Global Information Assurance Certification Paper

Brett J. Kopetsky

GIAC Certified Unix Administrator (GCUX) Practical Assignment
Examination Questions
SANS Network Security 2000 (Monterey, CA)

Format used in this practical assignment:

#. Question statement
   A. Choice 1
   B. Choice 2
   C. Choice 3
   D. Choice 4

   Answer (Track.Course Book Title, page/slide number)

1. What is the name of the program that starts all other boot processes?
   A. `sched`
   B. `init`
   C. `pagedaemon`
   D. `ps`

   B (6.1 Unix Basics for the Security Professional, page 2-13)

2. Which of the following characters is not allowed in a Unix filename?
   A. /
   B. ?
   C. -
   D. *

   A (6.1 Unix Basics for the Security Professional, page 2-25)

3. Which directory holds most Unix system configuration files?
   A. /usr
   B. /var
   C. /etc
   D. /home

   C (6.1 Unix Basics for the Security Professional, page 2-29)

4. Which is not one of the standard Unix file permission bits?
   A. read
   B. write
   C. change
   D. execute

   C (6.1 Unix Basics for the Security Professional, page 2-35)

5. What is the result of setting the sticky bit on a directory?
   A. Anyone may add files to the directory.
   B. Anyone may remove files from the directory.
   C. Only the owner may add files to the directory.
   D. Only the owner may remove files from the directory.

   D (6.1 Unix Basics for the Security Professional, page 2-37)

6. Which of the following commands will copy an entire directory tree?
   A. `cp -R`
   B. `xcopy`
   C. `mv`
   D. `cp -p`

   A (6.1 Unix Basics for the Security Professional, page 2-46)

7. What Unix command displays the path of the current working directory?
   A. `ls`
   B. `pwd`
   C. `cwd`
   D. `path`

   B (6.1 Unix Basics for the Security Professional, page 2-50)

8. What is the minimum link count for a directory?
   A. Zero
   B. One
   C. Two
   D. Three

   C (6.1 Unix Basics for the Security Professional, page 2-51)

9. What is the Unix command used to find strings in text files?
   A. `strings`
   B. `file`
   C. `find`
   D. `grep`

   D (6.1 Unix Basics for the Security Professional, page 2-55)

10. What is the Unix command used to replace strings within text files?
    A. `sed`
    B. `awk`
    C. `mv`
    D. `replace`

    A (6.1 Unix Basics for the Security Professional, page 2-56)

11. What is the Unix command used to extract strings from binary files?
    A. `strings`
    B. `file`
    C. `find`
    D `grep`

    A (6.1 Unix Basics for the Security Professional, page 2-57)

12. What is the Unix command that describes the contents of a file?
    A. `strings`
    B. `file`
    C. `find`
    D. `grep`

    B (6.1 Unix Basics for the Security Professional, page 2-58)

13. What is the Unix command used to display the beginning of a file?
    A. `head`
    B. `first`
    C. `begin`
    D. `front`

    A (6.1 Unix Basics for the Security Professional, page 2-59)

14. What is the Unix command used to display the end of a file?
    A. `last`
    B. `end`
    C. `back`
    D. `tail`

    D (6.1 Unix Basics for the Security Professional, page 2-59)

15. What is the third field of the password file?
    A. username
    B. password
    C. user ID
    D. full name

    C (6.1 Unix Basics for the Security Professional, page 2-66)

16. What is the UID of the superuser account?
    A. 0
    B. 1
    C. 100
    D. 65535

    A (6.1 Unix Basics for the Security Professional, page 2-71)

17. What Unix command is used to send a signal to a running process?
    A. `exec`
    B. `kill`
    C. `signal`
    D. `call`

    B (6.1 Unix Basics for the Security Professional, page 2-79)

18. Which signal causes many daemons to reread their configuration files?
    A. SIGHUP
    B. SIGINT
    C. SIGTERM
    D. SIGCHLD

    A (6.1 Unix Basics for the Security Professional, page 2-80)

19. Which of the following information is not returned by the `ifconfig` command?
    A. IP address
    B. hardware address
    C. netmask
    D. hostname

    D (6.1 Unix Basics for the Security Professional, page 2-87)

20. Which configuration file specifies the address of the name server?
    A. /etc/nsswitch.conf
    B. /etc/nodename
    C. /etc/resolv.conf
    D. /etc/hosts

    C (6.1 Unix Basics for the Security Professional, page 2-93)

21. Which Unix command can be used to list the current routing table?
    A. `route -l`
    B. `route -a`
    C. `netstat -a`
    D. `netstat -r`

    D (6.1 Unix Basics for the Security Professional, page 2-100)

22. Which protocol is used to map hardware address to IP addresses?
    A. HTTP
    B. ARP
    C. QIP
    D. None of the above

    B (6.1 Unix Basics for the Security Professional, page 2-102)

23. What is the command that is used to determine if a host is alive on the network?
    A. `nslookup`
    B. `telnet`
    C. `ping`
    D. `arp`

    C (6.1 Unix Basics for the Security Professional, page 2-105)

24. What service is used to schedule recurring events?
    A. cron
    B. syslog
    C. at
    D. lp

    A (6.1 Unix Basics for the Security Professional, page 2-110)

25. What command should be used by a user to edit his own list of scheduled jobs?
    A. `vi /var/cron/crontabs/username`
    B. `crontab -l`
    C. `crontab -e`
    D. `crontab -c`

    C (6.1 Unix Basics for the Security Professional, page 2-118)

26. What property of a Unix password allows an attack to succeed?
    A. non-repudiation
    B. reuse
    C. encryption
    D. length

    B (6.2 Common Issues and Vulnerabilities in Unix Security, page 8)

27. Which of the following can be used to defeat password sniffing?
    A. switched network
    B. SSH
    C. both A & B
    D. there is no way to defeat password sniffing

    C (6.2 Common Issues and Vulnerabilities in Unix Security, page 11)

