UNIX CERTIFICATION PRACTICAL

AMANDA HYATT

November 2000

61Questions (Unix Basics for the Security Professional)

1.)Who can use the passwd command? 6.1 p.2-36

a.) Only root can change passwords.
b.) Normal users can issue the command to change their own password.
c.) No one can use it, until Sudo or RBAC is configured to allow it.
d.) Both A and B are correct.

Correct answer: D

2.) A file with permissions of 640 allows: 6.1 p.2-35

a.) The *owner, group* and *other* (world) can each READ the file, but only the *owner* can modify the file.
b.) The *owner, group* and *other* (world) can each read and modify the file.
c.) The *owner* can read and modify the file, the *group* can read the file and *other* has no permission.
d.) The *owner* has read, write and execute permission, the *group* has read and write permission.

Correct answer: C

3.)A directory with permissions of 640 allows: 6.1 p.2-37

a.)Only the *owner* can get directory listings (ls) and create/remove files within the directory.
b.)The *owner* can get directory listings (ls) and create/remove files within the directory. and *group* can get directory listings (ls). Other has no access.
c.)All can get directory listings, but only the owner can create and remove files from the directory.
d.) None of the above.

Correct answer: B

4.) What does applying the "Sticky Bit" to a directory do? 6.1 p.2-37

a.)Grants One-time write access to a directory by a user who has only read permissions.

b.)Keeps users from adding files to the directory.
c.)Hides files with certain permission sets from being seen when a user attempts to view files within the directory.
d.)Allows only the owner of a given file to remove the file from the directory. This is especially helpful on Group or World-writeable directories.

Correct answer: D

5.) What command is used to change permissions on a file or directory? 6.1 p.2-39

a.)chmode
b.)chmod
c.)perm
d.)chown

Correct answer: B

6.) What command can be used on a directory so that new files and programs created within the directory will be created with non-standard permissions? 6.1 p.2-39

a.) unmask
b.) mask
c.) umask
d.) chmod

Correct answer: C

7.) To turn off ALL bits except those which apply to the owner of the file dbfile: 6.1 p.2-39

a.) chmod 644 dbfile
b.) chmod 755 dbfile
c.) chmod 700 dbfile
d.) chmod 600 dbfile

Correct answer: D (because I specified file NOT program)

8.)The df -k command displays what information? 6.1

p.2-43

a.) "disk free"- the available space in kilobytes of currently mounted file systems.
b.) The total partition size.
c.) The space used.
d.) All of the above.

Correct answer: D

9.) The inode stores which time value relating to the file? 6.1 p.2-44

a.) last modified time (seen with ls -l)
b.) last accessed time (seen with ls -lu)
c.) last time the inode information for the file was modified (seen with ls -lc)
d.) All of the above.

Correct answer: D

10.)The inode change time will be updated by which of the following: 6.1 p.2-46

a.)The ownership of the file changes
b.)The permissions of the file changes
c.)The file is accessed.
d.)Both A and B

Correct answer: D

11.)Which of the following commands will keep the existing inode for 'file' when copying to or renaming as 'newfile'? 6.1 p.2-46

a.) cp file newfile
b.) mv file newfile (simply renaming the file within the same directory)
c.) mv file /otherdir/newfile (renaming & moving file to another directory but on the same partition)
d.) Both B and C

Correct answer: D

12.) With a umask of 022 on a directory, the newly created files within it will have the following permissions: 6.1 p.2-39

a.) 644 (regular files), 755 (program)
b.) 640 (regular files), 755 (program)
c.) 600 (regular files), 750 (program)
d.) 640 (regular files), 777 (program)

Correct answer: A

13.)Which types of links allow the files being linked to share the same inode? 6.1 p.2-49

a.) Symbolic link
b.) Hard link
c.) Both
d.) Neither

Correct answer: B

14.)Which command would you use to view 'hidden' files (files that begin with a ".")? 6.1 p.2-51

a.) ls -l
b.) ls -A
c.) ls -a
d.) ls -b
e.) Both B and C

Correct answer: E (ls -A shows the same thing as ls -a with the exception of the working and the parent directory).

15.)How can the command grep be used to perform case insensitive matches? 6.1 p.2-55

a.) grep -i
b.) grep -c

c.) grep -v
d.) grep -nocase

Correct answer: A (For example #grep -i security /export/home/Solarissec will find all instances of the word security regardless of case (i.e. security, SECURITY, Security) within the file Solarissec)

16.)How can you view text (any printable characters, 4 characters or longer) from the binary file /usr/local/sbin/sshd? 6.1 p.2-57

a.) strings /usr/local/sbin/sshd
b.) more /usr/local/sbin/sshd
c.) cat /usr/local/sbin/sshd
d.) vi /usr/local/sbin/sshd

Correct answer: A

17.)To view only the last 800 lines of the file /var/adm/messages, you could: 6.1 p.2-59

a.) more /var/adm/messages
b.) cat /var/adm/messages
c.) head 800 /var/adm/messages
d.) tail -800 /var/adm/messages

Correct answer: D

18.)Appropriate uses for the find command are: 6.1 p.2-63

a.) find / -name Netscape
b.) find /dev -type d
c.) find /etc -mtime -3
d.) all of the above

Correct answer: D

19.)Which file contains the users encrypted password on a Solaris system? 6.1 p.2-67

a.) /etc/hosts
b.) /etc/shadow
c.) /etc/passwd

d.) /etc/users

Correct answer: B

20.)Which of the following are true pertaining to groups? 6.1 p.2-67

a.) Users can be assigned to a group via useradd, usermod or admintool.
b.) The groups command will display which groups you belong to.
c.) Users may be assigned to additional groups within the file /etc/groups.
d.) Both A and C.
e.) All of the above.

