Global Information Assurance Certification Paper

Question	Section	Page
1. Knowing whether the version of UNIX your using is based on SYSV or BSD will help you determine: a. where the startup scripts are located. b. how UNIX permissions will work. c. what the process listing will look like. d. a. and c. d is the correct answer.	6.1	14, 17, 77, 78
2. The early stages of the UNIX boot process: a. are not clearly defined and entirely up to the vendor. b. were standardized with AT&T System V. c. haven't changed in the last 20 years. d. are controlled by the bootp protocol. a is the correct answer.	6.1	11
3. The usual NFS client daemons are: a. lockd and statd. b. nfsd. c. nfsd and lockd. d. statd and mountd. a is the correct answer.	6.1	22
4. The purpose of cron is to: a. run processes automatically at certain times of the day. b. turn consistency reporting on. c. enable crash dumps. d. synchronize UNIX system time. a is the correct answer.	6.1	23
5. UNIX file names can contain: a. any characters except "/" and null. b. any printable characters. c. any alpha-numeric character, "-", and "_". d. any characters. a is the correct answer.	6.1	25

Question	Section	Page
6. The length limit of a UNIX directory pathname is: a. 1024 characters. b. unlimited. c. 512 for SYSV-based UNIX, 1024 for BSD-based UNIX. d. 8192 characters. a is the correct answer.	6.1	25
7. The UNIX command to display the unprintable characters in a filename is: a. ls -b b. ls -l c. files d. ls -u a is the correct answer.	6.1	27
8. Write permission to a directory (drwxrwxrwx) grants the ability: a. to create or remove any files from the directory. b. to create, modify, or remove any files from the directory. c. to only create files in the directory. d. for anyone to create a file, but only the file's owner to remove files from the directory. a is the correct answer.	6.1	37
9. Write permission to a directory with the "sticky bit" set (drwxrwxrwt) grants the ability: a. for anyone to create a file, but only the file's owner to remove files from the directory. b. to create or remove any files from the directory. c. to create, modify, or remove any files from the directory. d. to only create files in the directory. a is the correct answer.	6.1	37
10. A umask of 026 will create files with default permisions: a. 640 (-rw-r--r--) b. 751 (-rwxr-x--x) c. 026 (-----w-rw-) d. 666 (-rw-rw-rw-) a is the correct answer.	6.1	39

Question	Section	Page
11. An inode contains: a. file parameters, including owner and permissions. b. system parameters, including hostname and host IP address. c. user parameters, including username and home directory. d. process parameters, including process owner, PID, and PPID. a is the correct answer.	6.1	44
12. The file "log" exists. The command to create a symbolic link to this file with the name "newlog" is: a. ln –s log newlog b. ln log newlog c. ln –s newlog log d. ln newlog log a is the correct answer.	6.1	49
13. The UNIX command that extracts printable character sequences from a binary file is: a. strings b. file c. cat d. print a is the correct answer.	6.1	57
14. What is field 3 in the /etc/passwd file for: a. UID b. GID c. GECOS d. login shell a is the correct answer.	6.1	66
15. If field 2 in the "/etc/passwd" file doesn't contain the encrypted password, it will usually be stored in the file: a. /etc/shadow b. /etc/passwd.shadow c. /etc/password d. /etc/users a is the correct answer.	6.1	67

Question	Section	Page
16. The "sudo" command: a. permits limited access to superuser privilege. b. runs the sulog rotation script. c. logs all root, su, and sudo privileged access. d. prompts for the root password. a is the correct answer.	6.1	72
17. The "sudo" command uses the configuration file: a. /etc/sudoers b. /var/sudo/access.conf c. /etc/sudo.conf d. ~/.sudoers a is the correct answer.	6.1	72
18. The difference between the commands "ps –ef" and "ps –aux" is: a. SYSV vs. BSD b. "extended, full" output vs. "all, user" output c. BSD vs. SYSV d. there is no difference: the output is identical a is the correct answer.	6.1	77, 78
19. What is not part of the information that can be displayed by the "ifconfig" command: a. collision statistics. b. IP address. c. whether the interface is in "promiscuous mode". d. Ethernet address. a is the correct answer.	6.1	86, 87
20. Which of the following is not a method for looking up an IP address from a hostname: a. ARP b. DNS c. look them up in /etc/hosts d. NIS a is the correct answer.	6.1	90

