D. uses the time lag between two operations in an application.

CA D, pages 33-36

14. A buffer overflow type of attack would occur

A. when the attacker blows the memory stack.
B. when the attacker takes over a user's mail file, typically in /var/mail or /var/spool/mail.
C. when the attacker gets passwords and/or other sensitive data from extraneous core files.
D. when a sniffer captures user account and password information across the network.

CA A, pages 34-38

15. An effective method of reducing the likelihood of a buffer overflow attack would include

A. defensive programming – exhaustive validation of user input strings.
B. deploying recent OS patches pertaining to vendor-specific security advisories.
C. guarding against "exec()" embedded in data entry strings.
D. all of these.

CA D, pages 39-40

16. Which of the following is a **true** statement?

A. Normal program instructions reside in the read-only area at the top of memory.
B. Well-behaved programs usually execute code in the of memory stack.
C. Buffer overflow attacks usually result in removing /etc/shadow.
D. One may modify the kernel to prevent programs from executing instructions in the stack area.

CA D, page 45

17. The ___ is a mechanism in Unix, which allows unprivileged users the ability to run certain programs with higher than normal privileges.

A. sticky bit
B. set-UID bit
C. entry **set noexec_user_stack=1 (entry in /etc/system)**
D. entry **set MAXUSER = n (entry in /etc/system)**

CA B, pages 44-45

18. In reference to an historic exploit which used the **expreserve** executable, which of the following is **false**?

    A. Resetting the IFS environment variable to equal tab was part of this exploit.
    B. It utilized a set_UID to root security hole.
    C. It took advantage of the Unix mail utility.
    D. It involved creating a couple of small files usually in the /tmp directory to gain privileged access.

CA A, pages 48-49.

19. From a security point of view, which of the following is **false**?

    A. Any set-UID program that opens arbitrary files without checking the path is suspicious.
    B. Scripts which use full path names but don't set PATH are often susceptible to IFS type of attacks.
    C. Secure programming includes unsetting the environment variables sent to your program then setting the environment, which your program requires.
    D. When the kernel executes any set-UID programs, it logs user activity to the /var/adm/messages file.

CA D, pages 54-56

20. Which of the following is **false**?

    A. Setting up **chroot**() environments is often tedious and complicated.
    B. Many new versions of BIND allow you to run the name server under **chroot**().
    C. Daemons such as **syslogd** and **smtp** use **chroot**() naturally.
    D. Only root can do **chroot**().

CA C, pages 62-53

21. From a system security perspective, it's wise to

    A. rollout SSH.
    B. rollout NFS.
    C. build a dynamically linked **ls** program.
    D. share libraries.

CA A, pages 66, 115-120; Book 6.6 pages 1-32, 1-33, 1-35, and 1-115

22. When setting up a **chroot**() environment for anonymous ftp, it's important to

A. create some "stub" files under the anonymous ftp's /etc/directory.
B. make a full copy of the /etc/shadow under the anonymous ftp's /etc/directory.
C. make the files in the **chroot**()ed /etc/directory non-world readable.
D. make the **chroot**()ed /etc/directory world read/write/executable.

CA A, page 68

23. Which of the following is a **false** statement?

A. Anonymous ftp uploads require permission resets.
B. Never set the set-UID bit on the **chroot**() program.
C. Because it's vulnerable to exploits, the **ls** command should be periodically scrutinized.
D. Running your web and ftp servers on the same server is highly secure.

CA D, pages 70-73

24. Which of the following is a **false** statement?

A. It is generally wise to include the "." in root's path.
B. The most common use of the Trojan horse attack is to provide backdoors into already compromised systems.
C. Running the **strings** command on a suspicious binary may reveal a Trojan horse method of login.
D. Always type full pathnames when running as root.

CA A, pages 73-74

25. Which of the following is a **false** statement?

A. Attackers love to hide files in /dev.
B. The typical Trojan rootkit will deliver Trojan versions of **sudo**, **chmod**, and **ln** and any other command that an administrator might use during the normal course of his job.
C. Linux RPM utilities may be used to detect bogus binaries.
D. Rootkits are not designed to hide certain running processes.

CA D, pages 76-78

6.3 UNIX Security Tools and Their Uses

1. When acquiring a non-commercial security tool, peruse the source code for all of the following, **except**

A. reporting results to the email address(es) of the author(s).
B. measures that would prevent buffer overflow problems.
C. system calls which would reduce the risk of race conditions.
D. heavy use of **printf**(), **sprintf**(), and **strcpy**().

CA D, slides 7 & 8

2. Which of the following is a **false** statement? Because IP addresses can be spoofed

A. replace them with C-shell aliases globally.
B. if using DNS, make sure it has forward and reverse entries.
C. look up the name associated with the IP address.
D. look up the IP address associated with the name.

CA A, slide 11

3. Which of the following is a **false** statement?

A. Security-related programs should by statically loaded.
B. Settings of the **PATH**, **IFS**, and **LD_LIBRARY_PATH** environment variables should be scrutinized.
C. Report results over unencrypted email on the Internet.
D. Watch out for routines which don't check ranges.

CA C, slides 13-16

4. Which of the following is not a system-integrity scan?

A. tripwire
B. COPS
C. PGP
D. lsof

CA C, slides 18, 371, 373

5. Which of the following is a **false** statement?

A. The root user should not be allowed to come in via **ftp**.
B. Ensure that a "+" exists in /etc/hosts.equiv.
C. World-writable memory devices is a bad idea.
D. World-writable system logs (such as /var/adm/sulog) is a bad idea.

CA B, slides 23 and 27

6. Which of the following is a **false** statement?

A. Avoid having world-writable files within crontab.
B. Avoid world-writable rc files.
C. Avoid non-alphanumeric group names.
D. Avoid spaces in root's password.

CA D, slides 30, 32, 34

7. Part of its reporting includes a list of all world-writable directories.

A. lsof
B. COPS
C. Tirewarp
D. Tripwire

CA B, slide 36

8. COPS reports on all of the following, **except**

A. anomalies in /etc/passwd.
B. anomalies in /etc/group.
C. unusual permissions on scripts such as .cshrc.
D. whether root exists in /etc/tftpusers.