Correct answer: E

21.)Which passwd option can an administrator use to force someone to change their password upon next login? 6.1 p.36

a.) -f
b.) -e
c.) -c
d.) none of the above

Correct answer: A

22.)Which passwd option would be used to set the expiration date of a users password? 6.1 p.36

a.) -e
b.) -f
c.) -t
d.) -d

Correct answer: E

23.) Which file contains the users encrypted password on a SunOS system? 6.1 p.2-67

a.) /etc/hosts
b.) /etc/shadow
c.) /etc/passwd
d.) /etc/users

Correct answer: C

24.)Which file defines the specific users shell? 6.1 p.2-67

a.) /etc/shells
b.) /etc/shadow
c.) /etc/passwd
d.) /etc/users

Correct answer: C

25.)Which file could tell you how many days are left before the password will expire? 6.1 p.2-67

a.) /etc/expire
b.) /etc/shadow
c.) /etc/passwd
d.) /etc/users

Correct answer: B

6.2 Common Issues and Vulnerabilities in UNIX Security

26.)Which of the following programs sends the login password in clear text? 6.2 p.10

a.) ssh
b.) scp
c.) telnet
d.) hotmail

Correct answer: C

27.)Among the following, which is the most secure "hub" that you could use to interconnect all of your systems and minimize the possibility of password sniffing (of LOCAL traffic): 6.2 p.11

a.) hub
b.) ethernet switch (layer 2 switch)
c.) ip switch (layer 3 switch)
d.) bridge

Correct answer: C

28.)If a "password sheet" must be used, which of the following would be a good rule to follow: 6.2 p.13

a.) limit the distribution of the password sheet and if possible, keep it under lock and key.
b.) write all of the passwords backwards next to the corresponding hostname.
c.) use a small algorithm to change out certain letters/numbers (change the letter "o" to a "0" zero or the letter "i" to a "1" one). But don't write the algorithm down!
d.) both A and C.
e.) All of the above

Correct answer: D (not E because it is NOT a good idea to include hostnames on the sheet, plus simply reversing the passwords is too easy).

29.)The first two characters of an encrypted password are not actually part of the encrypted password. Rather, these 2 characters are used to permute the encrypted password, yielding numerous encryption results from the same password. These 2 characters are called: 6.2 p.16

a.) sugar
b.) trick
c.) mix
d.) salt

Correct answer: D

30.)Password cracking programs use which of the following in an attempt to de-encrypt a password? 6.2 p.22

a.) standard dictionaries
b.) dictionaries developed to include non-standard words, titles, names, etc.
c.) hints about a given user (i.e. birthday, automobile, girlfriends' name, etc.)
d.) all of the above.

Correct answer: D

31.)When a users password has been configured with a password aging of 5 days, what will happen at 5 days? 6.2 p.25

a.) the password will expire
b.) the password may now be changed
c.) 5 days worth of password changes will be logged
d.) all of the above

Correct answer: B

32.)The standard UNIX password hashing algorithm is: 6.2 p.25

a.) 56-bit
b.) 128-bit
c.) 192-bit
d.) 256-bit

33.)A process owner can generating a core file by killing a process 6.2 p.29
with which kill option?

a.) 9
b.) HUP
c.) QUIT
d.) all of the above

Correct answer: C

34.)A hacker might be interested in running strings against a core file 6.2 p29
because ____________ might be obtained.

a.) encrypted passwords
b.) PATH information
c.) file contents
d.) all of the above

Correct answer: D

35.)How can a Solaris system administrator configure 6.2 p.30
their system to NOT generate core files?

a.) add the following line to the /etc/system file: set sys:coredumpsize = 0
b.) putting the following command in the .cshrc file: limit coredumpsize 0
c.) putting the following command in the .profile file: ulimit -c 0
d.) all of the above are correct, A is system-wide B and C configure
on a per user basis.

Correct answer: D

36.)Where might a hacker be most likely to hide a root kit? 6.2 p.76

a.) in /dev
b.) in /
c.) in the user's home directory
d.) in the .profile file

Correct answer: A

37.)A user listed in hosts.equiv is allowed to: 6.2 p.85

a.) log in as himself
b.) not log in at all
c.) log in a any user on the system
d.) none of the above

Correct answer: C

38.)The .rhosts file can be configured to: 6.2 p.86

a.) Allow universal access with a '+'
b.) Allow access to ANY user on a host with only a hostname listed.
c.) Allow access to a specific user on a host with the hostname followed by the user.
d.) All of the above.

Correct answer: D

39.)It is recommended that all of the "r" commands (rlogin, rcp and rsh) be replaced with: 6.2 p.100

a.) telnet and ftp
b.) ssh
c.) skip
d.) all of the above

Correct answer: B

40.)On a Solaris system _______ is responsible for "registering" sun-specific, rpc services to a port number at boot. 6.2 p.103

a.) rpcbind
b.) rpcmap
c.) binder
d.) mapperd

Correct answer: A

41.) On a SunOS system _______ is responsible for "registering" sun-specific, rpc services to a port number at boot. 6.2 p.103

a.) rpcbind
b.) rpcmap
c.) portmap
d.) mapd

Correct answer: C

42.)Well known services have _________ ports and rpc services have ___________ ports. 6.2 p.103

a.) fixed, random
b.) fixed, fixed
c.) random, fixed
d.) anonymous, random

Correct answer: A

43.)To disable a service, you must:

a.) Comment it out of the /etc/inetd.conf file and kill -HUP inetd.
b.) Modify a startup script so that it will not ever run a particular service.
c.) Remove the daemon.
d.) All of the above are correct. It is important to remember a service may be called upon in a start-up script or waiting for the 'mother daemon inetd to call upon it, so that you remember how to disable it.

Correct answer: D

44.)A Classic Trojan Horse had which of the following characteristics: 6.2 p.73
a.) It preyed on a user having a "." in the search path.
b.) It was named after commonly used commands such as 'ls' or 'su'

c.) Might be named after a typical typo to the commonly used commands. For example 'lsd' or 'ifcnofig'.
d.) A and B
e.) all of the above

Correct answer: E

45.)Which of the following would provide the most accurate information when trying to determine if a file has been tampered with? 6.2 p.80

a.) file size
b.) last modified date
c.) checksum
d.) viewing the few line of a file

Correct answer: C

46.)Comparison of the original checksum of that file and a new checksum can be accomplished: 6.2 p.80

a.) manually with the use of commands such a 'sum' and 'cksum'
b.) with applications such as Tripwire
c.) with SSH
d.) with both A and B
e.) all of the above

Correct answer: D

47.)An administrator can require a user to change his password upon next login with the command: 6.2 p.24

a.) login -f
b.) passwd -f user1
c.) passwd -lock user1
d.) passwd change user1

Correct answer: B

48.)The default minimum password length on most UNIX systems is: 6.2 p.24

a.) 6 character min. for regular users, no limit for root
b.) 6 character min. for all users
c.) 8 character min. for regular users, 2 character limit for root
d.) 4 character min. for all users.

Correct answer: A

49.)If password aging were used, then a user: 6.2 p.24

a.) must keep their password for the configured # of days or weeks.
b.) must get rid of their password immediately.
c.) must increase the length of their password each time it is changed.
d.) none of the above.

Correct answer: A

50.)For an entire system, password aging, password history and minimum password length may be configured: 6.2 p.24

a.) within the /etc/passwd file
b.) within the /etc/system file
c.) within the /etc/default/passwd file
d.) it cannot be configured for an entire system.