Question	Section	Page
21. The DNS configuration file, "resolv.conf" is used to specify: a. the systems domain name. b. the domains nameservers. c. the DNS root servers. d. a. and b. d is the correct answer.	6.1	93
22. The "secure" parameter in the "/etc/ttys" file specifies: a. root login is allowed for that device. b. passwords are required for that device. c. the audit system will track that device. d. root login is not allowed for that device. a is the correct answer.	6.1	113
23. Processes or jobs started by the cron daemon run as: a. the user associated with that crontab. b. cron. c. root. d. nobody. a is the correct answer.	6.1	114
24. The inetd daemon is used: a. to start other network daemons. b. to process all internet traffic. c. to network to iMac computers. d. to give status information about network connections. a is the correct answer.	6.1	135
25. The simplest and most secure way to handle routing on a UNIX system is with: a. static routing b. dynamic routing c. routed d. gated a is the correct answer.	6.1	130

Question	Section	Page
26. Password threats include all of the following, except: a. digression b. sniffing c. off-line attacks d. "shoulder surfing" a is the correct answer.	6.2	7
27. The first 2 characters of a standard encrypted UNIX password are the _____ value used to permute the encryption algorithm. a. salt b. seed c. spice d. key a is the correct answer.	6.2	18
28. The UNIX system function used to encrypt a password is: a. crypt b. passwd c. encrypt d. getpwnam a is the correct answer.	6.2	19
29. The most secure way to write a SetUID script is: a. not to write it. SetUID scripts are not secure. b. to use full pathnames. c. to set execute but not read permission on the script. d. set the secure SetUID script kernel variable. a is the correct answer.	6.2	51
30. All of the following are alternatives to using SetUID scripts, except: a. set the secure SetUID script kernel variable. b. use suidperl. c. use C. d. use a SetUID wrapper (coded in C). a is the correct answer.	6.2	58

Question	Section	Page
31. The UNIX command "chroot" is used to: a. create a process jail. b. change the root password. c. change root privileges. d. create a new root shell. a is the correct answer.	6.2	60
32. A "rootkit" is: a. a prepackaged bundle of software used to compromise a system. b. a procedure for creating a process jail. c. public domain software for verifying root integrity. d. used by the chroot command to increase security. a is the correct answer.	6.2	75
33. Which of the following is not a feature of a "backdoor": a. most commonly target DNS and RPC services. b. utilizes modified/replaced system commands. c. often difficult to detect d. an unobtrusive, illegitimate access method to a system. a is the correct answer.	6.2	74
34. A "rootkit" currently helps an intruder avoid detection by all of the following, except: a. hiding kernel hacks b. hiding files. c. hiding processes. d. hiding network connections. a is the correct answer.	6.2	77, 78, 79, 81
35. Security tools should be brought to a compromised system on a CD-ROM because CD-ROMS: a. are read-only. b. are slow. c. use hsfs instead of ufs. d. don't use SetUID. a is the correct answer.	6.2	82

Question	Section	Page
36. The .rhosts file is used: a. by hackers to exploit trust relationships. b. by users to avoid typing in passwords. c. by systems administrators who don't know any better. d. all of the above. d is the correct answer.	6.2	84
37. "Remote Reconnaissance" refers to: a. intruders using informational network services. b. "shoulder surfing". c. social engineering. d. attacks against non-Tempest grade equipment. a is the correct answer.	6.2	96
38. The following are primary defenses against session hijacking, except: a. using ARP b. using ssh c. using IPSEC d. using VPN a is the correct answer.	6.2	100
39. When using NIS on a network with systems using shadow passwords (the /etc/shadow file), the command "ypcat passwd" will display: a. the password map-with encrypted passwords. b. the password map-without encrypted passwords. c. the password map-with non-UID 0 encrypted passwords. d. an error message. a is the correct answer.	6.2	109
40. The following are features of NIS+ except: a. widely supported by most UNIX vendors. b. supports encryption and mutual authentication. c. difficult to setup. d. "NIS compatibility mode" disables most security features. a is the correct answer.	6.2	113