28. Which of the following should not be done if printing a password sheet?
    A. Distribute on a need to know basis
    B. Use a small font
    C. List system names
    D. Permute the actual passwords

    C (6.2 Common Issues and Vulnerabilities in Unix Security, page 14)

29. What algorithm is used to encrypt most Unix passwords?
    A. IDEA
    B. Blowfish
    C. 3DES
    D. DES

    D (6.2 Common Issues and Vulnerabilities in Unix Security, page 17)

30. Approximately how many unique Unix passwords are there?
    A. 1 million
    B. 12 billion
    C. 800000
    D. 7 trillion

    D (6.2 Common Issues and Vulnerabilities in Unix Security, page 21)

31. Where does a modern Unix system store encrypted passwords?
    A. in memory
    B. /etc/shadow
    C. /etc/passwd
    D. none of the above

    B (6.2 Common Issues and Vulnerabilities in Unix Security, page 23)

32. On modern Unix system, which user(s) is/are allowed to read the encrypted passwords?
    A. root
    B. all users
    C. members of group wheel
    D. Only A & C

    A (6.2 Common Issues and Vulnerabilities in Unix Security, page 23)

33. Which of the following may generate a core file?
    A. Programming errors
    B. Buffer overflow
    C. SIGQUIT
    D. all of the above

    D (6.2 Common Issues and Vulnerabilities in Unix Security, page 28)

34. How can a user prevent core files from being generated?
    A. Issue `ulimit -c 0`
    B. Issue `limit coredumpsize 0`
    C. This can be done but is dependent on which shell the user is running.
    D. Users cannot prevent core files.

    C (6.2 Common Issues and Vulnerabilities in Unix Security, page 30)

35. When do race conditions occur?
    A. When there is a time lag between two file operations
    B. When there is a time lag between opening and writing to a file
    C. When there is a time lag between logging in and beginning to do work
    D. None of the above

    A (6.2 Common Issues and Vulnerabilities in Unix Security, page 33)

36. How does a buffer overflow occur?
    A. Long input strings are given to a program.
    B. Programs do not check input length, accepting any input that they are given.
    C. Two large numbers are multiplied together.
    D. Passwords that are too long are created.

    B (6.2 Common Issues and Vulnerabilities in Unix Security, page 39)

37. What can be done to prevent a buffer overflow attack from succeeding?
    A. Alter program code to reject input that is too long.
    B. Modify the OS kernel so that it does not execute instructions from the stack.
    C. Increase the size of the buffer.
    D. Both A & B

    D (6.2 Common Issues and Vulnerabilities in Unix Security, pages 44-45)

38. Which of the following is not a viable alternative to using set UID shell scripts?
    A. Give everyone the password to the root account.
    B. Write the script in Perl, using its mechanism for handling set UID.
    C. Write the program in a compiled language.
    D. Use a compiled wrapper program to sanitize the environment before the script runs.

    A (6.2 Common Issues and Vulnerabilities in Unix Security, page 58)

39. Which of the following commands can be used to create a "jail" in which to run processes?
    A. `chmod`
    B. `chown`
    C. `chroot`
    D. `chgrp`

    C (6.2 Common Issues and Vulnerabilities in Unix Security, page 62)

40. Which file should never be copied into an FTP server's jail?
    A. /etc/password
    B. /bin/ls
    C. /usr/lib/ld.so.1
    D. /etc/shadow

    D (6.2 Common Issues and Vulnerabilities in Unix Security, page 68)

41. Which file specifies a list of hosts and/or users who may login without a password?
    A. .rhosts
    B. ftp.users
    C. hosts
    D. passwd

    A (6.2 Common Issues and Vulnerabilities in Unix Security, page 84)

42. What does a + indicate in a .rhosts file?
    A. Username "+" may log in.
    B. The name following the + may not log in.
    C. It is a wildcard, allowing anyone to log in.
    D. It indicates a comment.

    C. *(6.2 Common Issues and Vulnerabilities in Unix Security, page 84)*

43. Why should usernames not be used in /etc/hosts.equiv?
    A. It becomes too difficult to maintain for large systems.
    B. It allows that remote user to log into the local host as any user.
    C. It invalidates the file.
    D. There is nothing wrong with this.

    B (6.2 Common Issues and Vulnerabilities in Unix Security, page 85)

44. What should the permissions be on a .rhosts file?
    A. 644
    B. 700
    C. 600
    D. 664

    C (6.2 Common Issues and Vulnerabilities in Unix Security, page 87)

45. Which of the following is not a concern with using .Xauthority to help secure X windows sessions?
    A. Users do not understand how to use it.
    B. Connection speed is slowed.
    C. NFS mounted home directories make it easier to steal a .Xauthority file.
    D. No method of cookie revocation exists.

    B (6.2 Common Issues and Vulnerabilities in Unix Security, page 91)

46. Which of the following services is dangerous because it allows for unauthenticated file transfers?
    A. rexec
    B. ftp
    C. telnet
    D. tftp

    D (6.2 Common Issues and Vulnerabilities in Unix Security, page 97)

47. Why should RPC based services be disabled?
    A. They have had numerous root compromise issues in the past.
    B. They tend to be exploited by denial of service tools.
    C. They rely on the remote host to authenticate a user.
    D. All of the above.

    D. *(6.2 Common Issues and Vulnerabilities in Unix Security, pages 104-106)*

48. How can RPC services be secured?
    A. Block access to the portmapper.
    B. Only allow root to use RPC services.
    C. Change the port on which the portmapper runs.
    D. RPC cannot be secured and should be disabled.

    A (6.2 Common Issues and Vulnerabilities in Unix Security, page 107)

49. What information can be retrieved using the `ypcat` command in a NIS environment?
    A. usernames
    B. full names of users
    C. encrypted password strings
    D. all of the above

    D (6.2 Common Issues and Vulnerabilities in Unix Security, page 109)

50. "A backup isn't a backup until:
    A. you lock it away."
    B. you store it offsite."
    C. you do a restore."
    D. you write it to CD-ROM."