Correct answer: C

61UNIX Security Tools and Their Uses

51.)COPS when run with default settings will check for all of the following except: 6.3 p.20

a.) check the umask value
b.) look for a '.' in root's path.
c.) look for a '.' in normal users path.
d.) check for a '+' in the /etc/hosts.equiv file
e.) check for root in ftpusers

Correct answer: C

52.) COPS is similar to what other tool? 6.3p.20

a.) ASET
b.) Satan
c.) Saint
d.) Skip

Correct answer: A

53.)Which Tripwire file contains the list of files whose integrity is to be checked? 6.3 p.118

a.) tw.config
b.)config.parse
c.)tripwire.conf
d.)twconvert

Correct answer: A

54.)Tripwire helps a system administrator : 6.3 p.116

a.) determine if there were any unexpected or unauthorized changes to a file.
b.) track and report when users login to the system.
c.) automatically fix problem files
d.) all of the above.

Correct answer: A

55.)A list of attributes to be used and attributes to be ignored are listed next to each file to be checked in the tw.config file. What would we be looking for with the following attributes: +imu5 ? 6.3 p.121

a.) internal, modification time, up time, scan 5 times
b.) inode, modification time, up time, scan 5 times
c.) inode, modification time, owner of the file, checksum (MD5)
d.) inode, modification time, up time, checksum (MD5)

Correct answer: C

56.)If you wanted Tripwire to NOT use any checksum techniques, last access time, or size of the file you would include ______. 6.3 p.121

a.) -12as
b.)012345678a
c.)-012345678as
d.)-cas

Correct answer: C

57.)Of the following applications, which one can see what processes are looking at what files: 6.3p.167

a.)lsof
b.)losf
c.)ls
d.)ps -ef | grep < >

Correct answer: A

58.)What command would you use to find WHAT processes the file, AUTHLOG open? 6.3 p.171

a.) lsof AUTHLOG
b.) losf AUTHLOG
c.) open AUTHLOG
d.) whodo AUTHLOG

Correct answer: A

59.) What command would you use to find who is connected to you using SSH? 6.3p .174

a.) lsof SSH
b.) lsof -i :ssh
c.) lsof -i ssh
d.) losf -open ssh

Correct answer: B

60.)Which command would you use to find who is connected to port # 21? 6.3p.174

a.)losf -port 21
b.)lsof -p :21
c.)lsof -i :21
d.)losf -open 24

Correct answer: C

61.)With lsof, what command will tell you what NFS Files are mounted? 6.3 p.175

a.) lsof -mount
b.) lsof -N
c.) lsof -M
d.) losf -open NFS

Correct answer: B

62.)With lsof, what command will list ALL open UNIX sockets? 6.3 p. 178

a.) lsof -open
b.) losf -open
c.) lsof -U
d.) lsof -u

Correct answer: C

63.)Which UNIX command indicates who is currently logged in (on the local net)? 6.3 p.211

a.) rup
b.) rusers
c.) who
d.) whodo

Correct answer: B

64.)When using the application SATAN, to scan a remote systems ports 32767 and up, you would run SATAN with a: 6.3 p.237

a.) heavy scan
b.) medium scan
c.) stealth scan
d.) light scan

Correct answer: A

65.)Which application might detect SATAN scans? 6.3 p.247

a.) Courtney
b.) Saint
c.) another host running SATAN
d.) none of the above

Correct answer: A

66.)An nmap TCP FIN scan is also known as: 6.3 p.257
a.) open connect scan
b.) 'stealth' scan
c.) almost complete TCP handshake
d.) raw scan

Correct answer: B

67.)An nmap TYP SYN scan is also known as: 6.3 p.257

a.) 'stealth' scan
b.) open connect scan
c.) half-open scan
d.) none of the above

Correct answer: C

68.)With nmap, what command would find UDP ports with listeners on zonker.wal? 6.3 p.269

a.) nmap -sU zonker.wal
b.) nmap -UDP zonker.wal
c.) nmap -UL zonker.wal
d.) nmap -o UDP zonker.wal

Correct answer: A

69.)How would you conduct a ping scan on network 128.50.1.0 with nmap? (assuming the last octet is used for hosts) 6.3 p.274

a.) ping all 128.50.1.0
b.) nmap -o ping net 128.50.1.0
c.) nmap -sP 128.50.1.1-254
d.) nmap -sP 128.50.1.*
e.) both C and D

Correct answer: E

70.)As a target for the ping scan you could use: 6.3 p.275

a.) hostname
b.) ip address
c.) ip addresses with wildcard (*)
d.) ip addresses with "/" netmask notation
e.) all of the above

Correct answer: E

71.)With nmap, which option can be used to 'guess' the OS type using the TCP sequence numbers? 6.3 p.276

a.) -O
b.) -Seq
c.) -OS
d.) -T

Correct answer: A

72.)With nmap, if you want to set your source port to something (perhaps DNS port 53) what option would you use? 6.3 p.276

a.) -p
b.) -sp <port number>
c.) -g <port number>
d.) -port <port number>

Correct answer: C

73.)With TCP WRAPPERS implemented, you can block access with the use of which file: 6.3 p.304

a.) /etc/hosts.deny
b.) /etc/hosts.allow
c.) /etc/hosts.noaccess
d.) /etc/hosts.tcpdeny

Correct answer: A

74.) With TCP WRAPPERS implemented, you can allow limited, controlled access with the use of which file(s): 6.3 p.304

a.) /etc/hosts.deny with ALL :ALL (default deny ALL services to ALL hosts) plus the use of the /etc/hosts.allow configured with specific services and hosts that can use those services.
b.) /etc/hosts.allow with ALL :ALL with the use of /etc/hosts.deny to specifically block certain hosts
c.) /etc/hosts.noaccess
d.) /etc/hosts.tcpdeny

Correct answer: A

6.4 Running Unix Applications Securely

75.)Which of the following is an example of a common DNS server security threats? 6.4 p.67

a.) Unauthorized hosts obtaining a zone transfer.
b.) Cache attack (also known as cache poisoning)
c.) Buffer overflow attacks.
d.) All of the above

Correct answer: D

76.)Which of the following options in the named.conf file would provide some security for your DNS server? 6.4 p.84

a.) version "some bogus version number or character string"
b.) allow-transfer { 128.50.1.2; 128.50.3.12}
c.) allow-query or allow-recursion { 128.50/16}
d.) all of the following.