CA D, slides 35, 37, 40, 43

9. Which of the following would weaken a system's security?

A. the sanitation of /etc/group
B. the removal of root from /etc/ftpusers
C. setting permissions to 444 on /etc/password
D. disabling **rexd**() as an **inetd** service

CA B, slide 41; book 6.4 page 12

10. Which of the following would strengthen a system's security?

A. Ensure that anonymous ftp is part of group wheel.
B. Ensure that users' home directories are strictly primary group writable.
C. Use Tripwire to check file integrity.
D. Increase the number of set-UID applications.

CA C, slices 48, 51; book 6.1 page 2-75

11. COPS will not

A. compare dates on programs with dates of known buggy versions.

B. remove duplicate accounts encountered in /etc/passwd.
C. check for files with set-UID and set-GID attributes.
D. check for directories with blanks in their names.

CA B, slides 37, 51-52

12. Which of the following is a **false** statement?

A. Use *carps* if interested in COPS summary reports.
B. If you run COPS twice on the same day, it will overwrite its previous output.
C. COPS is one of the newest Open Source system integrity tools.
D. COPS cannot be used in a DEC Ultrix environment.

CA C, slides 53-59, 60, 64

13. As a result of numerous computer system break-ins at Texas A & M, ____ was developed.

A. Tiger
B. COPS
C. Robbers
D. lsof

CA A, slide 65

14. Two configuration files, _____ and _____ need to be set up before running Tiger.

A. site-sample and tigerrc
B. /etc/inetd.conf and /etc/syslog.conf
C. /etc/tiger.system /etc/tiger.home
D. tiger-get-hosts and tiger-automount

CA A, slide 67

15. Environment variables **TIGERHOME**, **TIGERWORK**, **TIGERLOGS**, and **TIGERBIN** need to be defined for Tiger in

A. a tiger-get-hosts rc script.
B. a Makefile.
C. a tiger-checksums file.
D. none of these.

CA B, slide 68

16. Tiger may be configured to check all of these, **except**

A. symbolic links
B. device files
C. DES encryption models
D. problems based on architecture

CA C, slides 66, 71, 72, 105

17. ____ were originally contributed to the Open Source community by folks at Purdue University.

A. COPs and PGP
B. ufsdump and Tiger
C. lsof and Tripwire
D. dd, tar, and cpio

CA C, slides 115 and 165

18. Get and utilize ___ if interested in file system integrity.

A. sudo
B. chroot
C. tripwire
D. rcs

CA C, slides 116, 328, 386 [book 6.2 chroot pages]

19. The entry **!/usr/spool** in the *tw.config* file means

A. "remove files in /usr/spool."
B. "store reporting information in /usr/spool."
C. "ignore /usr/spool."
D. "report on the file system capacity of /usr/spool."

CA C, slide 118

20. The SANS Unix course recommends that when running Tripwire,

A. use all 9 checksums against your file systems.
B. remove Crack and PGP due to compatibility issues.
C. watch out for and prevent core dumps.
D. establish your parameters in the *tw.config* file.

CA D, slides 118, 121-122

21. ___ , written in Perl, has the purpose of analyzing and reading log entries and then executing commands based on those entries.

A. PGP
B. Swatch
C. Tripwire
D. COPS

CA B, slides 20, 116, 139, 373

22. ____ provides digital signatures.

A. PGP
B. Swatch
C. Tripwire
D. COPS

CA A, slides 20, 116, 139, 373

23. _____ is useful in keeping track of who did what.

A. Logcheck
B. Lsof
C. RCS
D. Crack

CA C, slides 152, 166, 386, 392, 401

24. _____is handy if you're looking for hidden, local files (with a link count of 0).

A. Logcheck
B. Lsof
C. RCS
D. Crack

CA B, slide 172

25. _____ is an implementation of one-time passwords.

A. PGP
B. ISS
C. Watcher
D. S/Key

CA D, slides 182, 199, 373, 428

6.4 Running UNIX Applications Securely

1. Which of the following is a **false** statement?

   A. Because ftp is a recent product, a default installation is highly secure.
   B. WU-FTPD, sendmail and procmail have all been exploited with corrupt **printf**() formats leading to stack attacks.
   C. OpenBSD has been diligent in auditing their security problems.
   D. Use of TCP Wrappers can improve security.

CA A, pages 5, 7, 13

2. Which is **false**?

   A. In Linux, the **anonftp** package sets up proper permissions.
   B. List only the users and groups necessary in /etc/passwd and /etc/group.
   C. Access to an FTP server for a company intranet can be limited with TCP Wrappers.
   D. One of the shortcomings of WU-FTP is its inability to support logs.

CA D, pages 17-18

3. Basic administration of a read-only FTP site is relatively free of security concerns, provided

   A. the anonymous FTP home directory is set up correctly and there are no world-writable permissions in the directory tree.
   B. the first field of each line of the /etc/passwd file has been copied into the /etc/ftpusers file.
   C. /etc/ftpusers is frequently audited for accounts such as bin, adm, sys and daemon.
   D. proper disclaimer and liability banners displayed after the login prompt.

CA A, page 19

4. Which is **false** in regards to file upload FTP sites?

   A. File upload FTP sites should be swept at lease once a day (whereby inbound files are moved elsewhere).
   B. WU-FTP has a number of holes which actually invite the setting up of a "where" site on an incoming directory.
   C. These sites are generally harder to secure than file download sites.
   D. Set the inbound files directory to permissions of 333.

CA B, pages 19, 21

5. Which is **true** in regard to file upload FTP sites?

   A. Give the FTP user a directory with read-write attributes only.
   B. Maintain WU-FTP attributes in the /etc/wu-ftpusers file.
   C. Ensure that a solid path-filter is in place for anonymous and guest accounts.
   D. Give the user an opportunity to delete the file(s) he uploaded.

CA C, pages 21-22

6. A strong WU-FTP path filter would

   A. prevent a file name from beginning with a dot or a hyphen.
   B. allow alphanumeric characters in any order for upload file names, but disallow nonprintable characters.
   C. limit the file name length
   D. limit the maximum number of white spaces in a file name to three.

CA A, page 22

7. If the WU-FTP file disposition for incoming files is defined as follows:

upload /home/ftp /incoming yes root ftp 0600 nodirs noretrive /home/ftp/incoming

then which of the following is **false**?

A. Files are owned by anonymous or guest.
B. Files receive a group ID of ftp.
C. Files cannot be deleted by the person doing the upload.
D. Files cannot be downloaded from the upload directory.