    C (6.2 Common Issues and Vulnerabilities in Unix Security, page 125)

51. Which of the following is not checked for the root account by COPS?
    A. root is in /etc/ftpusers
    B. root is not in any user's .rhost file
    C. a "+" does not appear in /etc/hosts.equiv
    D. non-root entries do not exist in /.rhosts

    B (6.3 Unix Security Tools and Their Uses, slide 23)

52. Which of these is not checked for by TIGER on an NFS server?
    A. Exporting of the root directory
    B. Giving anonymous access UID 0
    C. Granting root access to other hosts
    D. Exporting a directory everywhere

    C (6.3 Unix Security Tools and Their Uses, slide 96)

53. Which of the following tools includes Kuang, which describes how to crack a system?
    A. TIGER
    B. COPS
    C. nmap
    D. Tripwire

    B (6.3 Unix Security Tools and Their Uses, slide 47)

54. Which of these tools can be used to examine log files for evidence of cracking?
    A. nmap
    B. ISS
    C. Logcheck
    D. Tripwire

    C (6.3 Unix Security Tools and Their Uses, slide 153)

55. What program may be run to identify what process are associated with open connections on the local system?
    A. `lsof`
    B. `nmap`
    C. `nessus`
    D. `SATAN`

    A (6.3 Unix Security Tools and Their Uses, slide 166)

56. Which of the following is a disadvantage when using lsof?
    A. It reports to much information.
    B. It opens security vulnerabilities while it is running.
    C. It may block.
    D. It has cryptic output.

    C (6.3 Unix Security Tools and Their Uses, slide 184)

57. Which of the following SMTP checks are not made by ISS?
    A. Aliases checks
    B. wiz command
    C. debug command
    D. None of the above

    D (6.3 Unix Security Tools and Their Uses, slides 204-205)

58. Which check is not done by the nfsbug tool?
    A. guessable NFS filehandles
    B. anonymous root access
    C. `chdir` allowing access outside of exported filesystem
    D. UID overflow bug

    B (6.3 Unix Security Tools and Their Uses, slide 217)

59. Which of the following is a disadvantage of using SATAN?
    A. It has a poor user interface.
    B. It only checks for well-known vulnerabilities.
    C. It allows administrators to add checks for the local site.
    D. Its scans may get written into system logs.

    B (6.3 Unix Security Tools and Their Uses, slide 243-244)

60. What is the purpose of courtney?
    A. Check for local system vulnerabilities
    B. Check for remote system vulnerabilities
    C. Detect system scanners such as SATAN
    D. Detect cracking attempts

    C (6.3 Unix Security Tools and Their Uses, slide 247)

61. Which of this is not a disadvantage of courtney?
    A. It generates a large number of false positives.
    B. It may cause core dumps on busy networks.
    C. It only detects one kind of attack.
    D. It can detect attacks on multiple hosts.

    D (6.3 Unix Security Tools and Their Uses, slides 252-253)

62. What is the purpose of nmap?
    A. Check for local system vulnerabilities
    B. Scan for open ports on remote hosts
    C. Detect system scanners such as SATAN
    D. Detect cracking attempts

    B (6.3 Unix Security Tools and Their Uses, slide 256)

63. Which of the following is nmap not capable of doing?
    A. Determining remote operating system
    B. Scanning multiple hosts in a single run
    C. Stealth scans
    D. Checking versions of running services

    D (6.3 Unix Security Tools and Their Uses, slides 262, 275-276)

64. How does one list authorized nessus users?
    A. `nessus -u`
    B. `nessus --users`
    C. `nessusd -L`
    D. `nessusd -u`

    C (6.3 Unix Security Tools and Their Uses, slide 285)

65. Which of the following is done by tcp_wrapper?
    A. Log outgoing connections
    B. Filter outgoing connections
    C. Filter incoming connections
    D. Snoop connections to remote hosts

    C (6.3 Unix Security Tools and Their Uses, slide 296)

66. Which of these programs tests tcp_wrapper access rules?
    A. `tcpdmatch`
    B. `tcpdchk`
    C. `tcpd`
    D. `tcpdump`

    A (6.3 Unix Security Tools and Their Uses, slide 299)

67. Which is not a short-coming of using tcp_wrapper?
    A. Inadequate checks
    B. No control over which daemons can be contacted
    C. False sense of security
    D. Unreliable mechanism to identify remote users

    B (6.3 Unix Security Tools and Their Uses, slide 324)

68. What is the purpose of `sudo`?
    A. Provide a restricted set of commands that may be run with privileges
    B. Restrict remote access to a host
    C. Run programs remotely
    D. Check for system vulnerabilities

    A (6.3 Unix Security Tools and Their Uses, slide 328)

69. What is the `sudo` timestamp file used for?
    A. Check the time of day for access restriction
    B. Log when users use `sudo`
    C. Prevent entry of password if it has been entered recently
    D. Update the system time to synchronize it with other hosts

    C (6.3 Unix Security Tools and Their Uses, slide 330)

70. What type of keys must be used with PGP to ensure compatibility with older versions?
    A. Diffe-Hellman
    B. Blowfish
    C. IDEA
    D. RSA

    D (6.3 Unix Security Tools and Their Uses, slide374)

71. Where should a PGP private key be stored for greatest security?
    A. On a secure FTP server
    B. In a user's home directory
    C. On a standalone system
    D. In a networked key repository

    C (6.3 Unix Security Tools and Their Uses, slide 384)

72. What RCS command is used to retrieve a file for editing?
    A. `co`
    B. `rcs -o`
    C. `rcs -l`
    D. `ci`

    A (6.3 Unix Security Tools and Their Uses, slide 389)

73. What is the purpose of the tool crack?
    A. Gain root access to a remote system
    B. Guess passwords
    C. Examine the local system for vulnerabilities
    D. Change the root password