Correct answer: D

77.)What is the file that can be created to define the u sers who may NOT log in via ftp. 6.4 p.12

a.) /etc/ftpaccess

b.) /etc/ftplimit
c.) /etc/ftpusers
d.) /etc/ftpstop

Correct answer: C

78.)The main ftp configuration file that defines the number of simultaneous ftp users, permitted file operations and classes of users based on source address? 6.4 p.12

a.) /etc/ftp.conf
b.) /etc/ftpaccess
c.) /etc/ftpusers
d.) /etc/ftphosts

Correct answer: B

79.)fptd is started, by default, by: 6.4 p.13

a.) the 'mother daemon' inetd
b.) a start-up script
c.) named
d.) none of the above

Correct answer: A

80.)What could you do to improve performance of an ftp server that is heavily used? 6.4 p.13

a.) log all sessions
b.) start ftpd from a run control script so that it does not have to continually be launched every time there is a connection request. The down side is that tcp wrappers can't be used.
c.) limit the number of simultaneous users.
d.) Both B and C

Correct answer: D

81.)What could you do to make your ftp server more secure? 6.4 p.12

a.) implement TCP Wrappers with and use /etc/hosts.deny file configured with

ALL :ALL and an /etc/hosts.allow configured with the specific services and host that can use those services listed.

b.) Do not allow anonymous or guest access - remove them from /etc/ftpaccess.

c.) Use the ftp configuration files: /etc/ftpusers to define who may not and /etc/ftphosts to define who may access the ftp server.

d.) None of the above.

e.) All of the above.

Correct answer: E

82.)Which of the following is not a common Sendmail problem or vulnerability? 6.4 p.108

a.) cache attack
b.) forged e-mails
c.) buffer overflows
d.) back doors
e.) address attacks

Correct answer: A

83.)Some could forge an email by doing the following: 6.4 p.109

a.) telnet <mailserver> 25
followed by: **mail from:** bogusname@domain.com
rcpt to: john@msnbc.com
data
(bogus header info message ending with a '.')
b.) mconnect (followed by the above listed steps).
c.) breaking into someone's e-mail account and sending mail as if you were them.
d.) All of the above.

Correct answer: D

84.)A typical Buffer Overflow attacks on a Sendmail server might: 6.4 p.113

a.) create core dumps that can be analyzed later to look for the contents of the shadow file.

b.) remove all sendmail configuration files.

c.) cause a denial of service.
d.) both A and C

Correct answer: D

85.)In addition to listening on port 25, the Sendmail daemon is also responsible for: 6.4 p.125

a.) Filing mail into users custom folders.
b.) Periodically flushing mail from the mail queues.
c.) Notifying a user that new mail has arrived.
d.) None of the above.

Correct answer: B

86.)What statement within the Sendmail.cf file would allow mail to appear to be from the domain 'mydomain.com' ? 6.4 p.128

a.) FEATURE (use mydomain.com)
b.) MASQUERADE (mydomain.com)
c.) MASQUERADE_AS (mydomain.com)
d.) MAIL_AS (mydomain.com)

Correct answer: C

87.)What directive within the Sendmail.cf file would tell Sendmail to ook in the Sendmail.cw file for a list of domains that are considered to be local? 6.4 p.128

a.) FEATURE (use_cw_file)
b.) FEATURE (use sendmail.cw)
c.) FEATURE (use_domain_file)
d.) define (use_cw_file)

Correct answer: A

88.)Which of the following is a real option within the Sendmail.cf file but not a good idea for internal mail servers? 6.4 p.130

a.) FEATURE (accept_unqualified_senders)
b.) FEATURE (promiscuous_relay)
c.) Both A and B

d.) Neither A or B

Correct answer: C

89.)Which of the following Apache files handles HTTP basic authentication? 6-4 p.31

a.) mod_access
b.) mod_auth
c.) mod_auth_anon
d.) mod_auth_db

Correct answer: B

90.)Which of the following Apache files handles the basic allow/deny access control? 6-4 p.31

a.) mod_access
b.) mod_auth
c.) mod_auth_anon
d.) mod_auth_db

Correct answer: A

91.)Which of the following Apache files enables basic authentication with the username/password authentication? 6-4 p.31

a.) mod_access
b.) mod_auth
c.) mod_auth_anon
d.) mod_auth_db

Correct Answer: C

92.)Apache supports Digest Authentication in addition to Basic Authentication. Which of the following is a true statement? 6-4 p.45

a.) Digest Authentication sends MD5 hashes instead of clear text.
b.) Basic Authentication sends passwords in the clear.
c.) If Digest Authentication was used, the clients would have to support it as well.
d.) None of the above.
e.) All of the above.

Correct answer: E

93.)Which of the following is a correct statement regarding SSL (Secure Socket Layer)? 6-4 p.57

a.) It encrypts each packet through the TH (Transport Header)
b.) It encrypts only the DATA portion of a packet/frame.
c.) It encrypts each packet through the IH (IP Header)
d.) It performs no encryption, only authentication.

Correct answer: A

94.)Which of the following is a correct statement regarding SSL? 6-4 p.57

a.) Both ends of a connection MUST support SSL.
b.) SSL performs only encryption.
c.) SSL performs on authentication.
d.) SSL uses public key encryption as an authentication method.
e.) Both A and D.

Correct answer: E

95.)A general rule of thumb in deciding which version of an application to install is to... 6-4 p.57

a.) always upgrade to the latest version, vendors release only more secure versions than the prior.
b.) visit sites such as www.securityfocus.com before upgrading to determine if there are any known weaknesses in the newer versions.
c.) visit your OS vendors site, to determine if they support the new version of BIND, DNS, Sendmail, etc.
d.) Both A and B.
e.) Both B and C.

Correct answer: E

96.)Assuming that you have an /etc/hosts.deny file (with TCP Wrappers) configured with ALL :ALL (deny ALL services to ALL hosts), how would you allow a host named bugsy.com to use ALL services? 6.3 p.310

a.) Within the /etc/hosts.allow have the line: ALL : bugsy.com
b.) Within the /etc/hosts.deny have the lines: ALL : ALL : bugsy.com EXCEPT
c.) do NOT have an /etc/hosts.deny file
d.) none of the above.

Correct answer: A

97.)If you wanted to warn an intruder that they are entering a secure system you could implement ________ with TCP Wrappers. 6.3 p.317

a.) warnings
b.) alerts
c.) banners
d.) none of the above

Correct answer: C

98.) With regard to question 97, where would you configure this option? 6.3p.317

a.) With the following structure in either (or both) /etc/hosts.allow and/or /etc/hosts.deny: service : hosts : banners /path-to-bannersfile

b.) With the following structure in either (or both) /etc/hosts.allow and/or /etc/hosts.deny:
service : hosts : include banners /path-to-bannersfile

c.) With the following structure in either (or both) /etc/hosts.allow and/or /etc/hosts.deny:
service : hosts : "message to be displayed"

d.) all of the above would work.