CA A, page 23

8. The Apache 1.3.x web server has two valuable files you should read before configuring the web server. They are

   A. apache.conf and apache.rc
   B. API and config.html
   C. README.configure and APACI
   D. /dev/random and /dev/urandom

CA C, page 30

9. The security modules of Apache web server are

   A. mod_random and mod_security

B. mod_deny and mod_access
C. mod_sec and mod_iss
D. mod_auth and mod_access

CA D, page 31

10. HTTP/1.1 Digest Authentication (RFC2617)

A. does anonymouns-FTP-style username/password authentication
B. handles basic allow/deny access control based on standard UNIX account administration.
C. is a challenge response system that sends MD5 hashes.
D. is authentication in name only – not *de facto* authentication.

CA C, page 31

11. What does http://localhost/manual provide?

A. access control settings for Apache web server
B. Apache web server's online documentation
C. Secure CGIs
D. The enablement of ScriptAlias

CA B, pages 33-34

12. To strengthen your web server's security,

A. improve performance by setting up URLs to ignore symlinks.
B. lock everyone out with *deny* then add on only those whom you explicitly allow.
C. allow users to execute CGI scripts from any directory.
D. scatter CGI scripts throughout the directory tree and name them something other than *.cgi.

CA B, pages 37, 39, 40.

13. Solid web design would include all of the following, **except**

A. allowing indexes to directories that don't have a default index page on a case by case basis.
B. using the *.https* extension on names of files which are server-parsed.
C. using the SymLinksIfOwnerMatch switch to prevent users from creating a link to root-owned sensitive files.
D. using overrides with care.

CA B, pages 40, 41, 42, 44

14. Secure web design would include all of the following, **except**

A. Make sure no one can request the .htaccess files in a URL.
B. Password protect directories containing sensitive data.
C. If there are only a few users that change sporadically, then building the password file with the *htpasswd* program one user at a time is usually OK.
D. The *AuthName*, or "Realm," is sparingly presented to the user as part of the prompt for username and password.

CA D, pages 44-47

15. Which of the following is a **false** premise in terms of secure web design?

A. Program with the following in mind: You can't trust a single thing that the users are telling you when they submit the forms and/or invoke the CGI scripts.
B. Keep web development on a separate server from the production web server.
C. When evaluating email addresses, metacharacters may be permitted in the input string.
D. Protect the CGI scripts from unauthorized alteration.

CA C, pages 48, 51, 53-34

16. In the context of limiting or securing CGI access by the public, which is **false**?

A. Protect CGI scripts from unauthorized alteration.
B. CGI scripts are run with the same UID/GID as the Apache server, typically this is the user "nobody."
C. "Nobody" typically owns one **chroot**()ed write directory – just one place to which user "nobody" may upload.
D. You might choose to run the Apache server under a dedicated UID/GID that has no other use and owns no files.

CA C, page 54

17. In the context of securing web scripts, which is **false**?

A. Purchase closed source scripts to save time in terms of testing.
B. If the script is written in Perl, check for the Perl "magic" characters in calls to **open**().
C. When testing CGIs try to break the scripts by entering bad data.
D. When installing third party CGIs, test them thoroughly in a controlled environment.

CA A., page 55

18. The Secure Socket Layer

A. is a weak protocol for authentication.
B. provides end-to-end encryption at the network socket level.
C. was first developed by Open Source.
D. is built into rlogin and telnet on most modern systems.

CA B, page 57

19. When you set your browser to http://www.sans.org, the Internet will look up the IP address for SANS Institute using the

A. Dynamic Naming System.
B. Domain Name Service.
C. NIS/NIS+ Internet Service.
D. YP Dictionary.

CA B, page 64

20. DNS

A. contains only hostnames and IP addresses.
B. may hold machine type and OS platform.
C. is used for authentication in conjunction with SSL.
D. Both A and B.

CA D, page 64

21. Information maintained on the **root name servers** on the Internet is maintained by

A. SANS Institute
B. the CERT organization at Carnegie Mellon University
C. the InterNIC
D. ISS

CA C, page 65

22. ___ has been the reference implementation for DNS on the Internet and is the basis for the DNS implementation provided with most modern operating systems.

A. Sendmail
B. BIND
C. AFS
D. NIS/NIS+

CA B, page 66

23. All of the following are DNS/BIND exploits discussed in the Unix Security course, **except**…

    A. An attacker may penetrate the interior of your network in an effort of making an anonymous attack on other Internet hosts.
    B. An attacker may break into your system by maximizing buffer overflow – particularly if you are running an older version of BIND.
    C. An attacker may embarrass an organization or exploit a trust relationship by poisoning a DNS name server's cache.
    D. An attacker may glean an organization's internal email routing in order to proceed with identity theft.

CA D, pages 67-68

24. Providing one set of server names and IP addresses to the public and keeping the rest of your organization's server names and IP addresses private is the theory behind

    A. *split-horizon* DNS.
    B. *root name servers.*
    C. *dynamic-cache* DNS.
    D. *secured-socket* DNS.

CA A, page 68

25. All of the following is true about BIND version 8, **except**

    A. It allows the administrator to change its version text field.
    B. It is possible to run two different name servers with different done databases on the same machine.
    C. It requires *split-horizon* DNS.
    D. It works with *slave forwarding name servers*, if desired.

CA C, page 69

BONUS QUESTION FROM BOOK 6.4

26. Which is **false**?

    A. A globally accessible anonymous FTP site doesn't have much use for TCP Wrappers.
    B. Lee Brotzman's gone broke paying out $20s to all who have provided him with solid reasons for not installing TCP Wrappers.
    C. A "guest" is an authenticated user who is then treated like an anonymous user.
    D. An anonymous user is one whose identity is truly not known.

CA B, pages 13, 15 …No one has provided Lee a valid reason. "Excuses" maybe.

Book 6.5 Linux Practicum

1. When installing a new OS on a machine, it's wise to do all of the following, **except**

A. Remove the machine from the LAN.
B. If you must install the OS on a machine connected to the LAN, then make sure it's on an isolated LAN.
C. Disregard the fact that network interfaces are active during the OS installation.
D. Strip down the OS by removing as many of the attacker-attractive tools as you can afford to easily live without.