Question	Section	Page
41. Changes in NFS exports parameters on the NFS server take effect on the NFS client: a. only after the client reboots. b. immediately. c. usually within 5-10 minutes. d. after the "nfspush" command. a is the correct answer.	6.2	117
42. By default, attempts by the root user to write on an NFS-mounted file system results in files owned by the user: a. nobody b. nfs c. root d. nfsd a is the correct answer.	6.2	116
43. "Buffer overflow" exploits can be prevented by all of the following, except: a. fixing the buffer. b. fixing the programs. c. fixing the programmers. d. fixing the stack. a is the correct answer.	6.2	44
44. The well-known "expreserve" exploit involves: a. a modified IFS environment variable. b. a race condition. c. a buffer overflow. d. a denial of service attack. a is the correct answer.	6.2	49
45. UNIX core files have security implications for all of the following reasons, except: a. they can be used for a race condition. b. they're often world-readable. c. they can contain passwords, filenames, and data. d. they can be used for a denial of service attack a is the correct answer.	6.2	29

Question	Section	Page
46. "chroot" is often used to secure all of the following network services, except: a. telnet b. FTP c. TFTP d. BIND a is the correct answer.	6.2	62
47. The "xhost" command is used for access control with: a. the X Window System b. the Berkeley r-commands c. xntp d. xns a is the correct answer.	6.2	89
48. Defenses against password sniffing include all of the following, except: a. using ARP b. using switched networks c. using encrypted transport mechanisms, e.g., ssh d. using VPN a is the correct answer.	6.2	11
49. Typical TFTP implementation safeguards include all of the following, except: a. require passwords b. chroot to tftpboot c. only permit download of world-readable files d. only permit upload of existing word-writeable files a is the correct answer.	6.2	97
50. Typical RPC implementation safeguards include all of the following, except: a. protect against buffer overflows. b. install a secure replacement for rpcbind. c. block spoofed address. d. block access to port 111 at the firewall. a is the correct answer.	6.2	107

Question	Section	Page
51. "COPS" is a system integrity tool that checks all of the following, except: a. verifies digital signatures. b. examines files, devices. c. examines group and password files. d. checks for miscellaneous problems. a is the correct answer.	6.3	20
52. When a security tool is ready to report results, the most secure method to use is: a. to watch the results, in person, on the screen. b. to send the results via Email. c. to save the results in a disk file. d. to post the results to a web page. a is the correct answer.	6.3	7
53. Using dynamically loaded security is risky, because: a. they're harder and more error-prone to compile. b. you may not get the correct version of the dynamic library at execution time. c. the load path environment variable can load the wrong library. d. b. and c. is the correct answer.	6.3	14
54. One of the most useful modules in "COPS" in "Kuang", which is used to: a. attempt a rules-based breakin of the system. b. verify correct FTP configuration. c. crack passwords using a special Asian dictionary. d. looks for the common ".kuang" rootkit a is the correct answer.	6.3	47
55. If "COPS" is run on a network, the results can be summarized using: a. carp b. SATAN c. COPS+ d. tiger a is the correct answer.	6.3	60

Question	Section	Page
56. An example of a host-based, multi-function security analysis tool would be: a. tiger b. crack c. sudo d. devcheck a is the correct answer.	6.3	65
57. "tripwire" is a: a. file integrity checking mechanism. b. network gateway protocol analyzer. c. security notification server d. network scanner detection program. a is the correct answer.	6.3	116
58. "tripwire" works using different all of these types of checksums, except: a. RSA b. Snefru c. MD-5 d. Haval a is the correct answer.	6.3	131, 132
59. A difference between "swatch" and "logcheck" is: a. swatch runs continuously while logcheck runs periodically. b. swatch was developed in Switzerland while logcheck was developed in the US. c. swatch ignores entries known not to be a problem while logcheck extracts relevant log entries. d. swatch is nolonger under development while logcheck is being actively maintained. a is the correct answer.	6.3	139, 152
60. The "lsof" security tool: a. lists files that are open. b. is a trojan horse-proof replacement for the "ls" command. c. encrypts data using the lsof algorithm. d. summarizes system logs. a is the correct answer.	6.3	166