Correct answer: A

99.)With the application sudo, which file is used to specify <u>who</u> can have superuser privilege and using <u>which</u> commands. 6.3 p.331

a.) sodoers

b.) sudoers
c.) sudo.config
d.) sudoer.cf

Correct answer: B

100.) Which editor can you use with sudo, that will do a syntax check on your main configuration file? 6.3 p.336

a.) vi
b.) xedit
c.) visudo
d.) visio

Correct answer: C

61Linux Practicum

101.) One of the options during installation of Red Hat Linux is the use "shadow" passwords with or without which hashing algorithm? 6.5 p.12

a.) MD5
b.) MD3
c.) MD4
d.) you have no choice but to use the default crypt() algorithm.

Correct answer: A

102.) Which control flag within the pam.conf file indicates that success of this module satisfies the application that this module type has succeeded; no additional 'required' modules are invoked? 6.5 p.23

a.) required
b.) sufficient
c.) requisite
d.) optional

Correct answer: B

103.) Which control flag within the pam.conf file indicates that success of this module is necessary and all remaining modules of 6.5 p.23

the same type are still executed.

a.) required
b.) sufficient
c.) requisite
d.) optional

Correct answer: A

104.) What is true of the MD5 hashing algorithm? 6.5 p.12

a.) it takes longer to compute than crypt ()
b.) it is not compatible with some password cracking programs
c.) it is more secure than crypt()
d.) all of the above

Correct answer: D

105.) Which of the following is not one of the pam.conf module types? 6.5 p.23

a.) auth
b.) session
c.) monitor
d.) password

Correct answer: C

106.) Which of the PAM module configuration files limits who has access to the system? 6.5 p.24

a.) /etc/who.conf
b.) /etc/security/pam.conf
c.) /etc/security/access.conf
d.) /etc/allow.conf

Correct answer: C

107.) Which of the PAM module configuration files limits what users are allowed to do (i.e # of active processes, file sizes, etc.)? 6.5 p.24

a.) /etc/security/whodo.conf
b.) /etc/security/limits.conf
c.) /etc/security/access.conf
d.) /etc/allow.conf

Correct answer: B

108.) Which of the PAM module configuration files would be be used if you wanted to permit logins only between 8:00 a.m 5:00 p.m. (for example)? 6.5 p.24

a.) /etc/security/time.conf
b.) /etc/security/limits.conf
c.) /etc/security/access.conf
d.) /etc/login.conf

Correct answer: A

109.) On a Linux system, what command would list expiration, aging, history etc. of a user's account? 6.5 p.28

a.) usermod
b.) chage -l username
c.) change -l username
d.) passwd -l

Correct answer: B

110.) Where would you configure default global settings of minimum and maximum number of days a password must be/can be used? 6.5 p.29

a.) /etc/default/passwd
b.) /etc/default/login
c.) /etc/default.defs
d.) /etc/login.defs

Correct answer: D

111.) Where would you configure default global settings of minimum maximum allowable UID values? 6.5 p.29

a.) /etc/default/passwd
b.) /etc/default/login
c.) /etc/default.defs
d.) /etc/login.defs

Correct answer: D

112.) Red Hat uses which daemon for logging kernel messages? 6.5 p.30

a.) kerneld
b.) klogd
c.) syslogd

d.) kdlog

Correct answer: B

113.) Red Hat uses which daemon for logging system messages? 6.5 p.30

a.) kerneld
b.) klogd
c.) syslogd
d.) kdlog

Correct answer: C

114.) Which file is used to configure which types of events are logged and where they are logged? 6.5 p.31

a.) /etc/syslog.conf (the same file used on most Unix systems)
b.) /etc/ksyslog.conf
c.) /etc/sysklog.conf
d.) none of the above

Correct answer: A

115.) With regard to question 114, what is the format of entries in this file? 6.5 p.31

a.) facility.level action
b.) level.facility action
c.) action facility.level
d.) action level.facility

Correct answer: A

116.) Which main configuration file does Red Hat use to set WHEN log files are to be rotated, how many back logs to keep and whether or not to compress the backlogs? 6.5 p.32

a.) /etc/logk.conf
b.) /etc/logrotate.d
c.) /etc/logrotate.conf
d.) /etc/klog.conf

Correct answer: C

117.) If you create a new log file, what permissions should be assigned? 6.5 p.34

a.) chmod 777 newlog
b.) chmod 666 newlog
c.) chmod 660 newlog
d.) chmod 600 newlog

Correct answer: D (read & write by owner root)

118.) After making changes to the log configuration file, you must: 6.5 p.34

a.) restart the syslog deamon with # /etc/rc.d/init.d/syslog restart
b.) kill the syslog daemon
c.) kill -reset syslogd
d.) nothing..the syslog deamon will pick up on the changes to its' configuration file.

Correct answer: A

119.) What does a kill -HUP do to the kernel log daemon, klogd? 6.5 p.35

a.) it terminates the signal
b.) it forces klogd to terminate and then start again
c.) it re-reads the configuration file /etc/syslog.conf
d.) all of the above

Correct answer: A

120.) What does a kill -HUP do to the syslog daemon, klogd? 6.5 p.35

a.) it terminates the signal and does NOT restart the daemon
b.) it does nothing. kill -HUP does not work on a Linux system
c.) it re-reads the configuration file /etc/syslog.conf
d.) all of the above

Correct answer: C

121.) To disable inetd services, you would comment out the service(s) in which file? 6.5 p.61

a.) /etc/kinetd.conf
b.) /etc/inetd.conf
c.) /etc/inetdk.conf
d.) /etc/services

Correct answer: B

122.) With regard to question #121, what would you do immediately after commenting out the service(s)? 6.5 p.61

a.) reboot
b.) killall -HUP inetd
c.) nothing..the changes are discovered by inetd
d.) kill -all inet

Correct answer: B

123.) If no services remain in the configuration file, you should turn off inetd. How would you do this? 6.5 p.62

a.) kill -HUP inetd
b.) remove the inetd.conf file
c.) /etc/rc.d/init.d/inet stop
   /sbin/chkconfig inet off
d.) none of the above.