CA C, page 6; plus book 6.6, pages 1-6, 1-26

2. If you absolutely *must* install a new Linux OS on a machine that's wide open to the Internet, then

A. Use **tcpdump** on another Linux box on the same network segment to monitor traffic to and from your new installation.
B. Perform a custom installation.
C. Plan your partitioning and swap requirements.
D. Make sure the root partition is within the first 1024 cylinders of the drive when setting up dual-boot computers.

CA A, pages 6-8

3. Which of the following is **false**?

A. A web server needs more space for */home*, where the Web page are kept.
B. The general rule for calculating how much swap space you need is to multiply the amount of physical memory by two.
C. There are three sets of standard Linux partitioning rules; pick your favorite of the three.
D. Samba and NFS are examples of file servers.

CA C, pages 8-9

4. Which of the following is **false**?

A. As a general rule, install "X windows" because it's light on resources.
B. The installation of Linux workstation packages can be appropriate for business, software development, and even general purpose workstations.

C. The installation of Linux server packages should be limited to the machine's specific purpose(s).
D. The fewer the number of services installed on a server, the greater its performance and tighter its security.

CA A, pages 10-11

5. Which of the following is **false**?

A. MD5 cryptographic hashing is faster to compute than **crypt**() hashing.
B. Putting Unix encrypted passwords in /etc/shadow is an improvement over putting them in /etc/passwd.
C. The /etc/passwd file is world-readable.
D. Make your Unix passwords 7 or 8 characters and really hard to guess.

CA A, page 12

6. The Red Hat GUI for OS installations is

A. Meinconf
B. Linuxconf
C. Unixconf
D. Webmin

CA B, page 15

7. A handy browser-based tool for installing Caldera OpenLinux and a range of services including BIND, NFS, and Samba is

A. Meinconf
B. Linuxconf
C. Unixconf
D. Webmin

CA D, page 16

8. Which of the following is a **true** statement?

A. In SYSV **init** is process 0 and all other processes descend from it.
B. The configuration file for **init** is /etc/init.conf.
C. On many flavors of Linux, the default runlevel is set in the "id" parameter of the **init** configuration file.
D. Upon installing Linux, remove the # (comment symbol) in the following code of the **init** configuration file:

```
#ca::ctrlaltdel:/sbin/shutdown –t3 –r now
```

CA C, pages 17-18

9. What do the "**S**" and "**K**" characters symbolize in symlink files found in /etc/rc.d/rc?.d?

   A. "System" and "Kernel" calls.
   B. "Sum" (for checksum on binaries) and "Korn" for Korn in lieu of Bourne shell.
   C. Start and Kill.
   D. None of these

CA C, page 19

10. Which of the following is **false**?

   A. At its most basic level, an **init** script has to be able to handle the arguments "start" and "stop."
   B. Probably the easiest way to write an **init** script is to start with a copy of an existing one.
   C. Directories within /etc/sysconfig (in example, /etc/sysconfig/network) will contain **init** script support data.
   D. Remember to change login programs when altering password encryption, and/or imposing access and/or resource limits.

CA D, pages 21-22

11. All modern distributions of Linux use ___ to perform authentication services.

   A. PAM
   B. **crypt**()
   C. Tivoli
   D. **sum**()

CA A, page 22

12. Which of the following is **false** in regard to Linux-based PAM files found in /etc/security?

   A. time.conf contains ranges when users can log in.
   B. login.conf contains user parameters such as password aging specifications.
   C. access.conf identifies who may log in to this machine.
   D. limits.conf provides maximum number of processes, stack size, CPU time, and file sizes a user may have.

CA B, page 24

13. Which of the following is **false**?

A. Each of PAM's /etc/security files uses the colon (":") as a field delimiter as in the /etc/passwd file.
B. The time.conf file includes complex "logic lists" of "!" (unary not), "&" (logical and), or "|" (logical not).
C. The command **chage –l username** is used to list the basic information (such as password aging) of a given account.
D. The /etc/login.defs file is where default global settings are found.

CA A, pages 25-29

14. In regard to the Linux environment, which of the following is **false**?

A. The /etc/syslog.conf file contains parameters for both syslogd and klogd.
B. Red Hat uses the rotatelog program to rotate logs (by default once a week).
C. The Linux sysklog package follows the basic syntax of other BSD-style syslog packages.
D. When configuring Red Hat for log rotation, activate the *compress* option in the appropriate configuration file.

CA B, pages 30-33

15. In regard to Linux and log files, which of the following is **false**?

A. The log server must be secure.
B. An advantage to creating non-standard log files is that the "script kiddies" may overlook them.
C. For log file compression, be sure to set the compress attribute in both the /etc/logrotate.conf and /etc/syslog.conf files.
D. The loghost should run no other services except syslog and perhaps SSH for remote administration.

CA C, pages 34-36

16. Under which circumstances would you want to add an "-r" attribute in the /etc/rc.d/init.d/syslog init script?

A. when you'd like to automate the removal of log files older than one week
B. when you'd like to accept log messages from remote hosts
C. when you'd like to rotate logs
D. when you'd like to "readjust" log rotation to a monthly basis

CA B, page 37

17. If you chose to add a service to your log server,

A. NTP for synchronizing the machine's clock would be a strong candidate.
B. FTP would fit well with a log server because it requires lots of disk storage.
C. Procmail may fit in nicely.
D. Elect for document imaging.

CA A, page 39

18. Which of the following is a **false** statement?

A. Limit the number of hosts sending messages to the loghost server to 512 or less.
B. Log messages are sent on UDP.
C. The loghost must be sufficiently sized to process and store all the logs.
D. UDP can handle any number of connections.

CA A, page 40

19. Which is **false** in regard to the Linux kernel?

A. Little hardware knowledge is required of the person performing the compilation.
B. The kernel version numbering convention is major.minor.release.
C. The "stable" kernel series has even-numbered minor numbers.
D. The "development" kernel series had odd minor version numbers.

CA A, pages 41-42

20. Which of the following is **not** a valid interface for Linux kernel compilation?

A. make xconfig
B. make menuconfig
C. make config
D. make winconfig

CA D, page 43

21. Which of the following is **false**?

A. Never delete your backup kernel that you know works until you are sure you have a working replacement.
B. During the kernel build process, you may sometimes skip the "clean previous objects" step.
C. Once you've gone through the "config" stage, you'll end up with the following file, /usr/src/linux/.config.
D. The first step in compiling the kernel is actually building the dependencies.