    B (6.3 Unix Security Tools and Their Uses, slide 401)

74. What is S/Key?
    A. A method of securing email
    B. A replacement for telnet
    C. A one time password implementation
    D. A replacement for rlogin

    C (6.3 Unix Security Tools and Their Uses, slide 428)

75. Who is the author of COPS?
    A. Mudge
    B. Craig Rowland
    C. Weitse Venema
    D. Dan Farmer

    D (6.3 Unix Security Tools and Their Uses, slide 19)

76. What file is used to control user access to wu-ftpd?
    A. /etc/ftpconversions
    B. /etc/ftpaccess
    C. /etc/ftpgroups
    D. /etc/ftpservers

    B (6.4 Running Unix Applications Securely, page 14)

77. How is guest access to a server running wu-ftp disabled within that file?
    A. `class  all  guest,anonymous  *`
    B. `class  all  guest  *`
    C. `class  all  real  *`
    D. `class  all  anonymous,real  *`

    C (6.4 Running Unix Applications Securely, page 15)

78. What is the name of the Linux package that configures permissions for anonymous FTP access?
    A. anonftp
    B. ftpconfig
    C. ftpaccess
    D. anon

    A (6.4 Running Unix Applications Securely, page 17)

79. How does one use TCP wrappers to limit ftp access to machines in mydomain.com?
    A. "ftp: mydomain.com" in hosts.allow
    B. "in.ftpd: .mydomain.com" in hosts.deny
    C. "in.ftpd: *.mydomain.com" in hosts.allow
    D. "in.ftpd: .mydomain.com" in hosts.allow

    D (6.4 Running Unix Applications Securely, page 18)

80. What is the proper hosts.allow entry to allow open access to an anonymous FTP server?
    A. in.ftpd: ALL
    B. in.ftpd: OPEN
    C. in.ftpd: ANONYMOUS
    D. TCP wrappers will not allow open access to an anonymous FTP server.

    A (6.4 Running Unix Applications Securely, page 18)

81. What should be the Unix permissions for an anonymous FTP upload directory?
    A. 666
    B. 777
    C. 333
    D. 644

    C (6.4 Running Unix Applications Securely, page 21)

82. Which of the following modules does Apache install by default?
    A. mod_auth_dbm
    B. mod_perl
    C. mod_digest
    D. mod_access

    D (6.4 Running Unix Applications Securely, page 31)

83. In recent versions of Apache, what is the name of the configuration file?
    A. httpd.conf
    B. apache.conf
    C. config.apache
    D. rc.httpd

    A (6.4 Running Unix Applications Securely, page 33)

84. What is the difference between specifying "order allow, deny" and "order deny, allow" in the Apache configuration?
    A. There is no difference; they may be used interchangeably.
    B. The first defaults to allow; the second defaults to deny.
    C. The first defaults to deny; the second defaults to allow.
    D. The second is not a valid command.

    C (6.4 Running Unix Applications Securely, page 37)

85. What is the proper Apache configuration syntax to reject connections from hackers.com?
    A. allow all but hackers.com
    B. deny hackers.com
    C. reject from hackers.com
    D. deny from hackers.com

    D (6.4 Running Unix Applications Securely, page 38)

86. When should Apache not be allowed to run CGI scripts out of any directory?
    A. The host needs to be kept secure.
    B. The users are trusted to write safe scripts.
    C. The system has no users and no visitors.
    D. The rest of the server is so vulnerable that one more risk is not significant.

    A (6.4 Running Unix Applications Securely, page 39)

87. Which configuration option prevents Apache from executing programs from within server parsed HTML files?
    A. NOEXEC
    B. IncludesNOEXEC
    C. NoIncludesExec
    D. NoParse

    B (6.4 Running Unix Applications Securely, page 41)

88. Which file in a directory overrides the default settings for that directory?
    A. httpd.conf
    B. apache.conf
    C. .htaccess
    D. .dirsettings

    C (6.4 Running Unix Applications Securely, page 43)

89. Which of the following attributes of a parameter of a CGI program is arbitrary?
    A. name
    B. value
    C. length
    D. all of the above

    D (6.4 Running Unix Applications Securely, page 52)

90. How is the global DNS database organized?
    A. Distributed and hierarchical
    B. Centralized and hierarchical
    C. Distributed and flat
    D. Centralized and flat

    A (6.4 Running Unix Applications Securely, page 64)

91. Which of the following is not a security issue when using BIND?
    A. Unnecessary release of information
    B. Buffer overflows
    C. Lack of authentication
    D. Cache poisoning

    C (6.4 Running Unix Applications Securely, page 67)

92. Under what username should BIND run?
    A. root
    B. bin
    C. any privileged user assigned for this purpose
    D. any non-privileged user assigned for this purpose

    D (6.4 Running Unix Applications Securely, page 96)

93. Which of the following is not a common security issue noted when running an SMTP server?
    A. mail forgery
    B. buffer overflow
    C. back doors
    D. none of the above

    D (6.4 Running Unix Applications Securely, page 108)

94. For what program was the first CERT advisory issued?
    A. BIND
    B. Sendmail
    C. wu-ftp
    D. Apache

    B (6.4 Running Unix Applications Securely, page 110)

95. Which of the following is a replacement MTA that can be used in place of Sendmail?
    A. Qmail
    B. EWAN
    C. WINE
    D. none of the above

    A. *(6.4 Running Unix Applications Securely, page 115)*

96. Which of the following is a good reason to disable spam checks on internal hosts?
    A. Spammers cannot use the host as a relay.
    B. Spam will be unable to reach the internal users.
    C. Internal mail may bounce.
    D. Both A & B.