Question	Section	Page
61. The purpose of the "watcher" security tool is to: a. execute commands and detect extreme or unusual output. b. watch system logs for specific log messages. c. monitor network flow for anomalies. d. provide network time or watch service. a is the correct answer.	6.3	187
62. The function of "ISS" security tool is to a. scan systems for vulnerabilities. b. detect scanning attacks. c. scan system log files for forensic data. d. control access from remote clients. a is the correct answer.	6.3	197
63. The purpose of the "SATAN" security tool is to: a. provide automated network vulnerability scanning. b. check for weak system passwords. c. watch system logs for specific log messages. d. manage host daemons. a is the correct answer.	6.3	231
64. A problem with security tools like "SATAN" and "ISS" is: a. they can only scan for known exploits, not new ones. b. their use on the network is undetectable. c. they provide a poor user interface. d. they can't control access from remote clients. a is the correct answer.	6.3	214, 244
65. The security utility that scans hosts in multiple ways looking for open ports is: a. nmap b. lsof c. portscan d. portmapper a is the correct answer.	6.3	256

Question	Section	Page
66. In the following grouping of similar security tools, which tools don't belong together: a. nmap, smrsh b. COPS, tiger c. nessus, SATAN d. swatch, logcheck a is the correct answer.	6.3	18, 197
67. All of the following are bad points associated with "tcp_wrappers" except: a. the overhead is unacceptable. b. some of the checks are not adequate. c. may give a false sense of security. d. user identification mechanism is not reliable. a is the correct answer.	6.3	324
68. When configuring "tcp_wrappers" for host access control, in what order are the "hosts.allow" and "hosts.deny" files consulted? a. hosts.allow first, and if no match then hosts.deny b. hosts.deny first, and if no match then hosts.allow c. hosts.allow first, and then hosts.deny d. hosts.deny first, and then hosts.deny a is the correct answer.	6.3	309, man page
69. The "smrsh" security tool is used to: a. provide a restricted shell for sendmail. b. provide a restricted environment for inside a process jail. c. disable network sniffers upon discovery. d. encrypt files prior to network transfer, a is the correct answer.	6.3	342
70. The security tool that provides digital signatures for signing files is: a. PGP b. RSA c. NTP d. MD-5 a is the correct answer.	6.3	373

Question	Section	Page
71. "PGP" encrypts and decrypts data using a pair of keys, called the _____ key and the _____key. a. public, private b. master, slave c. client, server d. alpha, beta a is the correct answer.	6.3	383, 384
72. With "PGP" encryption, your secrets are as secure as your: a. private key b. public key c. master key d. root password a is the correct answer.	6.3	384
73. Several catagories of bad password choices include all of the following except: a. passwords which are a concatenation of letters and numbers b. passwords which match a word in the dictionary. c. passwords based on the user's account name, initials or given name. d. passwords which are acronyms, geographical and product names, and technical terms. a is the correct answer.	6.3	406, 407, 408, 409
74. The security tool that checks for bad, existing passwords is: a. crack b. passwd c. passwd+ d. pwck a is the correct answer.	6.3	411
75. "passwd+" is: a. a proactive password changing program. b. a security tool that checks for bad existing passwords. c. a one-time password program. d. a password auditing program. a is the correct answer.	6.3	450, 451, 452