CA B, pages 43 and 46

22. **RPM** is

A. Red Hat's kernel configuration program.
B. Red Hat's package add facility.
C. Candera's auto-download of latest revisions facility.
D. OpenBSD's kernel name.

CA B, page 49

23. Which of the following is a **false** statement?

A. To qualify for checking Red Hat's priority.redhat.com you must register a perchased version of the software of buy a subscription service.
B. *Up2date* can be configured to get it's updated from authorized Red Hat servers.
C. By default *Up2date* only displays only those packages that update something you have already installed.
D. Red Hat has a free anonymous ftp site.

CA C, pages 49-52

24. Which is a **false** statement?

A. If no services are allowed in /etc/inetd.conf, you can just turn it off by stopping the service and removing it from the SYSV init startup sequence.
B. If you absolutely need an inetd service, use TCP wrappers to restrict access.
C. TCP wrappers are standard issue with Linux, and comes, by default, with /etc/hosts.allow populated.
D. If no match is found in either /etc/hosts.allow or /etc/hosts.deny then access is allowed.

CA C, pages 62-63

25. In terms of enhancing system security, which is a **false** statement?

A. Replace the Berkeley LRPng with **lpr**/**lpd**.
B. The system call, **netstat**, can be used to "nmap" ports that are open and "listening" for connections.
C. For Red Hat Linux, you can easily disable the links from the runlevel directories by editing the /sbin/config program.
D. Red Hat Linux uses "kernel-space" NFS.

CA A, pages 66, 68, 70, 76

Book 6.6 Solaris Practicum

1. Which of the following servers were **not** discussed in this course as applications for Secure Hosts?

   A. NFS and NIS servers.
   B. Web and Anonymous FTP servers.
   C. Mail Gateway and Database servers
   D. Kerberos and Bastion Host/Proxy Servers

CA A, page 1-4

2. Which of the following is a **false** statement?

   A. An organization's security policy should include commentary with regards to internal spoofing of IP source addresses.
   B. Security is a technology decision.
   C. Security concepts for deploying Internet servers may be equally relevant in the deployment of Intranet servers.
   D. It is important for organizations to publish (at least internally) their security policy.

CA B, pages 1-4 and 1-5

3. Which of the following is a **false** statement?

   A. When using Jumpstart to build Solaris servers, put the servers on a private subnet.
   B. It is preferable to install the Solaris OS on a new machine *off*, rather than *on*, the network.
   C. Once a secure server is built on the organization's Intranet, it need not be monitored against attacks.
   D. There are documented cases of hosts being attacked within 5 minutes of being connected to an external network.

CA C, pages 1-5, 1-13.

3. Which of the following is a **false** statement?

   A. When building a system, which is intended for the network, in a stand-alone environment, go ahead and configure it for the network during the OS installation.
   B. If you bought a machine with Solaris pre-installed, it is preferable to secure that image as opposed to re-installing the OS.
   C. As a rule, elect security over convenience.
   D. When concerned with securing the machine, one should install the smallest OS possible.

CA B, pages 1-14 through 1-16

4. When installing Solaris with security in mind, which of the following would be **false**?

   A. Select the largest cluster available for installation.
   B. The smallest cluster for installation may still contain dangerous services.
   C. Without installing the SUNWter package, remote administration may later provide "heartburn."
   D. Sun provides four cluster-install choices -- full, developer, end-user, and core.

CA A, pages 1-16 and 1-17

5. Which of the following is a **false** statement?

   A. Solaris 2.x systems require as much swap space as physical memory.
   B. When building a general-purpose machine, install the core cluster and selectively add functionality.
   C. When building an Internet bastion host, install the core cluster.
   D. The course suggests putting third-party software in the /local file system.

CA A, pages 1-17, and 1-18

6. Which of the following is **false**?

   A. Install only what you need.
   B. For ease in later remote administration, consider adding X server packages on your secure machine.
   C. Save two partitions to encapsulate and mirror the root drive when using Veritas Volume Manager.
   D. If setting up X, consider using SSH to forward secure X sessions to your local machine.

CA B, pages 1-18 and 1-19

7. Which of the following packages does Sun's SE Performance Monitoring tool require?

   A. SUNWsprot
   B. SUNWvxva
   C. SUNWlibCf
   D. SUNWnptr

CA A, page 1-19

8. Which of the following is a **false** statement?

A. Solaris **pkgadd** will not install patches on your system, if the packages, to which the patches belong, have not been installed.
B. If downloading packages from a Sunsolve ftp site, it's wise to run an MD5 checksum on the patch cluster files.
C. The Solaris **pkgadd** utility prohibits the use of shell wildcards.
D. */var/sadm/install/contents* not only lists everything installed, but also provides a cross reference between specific files and the packages to which they belong.

CA C, pages 1-20, 1-22, 1-23, 1-24

9. If you install only the *core system* of Solaris 2.6 and afterwards **patchadd** fails, what do you probably need to do.

A. Change all **grep** references in the script to point to */usr/bin/grep*.
B. Set the set-UID sticky bit on the script.
C. Look to see whether the objects are in *.tar.Z versus *.zip format
D. Get the latest Solaris2.6 PatchReport and research the issue therein.

CA A, pages 1-23 through 1-25

10. Which of the following is **false**?

A. On Solaris 7 and Solaris 8, you may disable the */etc/rcS.d/S50devfsadm* symlink if you wish to prevent the hot-pluggable device daemons from running.
B. One typically finds the BSD Unix /etc/rc* scripts under the /etc/init.d directory in SYSV Unix.
C. SYSV boot scripts are written to take either "start" or "stop" as acceptable arguments.
D. In SYSV environments the boot scripts physically reside in the /etc/rc[S0-3].d infrastructure and the symlinks reside in /etc/init.d

CA D, pages 1-27 and 1-28

11. Which if the following is a **false** statement?

A. Tuning tcp_conn_req_max_q0 can help protect the system against "SYN flooding attacks."
B. When editing the /etc/init.d/inetinit file, put all your settings at the end of the file.
C. Boot time scripts which do not end in .sh get executed in a subshell rather than in the environment of the parent init process.
D. Solaris provides no kernel parameters which may help in preventing "smurf" attacks.