    C (6.4 Running Unix Applications Securely, page 120)

97. Which hosts should run SMTP daemons?
    A. all internal hosts
    B. all external hosts
    C. any host which receives mail
    D. any host which sends mail

    C (6.4 Running Unix Applications Securely, page 125)

98. What information does Sendmail's relay-domains file contain?
    A. A list of domains from which mail may be accepted
    B. A list of IP addresses to which to which mail may be relayed
    C. A list of domains to which mail may be sent
    D. A list of IP addresses from which mail may be relayed

    D. *(6.4 Running Unix Applications Securely, page 118)*

99. What is required in order to use SSL for e-commerce?
    A. The Apache web server
    B. A certificate from a recognized Certificate Authority
    C. OpenSSL
    D. All of the above

    B (6.4 Running Unix Applications Securely, page 59)

100. Which entry in the Apache configuration forces Apache to only accept connections from the localhost?
    A. Listen 127.0.0.1:80
    B. Accept 127.0.0.1:80
    C. Server 127.0.0.1:80
    D. Server localhost:80

    A (6.4 Running Unix Applications Securely, page 49)

101. Which type of install is not an option when installing Red Hat Linux?
    A. Workstation
    B. Server
    C. Minimal
    D. Custom

    C (6.5 Linux Practicum, page 7)

102. Under Linux, how big of a partition should be reserved for logs?
    A. 25% of total disk
    B. 100 MB
    C. 50 MB
    D. Depends on host's usage

    D (6.5 Linux Practicum, page 9)

103. Which of these operating systems is not supported by Webmin?
    A. Irix
    B. Linux
    C. Unicos
    D. Solaris

    C (6.5 Linux Practicum, page 16)

104. Which of the following is not a system log message criticality level?
    A. emerg
    B. crit
    C. info
    D. mesg

    D (6.5 Linux Practicum, page 30)

105. What Red Hat program allows log files to be archived periodically?
    A. `rotate`
    B. `logrotate`
    C. `rotatelog`
    D. `logarchive`

    B (6.5 Linux Practicum, page 33)

106. What is the current stable series of Linux kernels?
    A. 1.2.x
    B. 2.2.x
    C. 2.3.x
    D. 2.4.x

    B (6.5 Linux Practicum, page 42)

107. What is the first command that should be issued when compiling a new kernel after it has been configured?
    A. `make dep`
    B. `make clean`
    C. `make zlilo`
    D. `make modules`

    A (6.5 Linux Practicum, page 46)

108. What services should be removed from /etc/inetd.conf on a Linux workstation?
    A. BSD "r" commands"
    B. TFTP
    C. Finger
    D. All of them

    D (6.5 Linux Practicum, page 61)

109. What is the default action for TCP wrappers if no rules are matched?
    A. It is service dependent.
    B. Access is allowed.
    C. Access is denied.
    D. There is no default, everything must have a matching rule.

    B (6.5 Linux Practicum, page 63)

110. Which of the following daemons is usually started from within inetd.conf?
    A. `httpd`
    B. `named`
    C. `nfsd`
    D. `ftpd`

    D (6.5 Linux Practicum, page 65)

111. Which command will list network ports that are listening for connections?
    A. `lsof -i +M`
    B. `netstat -at`
    C. either of the above
    D. none of the above

    C (6.5 Linux Practicum, pages 66-67)

112. Which version of the print daemon does Red Hat provide by default?
    A. SYSV
    B. Proprietary
    C. LPRng
    D. BSD

    D (6.5 Linux Practicum, page 75)

113 Which version of the print daemon does Debian provide by default?
    A. SYSV
    B. Proprietary
    C. LPRng
    D. BSD

    C (6.5 Linux Practicum, page 76)

114. For what purpose is Samba used?
    A. Sharing files between Unix hosts
    B. Sharing files between MS Windows hosts
    C. Sharing files from a MS Windows host to an Unix host
    D. Sharing files from a Unix host to MS Windows hosts

    D. *(6.5 Linux Practicum, page 78)*

115. Which is not a security level that may be set for Samba?
    A. Directory
    B. Share
    C. User
    D. Domain

    A (6.5 Linux Practicum, page 81)

116. How are null passwords indicated in /et/smb.conf?
    A. A blank password field
    B. A password field consisting of "NO PASSWORD" and 21 Xs
    C. A password filed consisting of "NO PASSWORD"
    D. Null passwords are not allowed

    B (6.5 Linux Practicum, page 83)

117. How are guest shares enabled in /etc/smb.conf?
    A. allow guest
    B. set guest = yes
    C. guest ok = yes
    D. guest = ok

    C (6.5 Linux Practicum, page 84)

118. What is the name of the packet firewall included with Linux?
    A. ipmasq
    B. Checkpoint
    C. ipnat
    D. ipchains

    D (6.5 Linux Practicum, page 85)

119. What is Bastille Linux?
    A. the French version of Linux
    B. a set of Perl scripts for securing certain Linux distribution
    C. a free Linux distribution
    D. none of the above

    B (6.5 Linux Practicum, page 96)

120. Which type of scan is not detected by PortSentry?
    A. ACK/WIN
    B. FIN
    C. NULL
    D. SYN

    A (6.5 Linux Practicum, page 101)

121. TARA is an upgrade to what security scanner?
    A. SATAN
    B. COPS
    C. TIGER
    D. nmap

    C (6.5 Linux Practicum, page 103)

122. Which of the following should be done before running a security scan on a network?
    A. Check company policy.
    B. Test the scan in an isolated environment.
    C. Notify system administrators.
    D. All of the above

    D (6.5 Linux Practicum, page 105)

123. SARA and SAINT are updated versions of what security scanner?
    A. SATAN
    B. COPS
    C. TIGER
    D. nmap

    A (6.5 Linux Practicum, page 106)

124. What program may be used to disable Red Hat Linux startup scripts?
    A. `init`
    B. `chkconfig`
    C. `sysconfig`
    D. `ifconfig`

    B (6.5 Linux Practicum, page 68)

125. Which of the following services should be run on a loghost?
    A. syslogd
    B. nfsd
    C. httpd
    D. both A & C

    A (6.5 Linux Practicum, page 36)