Correct answer: C

124.) Which netstat switch(es) will list ports that are listening as well as an additional column for process name/process id? 6.5 p.66

a.) netstat -id
c.) netstat -ni
d.) netstat -nr
d.) netstat -atp

Correct answer: D

125.) Which file specifies which directories are exported to clients?6.5 p.74

a.) /etc/share
b.) /etc/export
c.) /etc/exports
d.) /etc/shareto

Correct answer: C

6.6 Solaris Practicum

126.) Starting with Solaris 7, Sun is supporting hot-swappable devices (devices that can be added while the system is running) on enterprise-class systems. You can disable this capability by: 6.6 p.28

a.) removing /etc/rcS.d/S50devfsadm
b.) renaming /etc/rcS.d/S50devfsadm
c.) removing /etc/rc2.d/S50devfsadm
d.) A or B would accomplish this

Correct answer: D

127.) Which file will keep a multi-homed system (a system with more than 1 configured interface) from being a router? 6.6 p.31

a.) /etc/notrouter
b.) /etc/dontroute
c.) /etc/hostname.*[0-9]
d.) there is no file that will do this, you must use ndd commands

Correct answer: A

NOTE: the following 5 questions involve ndd parameters that are set relatively *conservatively (securely) by default. However, certain conditions might cause the settings to change. if you are concerned about them you could provide additional protection by adding these parameters to the /etc/init.d/inetinit script.*

128.) If you wanted to configure your system (at startup) to ignore ICMP redirects, what command would you add to the end of the /etc/init.d/inetinit script? 6.6 p.31

a.) ndd /dev/ip ip_ignore_redirect 1
b.) ndd -set /dev/ip ip_ignore_redirect 1
c.) ndd -set /dev/ip ip_ignore_redirect 0
d.) ndd -set /dev/tcp ignore_redirect 1

Correct answer: B (1 = true)

129.) If you wanted to configure your system (at startup) to NOT forward any source-routed packets what command would you add to the end of the /etc/init.d/inetinit script? 6.6 p.31

a.) ndd /dev/ip ip_ignore_src_routed 1
b.) ndd -set /dev/ip ip_forward_src_routed 1
c.) ndd -set /dev/ip ip_forward_src_routed 0
d.) ndd -set /dev/ip ip_dontforward_src_routed 1

Correct answer: C

130.) If you wanted to configure your system (at startup) to NOT forward any directed broadcast packets what command would you add to the end of the /etc/init.d/inetinit script? 6.6 p.31

a.) ndd -set /dev/ip ip_ignore_direct_packets 1
b.) ndd -set /dev/ip ip_forward_src_routed 1
c.) ndd -set /dev/ip ip_forward_direct_broadcst 1
d.) ndd -set /dev/ip ip_forward_directed_broadcasts 1

Correct answer: D

131.) If you wanted to configure your system (at startup) to NOT forward any packets (at all) what command would you add to the end of the /etc/init.d/inetinit script? 6.6 p.31

a.) ndd -set /dev/ip ip_ignore_all_packets 1
b.) ndd -set /dev/ip ip_forward 0
c.) ndd -set /dev/ip ip_forwarding 1
d.) ndd -set /dev/ip ip_forwarding 0

Correct answer: D

132.) If you wanted to configure your system (at startup) to limit the number of tcp connection requests to 768 what command would you add to the end of the /etc/init.d/inetinit script? 6.6 p.31

a.) ndd -set /dev/ip ip_conn_req_768
b.) ndd -set /dev/tcp tcp_conn_req_max_q0 768
c.) ndd -set /dev/tcp tcp_connection_req_max_q0 768
d.) ndd -set /dev/ip tcp_connection_req_max_q0 768

Correct answer: B

133.) To limit the possibility of ARP spoofing attacks, you could decrease the amount of time cached entries live in your ARP table to 60 seconds from the default of 20 minutes by adding what command(s) to the end of the /etc/init.d/inetinit script? 6.6 p.31

a.) ndd -set /dev/ip ip_ire_flush_interval 60
    ndd -set /dev/arp arp_cleanup_interval 60
b.) ndd -set /dev/ip ip_ire_flush_interval 60000
    ndd -set /dev/arp arp_cleanup_interval 60000
c.) ndd -set /dev/ip ip_ire_flush_interval 60000
d.) ndd -set /dev/arp arp_cleanup_interval 60

Correct answer: B (the value is in microseconds)

134.) How would you view all of the possible ndd parameters relating to ip that could be read or set? 6.6 p.34

a.) ndd /dev/ip ?
b.) ndd /dev/ip help
c.) ndd /dev/ip \?
d.) ndd /dev/ip list

Correct answer: C

135.) How would you view all of the possible ndd parameters relating to udp that could be read or set? 6.6 p.34

a.) ndd /dev/udp ?
b.) ndd /dev/udp help
c.) ndd /dev/udp \?
d.) ndd /dev/udp list

Correct answer: C

136.) If you had an hme type interface, how could you view all of the ndd parameters for the interface? 6.6 p.34

a.) ndd /dev/if \?
b.) ndd /dev/hme \?
c.) ndd /dev/hme0 \?
d.) ndd /dev/hme0 ?

Correct answer: B

137.) How would you view extended, full listing of processes currently running on your system? 6.6 p.38

a.) ps -ef
b.) ps
c.) ps -all
d.) none of the above

Correct answer: A

138.) Which file tells your system <u>initially</u> how or where to resolve names? 6.6 p.39
a.) /etc/resolv.conf
b.) /etc/nsswitch.conf
c.) /etc/hosts
d.) /etc/hostname.*[0-9]

Correct answer: B

139.) If DNS is the specified method for name resolution, which file indicates the ip address of your name server? 6.6 p.39

a.) /etc/resolv.conf
b.) /etc/nsswitch.conf
c.) /etc/resolve.conf
d.) /etc/default/domain

Correct answer: A

140.) How would you specify within the /etc/nsswitch.conf that you would first like to resolve names through the /etc/hosts table and then through your DNS server. 6.6 p.39

a.) hosts: files dns
b.) hosts: files [if not found=return] dns
c.) hosts: hosts dns
d.) hosts: hosts <nameserver ip>

Correct answer: A

141.) With regard to Sendmail you should: 6.6 p.40

a.) set your system up as a null client
b.) remove the boot script that starts the sendmail daemon.
c.) run /usr/lib/sendmail -q periodically from cron to clean out the mail queue.
d.) all of the above

Correct answer: D

142.) If you don't know which script is responsible for starting a given daemon, which of the following is the most effective way to find out? 6.6 p.40

a.) grep <service name> /etc/init.d/*
(i.e #grep sendmail /etc/init.d/*)
b.) grep <service name> /etc/inet.conf
d.) grep <service name> /etc/rc2.d/*
e.) refer to technical manuals

Correct answer: A

143.) How would you configure the /etc/default/login file to prevent remote root logins? 6.6 p.62

a.) CONSOLE=/dev/console
b.) CONSOLE=/dev/null
c.) #CONSOLE=/dev/console
d.) #CONSOLE=/dev/null

Correct answer: A

143.) How would you configure the /etc/default/login file to prevent ANY root logins? 6.6 p.62

a.) CONSOLE=/dev/console
b.) CONSOLE=/dev/null
c.) #CONSOLE=/dev/console
d.) #CONSOLE=/dev/null