CA D, pages 1-30, 1-31, 1-33

12. To replace **telnet**, **ftp**, and **rlogin**,

A. turn on IP forwarding.
B. create /etc/notrouter and reboot.
C. enable DHCP first.
D. install ssh.

CA D, pages 1-32, 1-33, 1-35

13. What does the following establish when found in the **/etc/inittab** file?

sc:234:respawn:/usr/lib/saf/sac –t 300

A. It sets up system accounting.
B. It disables the login prompt.
C. It unlinks /etc/inetd.conf (which is typically linked to /etc/inet/inetd.conf).
D. It sets up the listener for serial ports.

CA D, pages 1-36 and 1-37

14. Which of these is **false**?

A. Static routing is preferred to unauthenticated dynamic routing.
B. Because the /etc/nsswitch.conf configuration takes effect immediately, create the /etc/resolv.conf file first (when setting up for DNS resolution).
C. The syslogd daemon is a known gateway for intrusion attacks.
D. Replace the Solaris binaries with the newest version of BIND.

CA C, pages 1-37, 1-39 and 1-40

15. Which of the following is the likeliest Trojan Horse replacement candidate if an unauthorized person has gained root access on your machine?

A. /usr/lib/sendmail
B. /usr/bin/login
C. /usr/sbin/cron
D. fsflush

CA B, pages 1-38, 1-40, 1-42

16. Which of the following is **false**?

A. Ensure that the root, /usr and /var file systems have a mount option of yes in /etc/vfstab.
B. If possible, run sendmail occasionally from cron rather than continuously.
C. To switch a file system from read-write to read-only, one must reboot.
D. Never apply the nosuid option to special file systems such as /tmp.

CA A, pages 1-40, 1-43, and 1-44.

17. Which of these if **false**?

A. During the standard boot process, the "/" (root) file system is not mounted until the /ect/vfstab file is read.
B. In Solaris, nosuid implies nodev.
C. In Solaris one cannot separate /devices from the "/" (root) partition.
D. Avoid mounting **chroot**()ed file systems as nosuid.

CA A, pages 1-44 and 1-45

18. Which of the following is a **true** statement?

A. **ssh** supports only Kerberos authentication.
B. **ssh** sends logins and passwords in clear text.
C. **ssh** provides an **rdist** replacement which allows administrators to securely update files.
D. **ssh** can not deny network access based on IP address.

CA C, pages 1-48 through 1-50

19. Which of the following is a **false** statement?

A. TCP Wrappers is great for controlling network sessions.
B. TCP Wrappers can only filter on IP addresses and is, therefore, no replacement for authentication.
C. The general rule for administering TCP Wrappers is: List a few "ok" hosts in hosts.allow and then deny everything in hosts.deny.
D. The default TCP Wrappers configuration file is /etc/sshd_config.

CA D, pages 1-51, 1-54, and 1-56

20. Which of the following is a **true** statement?

A. With RSA public key encryption, passwords must still be sent over the wire.
B. If your public key is stolen, someone may masquerade as you.
C. Reusable encrypted passwords are uncrackable.
D. Similar to /etc/passwd, **ssh** and TCP Wrappers configuration file must be world-readable.

CA B, pages 1-57 through 1-60

21. Which of the following is **incorrect** in setting up system accounting?

A. Ensure that the SUNWaccr and SUNWaccu packages are fully installed.
B. Reset the default shell for user sys with:
   # passmgmt –d sys
C. Uncomment appropriate lines in /etc/init.d/perf.
D. Edit /var/spool/cron/crontabs/sys by un-commenting appropriate lines and initialize the logs with /etc/init.d/perf start. Then reboot.

CA B, pages 1-63, 1-72

22. Which of the following is a **false** statement?

A. Never allow remote login as root.
B. Make the /etc/ftpusers file mode 600 owned by root.
C. Before enabling process accounting, ensure that the SUNWpacct packages is fully installed.
D. The /etc/syslog.conf file contains records which are strictly *tab* delimited.

CA C, pages 1-62, 1-64, 1-66, 1-75

23. Which of the following is a **false** statement?

A. If you do not set the EEPROM password, then an attacker who gets root access to your machine can set the password, set the secuirty-mode to full, and reboot your machine.
B. The system cannot reboot without a human operator if the following is in effect:
   # eeprom security-mode=full
C. The umask may be set in /etc/profile and /etc/.login.
D. Add # to the beginning of the UMASK line in /etc/default/login to globally set the umask.

CA D, pages 1-80 through 1-82

24. Which of the following would prevent an attacker who has access to your computer room from inserting a ufs-formatted floppy disk into your server and running a set-UID script from it?

A. The creation of /etc/default/telnetd with the following entry:
   BANNER=””
B. The creation of /etc/default/ftpd with the following entry:
   BANNER=””
C. Having the following entry in /etc/rmmount.conf:
   mount ufs –o suid
D. Adding the following entry to /etc/system:
   set ufsfloppy:nosetuid = 0

CA C, pages 1-79, 1-84, 1-85

25. From a security perspective, which of the following is an **invalid** statement?

A. Verify backups by restoring.
B. Networked backups are superior to local backups, because local backups require an operator to change the tapes.
C. If the r-commands are enabled (Berkeley rlogin, rsh, rcp), remove the rhosts_auth lines from pam.conf. The system will disregard .rhosts authorization.
D. Even if **ftpd** isn't running, it wouldn't hurt to have a populated /etc/ftpusers file.

CA B, pages 1-86, 1-97, 1-98

Book: Network Time Protocol (Unix@Night)

1. The Internet standard time synchronization protocol is

A. sync
B. fsck
C. NTP
D. SMTP

CA C, page 4

2. The **NTP** distribution comes with an …

A. ntpdate program
B. rdate probram
C. rdist program
D. ntptimer

CA A, page 4

3. The **ntpdate** program can be used on client machines

A. at boot time.
B. to be called from cron at administrator-determined intervals.
C. to be run in daemon mode.
D. all of these

CA D, page 4

4. From a security perspective, time synchronization across the serves is important because

A. log file timestamps need to be consistent.
B. SecurID is a time-based product.
C. Kerberos is a time-based product.
D. All of these.

CA D, page 5

5. Which of the following is a **false** statement?

A. NTP ports across a wide range of platforms.
B. NTP v4 is being developed for the first time for PCs.
C. The current Internet standard of NTP is v3, commonly know as "XNTP."
D. NTP is a distributed, hierarchical system.