126. Which Solaris OS cluster choice should be used for a highly secure host?
    A. End-User
    B. Developer
    C. Full
    D. Core System Support

    D (6.6 Solaris Practicum, page 1-17)

127. Which command would be most effective in determining what file(s) an application needs in order to execute properly?
   A. `grep`
   B. `strings`
   C. `truss`
   D. `ls`

   C (6.6 Solaris Practicum, page 1-20)

128. Which of the following Solaris packages need to be installed in order to display manual pages?
   A. SUNWlibC
   B. SUNWdoc
   C. SUNWman
   D. All of the above

   D (6.6 Solaris Practicum, page 1-22)

129. Which of the following commands will prevent Solaris from forwarding packets?
   A. `ndd -set /dev/ip ip_forwarding 0`
   B. `ndd -set ip_send_redirects 0`
   C. `touch /etc/notrouter`
   D. both A & C

   D (6.6 Solaris Practicum, page 1-33)

130. What effect does removing the line
   `sc:234:respawn:/usr/lib/saf/sac -t 300`
   from /etc/inittab have on a Solaris host?
   A. It has no effect.
   B. It disables inetd.
   C. It disables listening on serial ports.
   D. It disables system performance monitoring.

   C (6.6 Solaris Practicum, page 1-36)

131. Which default crontab files should be removed?
   A. adm
   B. lp
   C. sys
   D. all of the above

   D (6.6 Solaris Practicum, page 1-37)

132. What is the correct entry in Solaris's /etc/resolv.conf to if you are running a nameserver on a host with IP address 192.168.2.21?
    A. dns 192.168.2.21
    B. nameserver 192.168.2.21
    C. named 192.168.2.21
    D. bind 192.168.2.21

    B (6.6 Solaris Practicum, page 1-39)

133. Which of the following is true about filesystems mounted with the nosuid option?
    A. The root filesystem can be mounted nosuid.
    B. They can have devices within them.
    C. They can be read only.
    D. Files cannot be created within them.

    C (6.6 Solaris Practicum, page 1-45)

134. Which of the following is a drop-in replacement for the BSD "r" commands?
    A. Apache
    B. SSH
    C. TCP Wrappers
    D. None of the above

    B (6.6 Solaris Practicum, page 1-49)

135. Which of these methods should a user use to gain root privilege on a host?
    A. Telnet and log in as root
    B. SSH and log in as root
    C. `rlogin -l root`
    D. Log in under user's own account and use /bin/su

    D (6.6 Solaris Practicum, page 1-62)

136. Which of the following should be used as a shell for accounts which are not allowed to log in?
    A. /dev/null
    B. /dev/rand
    C. /bin/true
    D. /bin/false

    A (6.6 Solaris Practicum, page 1-63)

137. Which of the following lists syslog priorities in descending order of importance?
   A. emerg, alert, err, warning
   B. emerg, crit, alert, notice
   C. warning, info, notice, debug
   D. crit, emerg, alert, warning

   A (6.6 Solaris Practicum, page 1-66)

138. Which of the following is not an advantage of using syslog-ng over the default Solaris syslog daemon?
   A. Messages may be routed based on regular expressions.
   B. Connections use TCP rather than UDP.
   C. Syslog-ng provides more levels of log messages.
   D. Loghosts may communicate with each other.

   C (6.6 Solaris Practicum, page 1-69)

139. Where are Solaris system accounting files stored?
   A. /var/log
   B. /var/adm/sa
   C. /usr/etc/sa
   D. /etc

   B (6.6 Solaris Practicum, page 1-70)

140. What is the typical performance degradation caused by enabling process accounting?
   A. 10-20%
   B. 20-30%
   C. 30-40%
   D. 40-50%

   A (6.6 Solaris Practicum, page 1-76)

141. Which of the following entries in /etc/default/inetinit causes a modern Solaris system to use a better algorithm to generate TCP sequence numbers?
   A. TCP_SEQUENCE = 2
   B. TCP_SEQUENCE = STRONG
   C. TCP_STRONG_ISS = 2
   D TCP_STRONG_ISS = YES

   C (6.6 Solaris Practicum, page 1-79)

142. What effect does setting CONSOLE in /etc/default/login have on a Solaris host?
   A. Users may only directly log in on the specified device.
   B. It specifies which device to use as a console.
   C. It specifies which devices may not act as consoles.
   D. Root may only directly log in on the specified device.

   D (6.6 Solaris Practicum, page 1-80)

143. What is not a possible setting for the eeprom password on Sun hardware?
   A. none
   B. command
   C. root
   D. full

   C (6.6 Solaris Practicum, page 1-82)

144. To which file should the lines
   mount hsfs –o nosuid
   mount ufs –o nosuid
   be added in order to prevent set-UID programs from being executed from removable media?
   A. /etc/vfstab
   B. /etc/rmmount.conf
   C. /etc/dfstab
   D. /etc/vold.conf

   B (6.6 Solaris Practicum, page 1-84)

145. Which of the following lines should be added to /etc/system to prevent some buffer overrun attacks?
   A. set noexec_user_stack = 1
   B. set exec_user_stack = 0
   C. set noexec_user_attack_log = 1
   D. set exec_user_attack_log = 0

   A (6.6 Solaris Practicum, page 1-85)

146. Which of the following is not a tool used for securing Solaris systems?
   A. YASSP
   B. TITAN
   C. Bastille
   D. fix-modes

   C (6.6 Solaris Practicum, pages 1-104 - 1-111)

147. Which of the following is not a new Solaris feature first included in version 8?
    A. IPSEC
    B. Smart Card support
    C. UFS logging
    D. Role-based access control

    C (6.6 Solaris Practicum, page 1-117)

148. Which of the following should not be allowed on a secure host?
    A. Networked backups
    B. Remote log in as root
    C. Packet forwarding
    D. All of the above

    D (6.6 Solaris Practicum, pages 1-33, 1-66, 1-98)