Correct answer: B

144.) Which log file will (by default) track all su attempts? 6.6 p.62

a.) sulog
b.) authlog
c.) syslog
d.) none of the above

Correct answer: A

145.) What entry in the /etc/syslog.conf file will log all auth.info events and higher to a log file called /var/log/authlog? 6.6 p.66

a.) auth.info /var/log/authlog
b.) auth.* /var/log/authlog
c.) authentication.* /var/log/authlog
d.) auth.info+ /var/log/authlog
e.) Both A and B would log events of auth.info and higher

Correct answer: E

146.) What entry in the /etc/syslog.conf file will log all critical events of any facility type to a log file called /var/log/crit? 6.6 p.66

a.) crit.* /var/log/crit
b.) critical.* /var/log/crit
c.) all.crit /var/log/crit
d.) *.crit /var/log/crit

Correct answer: D

147.) What entry in the /etc/syslog.conf file will send all critical events of any facility type plus all auth facility event to host *tiger*. 6.6 p.66

a.) crit.*, auth.* tiger
b.) crit.*; auth.* @tiger
c.) crit.all; auth.* @tiger
d.) *.crit; auth.* @tiger

Correct answer: D

148.) What package(s) would you need to enable system accounting? 6.6 p.72

a.) SUNWacc and SUNaccr
b.) SUNWaccr and SUNaccu
c.) None, its part of the kernel
d.) SUNWacc

Correct answer: B

149.) In which file can you disable stop-A with the entry KEYBOARD_ABORT=disabled ? 6.6 p.80

a.) /etc/default/kbd
b.) /etc/default/keyboard
c.) /etc/default/system
d.) /etc/default/login

Correct answer: A

150) In the file /etc/default/passwd how would you set the minimum password length (for regular users) to 4 ? 6.6 p.80

a.) MINLENGTH 4
b.)PASSLENGTH 4
c.) PASSWDLENGTH 4
d.) min. 4

Correct answer: B

UNIX@NIGHT – Network Time Protocol

151.) Which daemon is responsible for keeping statistics on how much average variance the local clock has from the time standard? NTP p.12

a.) ntpd
b.)xntpd
c.)driftd
d.)shiftd

Correct answer: B

152.) If your system clock differs significantly from your external clock source, the following may happen: NTP p.27

a.) the external clock source will adjust the time without hesitation.
b.) the two systems will auto-negotiate a mutual time.
c.) your NTP daemon may refuse to work at all.
d.) none of the above

Correct answer: C

153.) To set yourself up as an NTP client you would first need to copy ________ to _________. NTP p.29

a.)ntp.client, ntp.conf

b.)ntp.conf, ntp.client
c.)ntp.serv, ntp.client
d.) none of the above

Correct answer: A

154.) What is the NTP v.4 daemon name? NTP p.27

a.)xntp
b.)ntpd
c.)xntpd
d.)timed

Correct answer: B

154.) What is the NTP v.3 daemon name? NTP p.27

a.)xntp
b.)ntpd
c.)xntpd
d.)timed
Correct answer: C

155.) Which of the following statements about Stratum levels is NOT true? NTP p.11

a.) GPS is a Stratum 1 clock source
b.) In order to determine the Stratum level of a time server, add "1" to the Stratum value of the device/server it is actively synching with.
c.) The lower the Stratum number, the more accurate the timing source.
d.) The greater the Stratum number, the more accurate the timing source.

Correct answer: D

156.) NTP servers can be configured as: NTP p.12

a.) peers
b.) master/slave
c.) relay agents
d.) both A and B

Correct answer: D

157.) NTP clients can be configured to accept timing from NTP p.14

a.) an external clock source
b.) an internal clock source
c.) more than 1 time server
d.) all of the above

Correct answer: D

158.) Why is time synchronization necessary? NTP p.4

a.) some authentication software relies on time stamp being the same between client and server.
b.) to accurately track when events occurred in the network by correctly reporting time to log files and network management software.
c.) for accounting purposes in a shared environment.
d.) all of the above

Correct answer: D

159.) Which of the following is true? NTP p.4

a.) NTP requires little network bandwidth
b.) NTP does not work through a firewall
c.) NTP requires significant network bandwidth
d.) NTP servers MUST be configured with the ip addresses of each of the NTP clients.

Correct answer: A

160.) Which of the following is a time-based security product? NTP p.5

a.)Kerberos
b.)SecurID
c.)crypt
d.)SSL
e.) both A and B

Correct answer: E

Unix@Night UNIX Forensics

161.) Which of the following best describes the 4 steps of Forensics? FOREN.p.3

a.) seek, compare, copy, and resolve problem
b.) read, create, modify, and destroy
c.) setup, watch, capture, and delete it
d.) prepare, collect, analysis, and event reconstruction
e.) stop, plop, drop and roll

Correct answer: D

162.) Hackers bundle tools together for fast deployment. This collection of tools is commonly referred to as a: FOREN.p.5

a.) snoopit
b.) hackit
c.) root kit
d.) watcher
e.) hacker kit

Correct answer: C

163.) Once a system has been compromised, what obstacles do you face in preserving the system state? FOREN.p.10

a.) recording data without disturbing its state
b.) disabling future logins to preserve the state during collection of evidence. This can be an inconvenience.
c.) you must take rapid action
d.) analysis and collection of evidence for legal defense
e.) all of the above

Correct answer: E

164.) If you chose not to disable logins during you investigation and you know that the system state can change with logins and su, what should you collect first? FOREN p.36

a.) memory, network connections, processes
b.) cdrom, disk activities, targets
c.) source code, applications, makefile

d.) disk utilization, free memory, libraries
e.) file space, disk blocks, libraries

Correct answer: A

165.) The script command helps you accomplish what? FOREN p.39

a.) makes a type script of everything printed on terminal
b.) makes a type script of commands entered
c.) can be used to track syslogd
d.) used to read binaries

Correct answer: A

166.) The netstat utility helps us view what? FOREN. p.44

a.) interface utilization
b.) port numbers of active or idle programs
c.) routing table information
d.) active connections from foreign addresses
e.) all of the above

Correct answer: E

167.) Lrk5, Linux Root Kit version 5 incorporates many which of the following is included? FOREN. p.13

a.) packet sniffer
b.) ability to hide network connections
c.) ability to wipe out log files
d.) sends mail to root user
e.) A, B and C
f.) all of the above

Correct answer: E

168.) TCP Wrappers provide which two basic functions? FOREN. p.29

a.) stops zone transfers and provides authentication
b.) logs requests for internet services and provides an

access control mechanism
c.) logs requests for TCP and UDP internet services
d.) none of the above

Correct answer: B

169.) What information does lsof provide? FOREN. p.41

a.) start of function variable
b.) no more information than ps -ef provides
c.) all open files and which process is using the open file
d.) all of the above

Correct answer: C

170.) Which of the following UNIX log files holds a current login snapshot? FOREN.p.74

a.) /var/log/auth
b.) /var/adm/messages
c.) /var/run/log
d.) /var/sadm/log
e.) /var/run/utmp