CA B, pages 4-6

6. Which of the following is a **false** statement?

A. The stratum of a server is one plus the lowest stratum value of any server it is actively synching with.
B. Time variance between the client and the NTP server is known as drift.
C. NTP servers are only configured peer-to-peer.
D. To prevent a prospective time hijack by an attacker, your server must be receiving updates from more than one external clock source.

CA C, pages 11-13

7. Which of the following is a **false** statement?

A. When a time server disconnects, it falls to "stratum 18."
B. NTP allows for the definition of pseudo clocks for redundancy.
C. Having several pseudo-clocks per site will prevent a single inaccurate machine from distorting your network time.
D. None of these.

CA A, pages 11 and 19

8. Which of the following is a **false** statement?

A. Pseudo-clocks should generally be configured at strata 5-8.
B. Routers are inappropriate devices for NTP server configuration.
C. Setting up a router as an NTP server could increase its impact as a single point of failure.
D. Configure your pseudo clocks so that they do not interfere with your real clock synchronization.

CA B, pages 19 and 21

9. Which of the following is a **false** statement?

   A. Although NTP servers may be configured for broadcasting time, this should be avoided.
   B. Running NTP is daemon mode is less accurate than running it from cron.
   C. Most vendor-supplied operating systems come packaged with NTP v3.
   D. The Open Source NTP distribution is easy to set up.

CA B, pages 22 and 24

10. Which of the following is a **false** statement.

    A. The /etc/ntp.conf file generally holds drift data.
    B. The driftfile directive specifies the full pathname of the file where NTP should store data regarding drift.
    C. It is good business practice to contact the administrator of each external clock server which you intend to access.
    D. None of these

CA A, pages 12, 27, and 28

Book: Secure Shell (SHH) (Unix@Night)

1. **SSH** is

   A. a secure replacement for **sendmail**.
   B. a secure replacement for **rlogin**, **rsh**, and **rcp**.
   C. a one-time-password encryption service.
   D. all of these.

CA B, page 5

2. **SSH** provides

   A. a data compression option, but it's only really useful over slow speed links.
   B. several encryption options.
   C. a replacement of the "r-commands" virtually transparent to the user.
   D. all of these.

CA D, pages 5 and 6

3. Which of the following was **not** an example of **SSH** usage discusses in this course?

A. SSH securing remote access from a conference
B. SSH working with backups and file distribution
C. SSH working with CDE.
D. SSH working with tools (such as **rdist**, **rsync**, **buffer**, **socket**, **ftpsshd**, **ppp**)

CA C, pages 42-49

4. Which of the following is a **false** statement?

A. SSH is compatible with X Windows.
B. SSH is compatible with Kerberos.
C. SSH will forward X11 over the encrypted channel.
D. SSH was developed by the X Windows consortium.

CA D, pages 5, 7, 13

5. When **SSH** is configured to user **tcp_wrappers**, entries for this are made in

A. ssh.conf
B. wrappers.conf
C. hosts.allow and hosts.deny
D. rsa.conf and wrappers.conf

CA C, page 14

6. **SSH** uses _____ to initialize a secure connection.

A. Kerberos
B. SecurID
C. rhost resolution
D. RSA public key/private key

CA D, page 17

7. Which of the following is **false**?

A. Keep /etc/ssh_known_hosts up to date.
B. It is possible to install SSH binaries on an NFS partition.
C. SSH is usually run under inetd.
D. The SSH **configure** mechanism has many options.

CA C, pages 23-25

8. Steve Acheson recommends …

A. compile SSH with IDEA.
B. compile SSH with RSA.
C. compile SSH with blowfish.
D. compile SSH with KNEESOCKS.

CA C, pages 26 and 27

9. To **minimally** invoke **ssh** as an end user, which of the following would work:

A. ssh
B. ssh *hostname*
C. ssh –l *myacct hostname*
D. sshd

CA B, page 35

10. When **SSH** is compiled with Wietse Venema's **tcp_wrappers**,

A. It adds several options to the /etc/hosts.allow and /etc/hosts.deny files.
B. It purges its configuration (so it is wise to keep a spare copy of your configuration files before proceeding).
C. Running SSH under inetd becomes a requirement.
D. All of these.

CA A, page 39

Book: One-Time Passwords (Unix@Night)

1. Which of the following is a **false** statement?

A. X Windows is highly secure and not a likely candidate for one-time passwords.
B. Many BSD-derived systems keep the encrypted version of your password in a world-readable file.
C. Most users choose terrible passwords and don't change them often.
D. If an attacker captures and OTP response in transit, it won't do him any good.

CA A, pages 4 and 5

2. Two factor authentication

A. usually refers to a slice of time during which a password is valid.
B. typically includes a hardware device and a secret key (or PIN).
C. is standardized with the Berkeley "r-commands."
D. requires biometrics and a PIN.

CA B, page 7

3. Which of the following is a **false** statement?

   A. There are generally two types of hardware tokens supplied by commercial OTP vendors.
   B. Challenge/Response tokens generate unique passwords every 30-60 seconds.
   C. Users generally prefer synchronous to challenge/response devices.
   D. RSA authentication is an example of public-key-based authentication.

CA B, pages 8 and 9

4. One-Time Passwords are currently being developed as freeware under the name

   A. FreeOTP
   B. Bellcore
   C. OPIE
   D. ActivCard

CA C, page 11

5. The dominant commercial OTP vendor is currently

   A. Defender
   B. ActivCard
   C. SafeWord
   D. SecurID

CA D, page12

6. Which of the following is a **false** statement?

   A. OTP is typically deployed at an organization's dial-in pools and Internet/VPN access points.
   B. Public-key based systems can be integrated in a fairly transparent fashion into most applications.
   C. Users may require a lot of hand-holding when OTP is initially rolled out.
   D. The use of one-time-passwords fits well with automatic login scripts.

CA D, page 13

7. Once Bellcore went commercial with their OTP product, __ picked up on the open development of OTP.

   A. SecurID

B. OpenBSD
C. the Navy Labs
D. Warner Brothers

CA C, page 15

8. Which of the following if a **false** statement?

A. The OPIE system has a per-machine /etc/opiekeys file which holds an encrypted form of the user's secret plus a random seed value and a decrementing counter.
B. If the user's counter drops to zero, the user cannot log in.
C. Users' secrets come pre-set with the initial OPIE installation.
D. OPIE secrets can be generated in advance.

CA C, pages 17 and 18.