149. Which application is not as likely to be run in a `chroot()`ed environment?
    A. Web servers
    B. FTP servers
    C. Telnet servers
    D. Name servers

    C (6.6 Solaris Practicum, page 1-45)

150. Which of the following startup scripts should not be removed when securing a Solaris 2.5 system?
    A. S73nfs.client
    B. S76nscd
    C. S74autofs
    D. S72sysid.net

    B (6.6 Solaris Practicum, page 1-27)

151. Which of the following depend on accurate timekeeping?
    A. Log files
    B. One time passwords
    C. Distributed software development
    D. All of the above

    D (Unix@Night: Network Time Protocol, page 5)

152. How is the global DNS database organized?
    A. Distributed and hierarchical
    B. Centralized and hierarchical
    C. Distributed and flat
    D. Centralized and flat

    A (Unix@Night: Network Time Protocol, page 9)

153. What is the name for an NTP server that synchronizes against an external time source?
    A. Secondary
    B. Primary
    C. Master
    D. Slave

    B (Unix@Night: Network Time Protocol, page 9)

154. What is the NTP stratum of a host which is not connected to a network?
    A. 1
    B. 2
    C. 12
    D. 16

    D (Unix@Night: Network Time Protocol, page 11)

155. How does a site defend against an attacker skewing the system clocks during synchronization?
    A. Block connections at the firewall
    B. Require all connections to use SSH
    C. Synchronize against multiple NTP servers
    D. Disable BSD "r" commands

    C (Unix@Night: Network Time Protocol, page 13)

156. What is a pseudo-clock?
    A. An NTP server which synchronizes to its internal clock
    B. An NTP server which has not properly calculated its own drift
    C. An NTP server which synchronizes to only one external source
    D. An NTP client which also acts as a server

    A (Unix@Night: Network Time Protocol, page 19)

157. Why should time update broadcasts not be used?
    A. Lack of accuracy
    B. Unreliability of transmission
    C. No significant bandwidth savings
    D. All of the above

    D (Unix@Night: Network Time Protocol, page 22)

158. Which of the following programs are required in order to run an NTP server?
    A. `ntpdate`
    B. `tickadj`
    C. `xntpd`
    D. None of the above

    C (Unix@Night: Network Time Protocol, page 25)

159. Which of the following features first appeared in NTP v3?
    A. Support for intermittently connected hosts
    B. Multicast support
    C. Symmetric key authentication
    D. Public key authentication

    C (Unix@Night: Network Time Protocol, page 7)

160. What is the stratum of a host which has available to it for synchronization four unique NTP servers at strata 2, 3, 5, and 8?
    A. 1
    B. 2
    C. 3
    D. 8

    C (Unix@Night: Network Time Protocol, page 11)

161. Which of the following protocols is not used by SSH for link encryption?
    A. IDEA
    B. RSA
    C. DES
    D. Blowfish

    B (Unix@Night: Secure Shell (SSH), page 5)

162. Which of the following is not supported by SSH v1?
    A. Kerberos
    B. SOCKS
    C. SecurID
    D. TCP Wrappers banners

    D (Unix@Night: Secure Shell (SSH), pages 7, 41)

163. For which of the following commands is SSH not a drop-in replacement?
    A. `rdist`
    B. `rlogin`
    C. `rcp`
    D. `rsh`

    A (Unix@Night: Secure Shell (SSH), page 22)

164. What is default size of the SSH server key?
    A. 64 bits
    B. 128 bits
    C. 768 bits
    D. 1024 bits

    C (Unix@Night: Secure Shell (SSH), page 32)

165. What method does SSH use to secure X11 connections?
    A. RSA
    B. xhost
    C. IDEA
    D. xauthority

    D (Unix@Night: Secure Shell (SSH), page 46)

166. Support for which of the following is being introduced in SSH v2?
    A. Diffie-Hellman key exchange
    B. DSA support
    C. Secure DNS
    D. Secure FTP

    D (Unix@Night: Secure Shell (SSH), page 54)

167. What option needs to be set in SSH's authorized_keys file in order to disable support for X Windows?
   A. no-X11-forwarding
   B. no-Xwindows-forwarding
   C. no-agent-forwarding
   D. no-port-forwarding

   A (Unix@Night: Secure Shell (SSH), page 38)

168. Which of these is not a valid choice for the PermitRootLogin option when configuring sshd?
   A. yes
   B. no
   C. nopwd
   D. pwdrequired

   D (Unix@Night: Secure Shell (SSH), page 34)

169. Why should sshd not be run from inetd?
   A. It cannot be run from inetd.
   B. Startup is delayed by key generation.
   C. inetd does not allow secure connections to succeed.
   D. sshd will not encrypt sessions started via inetd.

   B (Unix@Night: Secure Shell (SSH), page 24)

170. Which of the following commands forwards requests from remote port 1999 on remote.domain.com to an internal webserver (www.me.com) when the user is connected via SSH to remote.domain.com from login.me.com?
   A. `ssh -L 1999:remote.domain.com:80 login.me.com`
   B. `ssh -L 1999:remote.domain.com:80 www.me.com`
   C. `ssh -R 1999:www.me.com:80 login.me.com`
   D. `ssh -R 80:remote.domain.com:1999 www.me.com`

   C (Unix@Night: Secure Shell (SSH), page 15)

171. Which of the following is not a vulnerability of standard Unix passwords?
   A. Packet sniffers may capture them
   B. Enciphered passwords may be viewed and cracked.
   C. The eight character length does not allow for enough permutations.
   D. The password encryption algorithm is weak.