Correct answer: E

UNIX@Night One-Time Passwords

171.) Which of the following is not a true statement about OTPs (One Time Password)? OTP p.6

a.) Brute force attacks are not possible
b.) User establishes a secret on remote server
c.) Server sends a challenge string
d.) Response is calculated using challenge and secret

Correct answer: A

172.) OTP uses ___________ user generated key pair. OTP p.9

a.) public/private
b.)challenge/response
c.)private/private
d.)none of the above

Correct answer: A

173.) How would you deploy / and store keys? OTP p.10

a.) email them to each other and store them in a local file with tight permissions
b.) keep encrypted secret in a file on disk, or use smart cards
c.) keep all of them on a central server which shares them out
d.) all of the above

Correct answer: B

174.) Most OTP systems include support for: OTP p.12

a.) telnet
b.) ftp
c.) su
d.) sendmail
e.) A, B and C
f.) A, B and D

Correct answer: E

175.) Which of the following is an alternative to S/Key? OTP p.15

a.)OPIE
b.)S+/Key
c.)SuperKey
d.) OPENKEY

Correct answer: A

176.) OTPs are good but: OTPp.6

a.)expensive
b.)not totally secure as the secret can be discovered by

"shoulder surfing"
c.) send too much clear-text information on the wire
d.) all of the above

Correct answer: B

177.) Standard UNIX passwords are limited to a maximum length of: OTP p.5

a.) 6
b.) 8
c.) 10
d.) 7
e.) 255

Correct answer: B

178.) By default, passwords are transmitted during remote connections how? OTP p.5

a.) clear text
b.) encrypted, taken straight from the /etc/shadow file
c.) there are no passwords required, systems by default allow remote connections with no authentication with a .rhosts file
d.) none of the above

Correct answer: A

179.) In older versions of SunOS, the encrypted password was stored in which file? OTP p.4

a.) /etc/shadow
b.) /etc/password
c.) /etc/passwd
d.) Both A and C
Correct answer: C

180.) On a Solaris system, the encrypted password is stored in which file? OTP p.4

a.) /etc/shadow
b.) /etc/password
c.) /etc/passwd
d.) Both A and C

Correct answer: A

UNIX@Night Secure Shell (SSH)

181.) SSH is a secure replacement for: SSH p.5

a.) the 'r' commands
b.) syslog
c.) mail programs, http connections
d.) only rsh at this time

Correct answer: A

182.) Which of the following is true of SSH? SSH p.6

a.) It provides several encryption options such as IDEA, 3DES blowfish, etc.
b.) Provides data compression option
c.) It can be configured to allow your system to fall back to rsh.
d.) It replaces rsh, rlogin and rcp
e.) all of the above

Correct answer: E

183.) What must be run to generate keys? SSH p.10

a.) ssh-keygen
b.) keygen
c.) ssh_autogen_key
d.) none of the above

Correct answer: A

184.) To run sshd using a specific configuration file what command and option must be used? SSH p.12

a.) sshd -f <configfile>
b.) sshd -u <configfile>
c.) sshd -i <configfile>
d.) sshd <configfile>

Correct answer: A

185.) To run sshd in debug mode, you would use which of the SSH p.32

following switches?

a.) -d
b.) -v
c.) -i
d.) -f

Correct answer: A

186.) To modify the grace period from its default of 600, to either increase or decrease the amount of time a client has to authenticate themselves you would use which switch? SSH p.32

a.) -b
b.) -i or -d (to increase or decrease)
c.) -g
d.) -k

Correct answer: C

187.) If you do not want sshd to log anything, you would use which switch? SSH p.32

a.) -q
b.) -suppress
c.) -d
d.) -i

Correct answer: A

188.) Which option within the SSH configuration file tells sshd to check file modes and ownership of the users home directory and .rhosts before accepting authentication? SSH p.34

a.) PermitRootLogin
b.) IgnoreRhosts
c.) StrictModes
d.) AllowModes
Correct answer: C

189.) Within the SSH configuration file you can enable/ disable root logins with which option? SSH p.34

a.) PermitRootLogin
b.) IgnoreRhosts
c.) StrictModes
d.) AllowModes

Correct answer: A

190.) Within the SSH configuration file you can disable the use of SSH p.34
.rhosts with which option?

a.) PermitRootLogin
b.) IgnoreRhosts
c.) StrictModes
d.) AllowModes

Correct answer: B

UNIX@Night Kerberos

191.) What does Kerberos provide? Kerb p.3
a.) Provides insecure authentication over secure networks
b.) Symmetric-key cryptography
c.) Secure authentication over insecure networks
d.) Use of shared secret key that is transmitted over the network.
e.) Both B and C
f.) Both B and D

Correct answer: E

192.) The default implementation of Kerberos uses what algorithm Kerb p.3

a.) 3DES
b.) DES
c.) MD5
d.) McGloughlin ciphertext

Correct answer: B

193.) Which of the following are correct Kerberos term definitions? Kerb p.5

a.) AS – Authorization Service
b.) TGT – Ticket Granting Ticket
c.) KCS – Kerberos Client Server
d.) A and b
e.) all of the above

Correct answer: B

194.) The KDC implements the AS and TGT, what is the KDC typically known as? Kerb p.5

a.) The system where all authorization takes place.
b.) The system where all authentication takes place.
c.) The ticketless system
d.) The Kerberos client

Correct answer: B

195.) Which of the following describe a Kerberos principle? Kerb p.6

a.) PAM
b.) It shares a secret with KDC
c.) The Kerberos process kerbd
d.) Kerberos user or service
e.) Both B and D

Correct answer: E

196.) Kerberos, by default, uses how many bits in its algorithm? Kerb p.9

a.)56
b.)64
c.)128
d.)96

Correct answer: A

197.) In Kerberos the "ticket" is the basis for authentication, what data does it hold? Kerb p.11

a.) session key
b.) start time
c.) server principal
d.) expiration time
e.) all of the above

198.) Put the following Kerberos Authentication steps in order: Kerb p.14

1-Server ticket
2-Ticket Granting Ticket
3-Request For Service
4-Request for Ticket Granting Ticket
5-Request for Server Ticket

a.) 2,4,5,3,1
b.) 4,2,5,1,3
c.) 5,1,3,2,4
d.) 1,2,4,5,3

Correct answer: B

199.) Which process initially authenticates the user to KDC? Kerb p.18

a.) kerbd
b.) kbd
c.) kinit
d.) start kbd

Correct answer: C

200.) A collection of systems serviced by one or more KDCs is called a: Kerb p.26

a.) world
b.) domain
c.) realm
d.) reem
e.) namespace

Correct answer: C