9. Which of these is **false**?

A. OPIE uses the Red Hat autconf mechanism, so building the package is usually easy.
B. **opielogin**, **opieftpd**, and **opiesu** are drop-in replacements for their OS counterparts.
C. OPIE will accept standard Unix passwords when you log in at the system console.
D. The manual installation of OPIE is preferred over the automated one.

CA A, pages 19 and 20.

10. Which of these is **false**?

A. During the OPIE installation process, keep a root shell available at your console.
B. Because it contains OPIE secrets, think of /etc/opiekeys as you would /etc/shadow and make it mode 644.
C. Never allow anonymous root logins.
D. Mac and Window OPIE calculators automatically manipulate the cut'n'paste buffer for the user.

CA B, pages 20-21 and 23

Book: Kerberos (Unix@Night)

1. Which of the following is a **false** statement?

A. Kerberos is a "trusted 3rd party" authentication protocol.
B. Kerberos uses shared secret DES key encryption.

C. Kerberos was designed for SNA protocol in OLTP database environments.
D. Kerberos was designed for TCP/IP networks.

CA C, page 3

2. Which of the following is a **false** statement?

A. Kerberos authentication is based on the idea of a "shared secret."
B. Kerberos authentication takes place over an encrypted channel.
C. Kerberos Encryption is limited to 56DES.
D. All Kerberos authentication takes place between clients and servers.

CA C, pages 3, 5, and 9.

3. The term "Kerberos server" generally refers to the

A. Key Distribution Center (the KDC).
B. Dynamic Key Allocator (the DKA).
C. Source Code Administrator (the SCA).
D. SANS Network Administrator (the SNA).

CA A, page 5

4. Kerberized programs that clients communicate with using Kerberos tickets for authentication are known as the

A. security server.
B. application server.
C. Kerberos control center.
D. principal key server.

CA B, page 5

5. Which of the following is a **true** statement?

A. The primary weakness of Kerberos is that the ticket is subject to spoofing.
B. Each principal shares a key with a paired principal.
C. "Credentials" refers to one authenticated ticket.
D. The KDC must be in a secured environment.

CA D, pages 5, 6, 12, and 13

6. For initial user authentication, ____ is typed by the user.

A. login (rlogin, or rsh)
B. kinit

C. telnet
D. gokerb

CA B, page 18

7. What is the **TGT** in Kerberos vernacular?

A. It's the Ticket Granting Ticket.
B. It's the Telnet Galvanized Ticket.
C. It has lost its meaning as an acronym, yet it refers to the Pre-authentication Server.
D. It's a toggle switch, which creates two tickets and sends one back to the client.

CA A, pages 14 and 22

8. Which of the following is a **true** statement?

A. A Kerberos system must contain only one Realm.
B. Kerberos provides no protection of transmitted data.
C. Kerberos is not compatible with API.
D. Kerberos does not protect against denial of service attacks.

CA D, pages 26, 39, and 40.

9. Kerberos mailing lists are available at whose web site?

A. SANS Institute
B. M.I.T.
C. Red Hat
D. OpenBSD

CA B, page 42

10. Which of these is a **false** statement?

A. Kerberos is designed to provide secure authentication over insecure networks.
B. Kerberos replaces your local binaries for **login**, **ftp**, **su**, and **telnet**.
C. Kerberos authentication is based on a "shared secret" that is never transmitted in clear text over the network.
D. Kerberos is based in symmetric-key cryptography.

CA B, pages 3 and 40.

Book: Unix Forensics (Unix@Night)

1. Which of the following most adequately reports login-logout history?

A. /var/log/utmp
B. /var/log/wtmp
C. /var/adm/messages
D. /etc/login

CA B, page 74

2. Which of the following may be used to capture network status, file status, as well as process information?

A. inetd
B. netstat
C. lsof
D. ifconfig

CA C, pages 41-43

3. What would the following command provide?

find / \(-perm –004000 –o –perm –002000 \) –type –f > report.txt

A. report all hidden files and recently modified binaries
B. extract suspicious entries in /etc/passwd
C. report anything "out of the ordinary" and concatenate shell histories into report.txt
D. list set-UID and set-GID files in report.txt

CA D, pages 84 and 88

4. Once a computer compromise has occurred, the caveat to the rapid action required of the incident handling team to investigate and recover is…

A. The process of how to investigate a Unix-based computer is clearly defined.
B. It's nearly impossible to collect evidence in a thorough manner.
C. The submission of evidence to the court is a straightforward and easy process.
D. The process of gathering logs changes the state of the computer.

CA B, page 10

5. Which of the following are **least likely** to be Trojaned?

A. telnet, in.telnetd
B. login, su, ftp
C. ls, ps, netstat, ifconfig
D. /etc/syslog.conf, /etc/rmmount.conf

CA D, page 12

6. Which of the following is a **false** statement in regard to the Linux rootkit, lrk version 5?

A. This kit trojanized numerous files such as passwd, killall, netstat, and ifconfig.
B. The tcpd daemon was unaffected in this exploit.
C. The rootkit altered syslogd and inetd.
D. The rootkit left all the Berkeley "r-commands" intact.

CA B, pages 14-18

7. Preparation as a step in Unix forensics includes all of these, **except**:

A. training
B. toolset comprised of dynamically linked libraries
C. preparing for the worst and administering accordingly
D. toolset comprised of basic binaries (such as find, ls, ps, and the like)

CA B, pages 21-15

8. In the hypothetical incident discussed in this course, which of the following was **not** part of the compromise?

A. The attacker leaves a toolkit trail.
B. Running a secure **truss** on system calls showed kernel alterations.
C. Some logs on the compromised host were either altered or removed.
D. A remote user's ID was sniffed due to his unsecured remote access from a conference.

CA B, pages 29-31, 33

9. Based on the six steps of incident handling discussed further in the course, what's your first step once you are notified that a machine may have been compromised?

A. Identification.
B. Containment.
C. Eradication.
D. Recovery.

CA A, page 32

10. Which of the following is **not** a basic premise of the Unix Forensics course?

A. Avoid restoring the system from backups if the backups themselves could hold compromised files.
B. Take detailed notes, possibly utilizing the Unix **script** command.
C. Gather evidence in the following order, if possible: disk blocks, network connections, file system, then memory and processes.
D. Use a safe toolkit when recovering the system (e.g., if possibly, boot to CD-ROM and set the environment to utilize safe binaries and libraries).

CA C, pages 38-39