   D (Unix@Night: One-Time Passwords, page 4)

172. What are the two factors of authentication used by most one-time password systems?
    A. Something you know and something you are
    B. Something you have and something you are
    C. Something you have and something you know
    D. Something you know and something you do

    C (Unix@Night: One-Time Passwords, page 7)

173. Which of the following is a freely available one-time password implementation?
    A. OPIE
    B. SecurID
    C. CryptoCard
    D. SafeWord

    A (Unix@Night: One-Time Passwords, page 11)

174. Which of the following is not stored in the opiekeys file?
    A. User's secret code
    B. Next challenge
    C. Random seed
    D. Counter

    B (Unix@Night: One-Time Passwords, page 17)

175. Which of the following binaries is not replaced when OPIE is installed?
    A. `login`
    B. `ftp`
    C. `su`
    D. `telnet`

    D (Unix@Night: One-Time Passwords, page 18)

176. Which of these is not an ongoing support issue when using a commercial one-time password system?
    A. Re-issuing tokens
    B. Creating secret identifiers for each user
    C. Upgrading the one-time password software
    D. Upgrading the operating system of the one-time password authentication server

    B (Unix@Night: One-Time Passwords, page 31)

177. What factors should be examined when considering a one-time password token system?
   A. Ease of use
   B. Software token availability
   C. Expiration
   D. All of the above

   D (Unix@Night: One-Time Passwords, page 34)

178. How can a one-time password system be compromised?
   A. Brute force attack after capturing a challenge and corresponding response
   B. "Shoulder surfing" to steal a user's secret and acquiring the user's token
   C. Either of the above
   D. None of the above

   C (Unix@Night: One-Time Passwords, page 6)

179. Which of the following lists classes of two factor devices?
   A. Challenge and Response
   B. Challenge/Response and Synchronous
   C. Synchronous and Asynchronous
   D. Hardware and Software

   B (Unix@Night: One-Time Passwords, page 8)

180. When using a public key authentication system, where should the secret key not be stored?
   A. On a smart card
   B. On a removable disk
   C. On a shared filesystem
   D. None of the above are acceptable places to store a secret key

   C (Unix@Night: One-Time Passwords, page 10)

181. What encryption algorithm is used by Kerberos?
   A. RSA
   B. Diffie-Hellman
   C. IDEA
   D. DES

   D (Unix@Night: Kerberos, page 3)

182. Which portion of the Kerberos system is often referred to as the "Kerberos server?"
   A. Key Distribution Center
   B. Authentication Server
   C. Ticket Granting Server
   D. Application Server

   A (Unix@Night: Kerberos, page 5)

183. Which of the following is not required for use of Kerberos?
    A. NTP
    B. DNS
    C. NIS
    D. KDC

    C (Unix@Night: Kerberos, page 7)

184. In the Kerberos world, what is a "principal?"
    A. A user
    B. A service
    C. A password
    D. Either A or B

    D (Unix@Night: Kerberos, page 8)

185. Which of the following is not a part of a Kerberos ticket?
    A. Client Principal
    B. User's passphrase
    C. Server Principal
    D. Expiration time

    B (Unix@Night: Kerberos, page 13)

186. What is the first step in Kerberos authentication?
    A. Request for server ticket
    B. Request for service
    C. Request for Ticket-Granting Ticket
    D. Request for authentication

    C (Unix@Night: Kerberos, page 14)

187. What is the term for a collection of systems serviced by a KDC?
    A. Realm
    B. Domain
    C. Kerb
    D. Room

    A (Unix@Night: Kerberos, page 26)

188. Which of the following is prevented by Kerberos?
    A. Denial of service
    B. Password guessing
    C. Misuse of privilege
    D. Password sniffing

    D (Unix@Night: Kerberos, page 40)

189. Who developed the key distribution model used by Kerberos?
    A. Diffie and Hellman
    B. Rivest, Shamir, and Adleman
    C. Needham and Schroeder
    D. Farmer and Spafford

    C (Unix@Night: Kerberos, page 3)

190. Which portion of the Kerberos system is responsible for verifying a user's identity?
    A. Key Distribution Center
    B. Ticket Granting Service
    C. Ticket Granting Ticket
    D. Authentication Server

    B (Unix@Night: Kerberos, page 5)

191. Which is not one of John Green's "Four Steps of Forensics?"
    A. Preparation
    B. Collection and Handling
    C. Event Reconstruction
    D. Prevention

    D (Unix@Night: Unix Forensics, page 3)

192. Which of the following tool sets should be included in a system analysis toolkit?
    A. `who`, `w`, `finger`
    B. `netstat`, `lsof`
    C. `chown`, `chgrp`, `chmod`
    D. All of the above

    D (Unix@Night: Unix Forensics, page 24)

193. Which information on a host is most volatile and should therefore be collected first?
    A. Memory contents
    B. Disk contents
    C. Process status
    D. Network connection status

    A (Unix@Night: Unix Forensics, page 36)

194. What command can be used to record actions taken during an investigation of a compromise?
    A. `truss`
    B. `lsof`
    C. `script`
    D. `write`

    C (Unix@Night: Unix Forensics, page 39)

195. Which of the following commands can be used to determine if a sniffer is running on a host?
    A. `lsof`
    B. `ifconfig`
    C. `netstat`
    D. `tcpdump`

    B (Unix@Night: Unix Forensics, page 46)

196. Which of the following is not a package for tracking and accessing file integrity?
    A. Tripwire
    B. Sherpa
    C. RIACS
    D. Logcheck

    D (Unix@Night: Unix Forensics, page 57)

197. Which log file contains a list of the users currently logged in?
    A. utmp
    B. wtmp
    C. loginlog
    D. messages

    A (Unix@Night: Unix Forensics, page 74)

198. After an attack, what type of files should be searched for?
    A. Newly created data files
    B. SUID files
    C. Executable files
    D. Root owned files

    B (Unix@Night: Unix Forensics, page 88)

199. What command is used to find unlinked, but still open files?
   A. `ls -O`
   B. `ls -l`
   C. `lsof +L1`
   D. `lsof -O`

   C (Unix@Night: Unix Forensics, page 90)

200. Which of the following binaries are replaced by the lrk5 rootkit for Linux?
   A. `ps`
   B. `passwd`
   C. `lsof`
   D. All of the above

   D (Unix@Night: Unix Forensics, page 14)