Question	Section	Page
76. The "wu-ftp" server is preferred to vender supplied versions of the ftp server for all of the following reasons, except: a. it works better in a chroot process jail. b. it was designed to support large sites. c. it includes a rich set of features. d. its vulnerabilities are known and rapidly fixed. a is the correct answer.	6.4	6, 22
77. Which of the following steps are not part of compiling and installing "wu-ftpd": a. get lastest version of wu-ftp b. ./configure –prefix=/usr/local c. generate public and private keys d. make && make install c is the correct answer.	6.4	9
78. Access files used by "wu-ftp" include all of the following except: a. ftp.conf b. ftpaccess c. ftpusers d. ftphosts a is the correct answer.	6.4	10
79. It's possible to eliminate anonymous access in "wu-ftp" by removing the "anonymous" parameter from "class" statement in the file: a. ftp.conf b. ftpaccess c. ftpusers d. ftphosts b is the correct answer.	6.4	13
80. "wu-ftp" will log file transfers in the log file: a. /var/log/xferlog b. /var/log/secure c. /var/adm/messages d. /var/log/SYSLOG a is the correct answer.	6.4	16

Question	Section	Page
81. The "Apache" web server can controlled by all of the following configuration files, except: a. apache.conf b. access.conf c. srm.conf d. httpd.conf a is the correct answer.	6.4	31
82. Reading the line "order allow,deny" in the "Apache" web server configuration file indicates that: a. default access is denied b. default access isn't specified c. default access is allowed d. default access is contingent on supplying a password a is the correct answer.	6.4	35
83. When using the "Apache" web server, the default name of the access override settings file is: a. .htaccess b. access.conf c. overrides.conf d. htaccess a is the correct answer.	6.4	41
84. The principle problem with using digest authentication (mod_auth) with the "Apache" web server is: a. most browsers still don't support it. b. digest authentication uses weak encryption. c. it's slow. d. digest authentication send passwords in clear text. a is the correct answer.	6.4	43
85. All of the following statements about the Common Gateway Interface (CGI) to the "Apache" web server are true, except: a. it's the most trusted means of obtaining user input. b. it's the most common means of processing user input. c. a few simple techniques limit the CGI security threat. d. it's the most common means of server compromise. a is the correct answer.	6.4	49

Question	Section	Page
86. "Apache" web server CGI security threats can be limited by all of the following techniques, except: a. check signatures on all input. b. test all input. c. don't trust any input. d. limit CGI access. a is the correct answer.	6.4	50, 51, 52
87. The most common security issues with BIND include all of the following except: a. trojan horses b. buffer overflows. c. cache poisoning. d. giving away too much information. a is the correct answer.	6.4	65
88. Which information in your DNS database is of most interest to an attacker? a. HINFO and TXT records b. MX and A records c. SOA and A records d. CNAME and PTR records a is the correct answer.	6.4	66
89. Split-Horizon DNS refers to: a. a secure DNS implementation strategy. b. a secure, commercial DNS solution marketed by Split-Horizon. c. performance-optimized DNS server. d. using DNS across time zones. a is the correct answer.	6.4	71
90. DNS main configuration file is: a. named.conf b. dns.conf c. bind.conf d. config.dns a is the correct answer.	6.4	82

Question	Section	Page
91. A DNS master server controls who can request zone transfers with: a. the "allow-transfer" option in the configuration file. b. the zones.allows file. c. with new versions of DNS, this can't be controlled. d. tcp-wrappers. a is the correct answer.	6.4	82
92. The DNS server daemon "named" is usually started: a. by a startup script b. by inetd c. by BIND d. manually a is the correct answer.	6.4	93
93. The most typical security problems associated with "sendmail" include: a. cache poisoning. b. buffer overflows. c. back doors. d. setUID exploits. a is the correct answer.	6.4	106
94. Alternatives to using the "sendmail" MTA include all of the following, except: a. MH b. Qmail c. Postfix d. Exim a is the correct answer.	6.4	113
95. For machines that are not going to be used as mail servers, "sendmail" can be configured as a: a. nullclient b. mailrelay c. simpleclient d. workstation a is the correct answer.	6.4	123

Question	Section	Page
96. The newest versions of "sendmail" include all of these anti-SPAM features, except: a. tcp-wrappers option. b. blacklist option. c. no unqualified sender addresses. d. domain name validity check. a is the correct answer.	6.4	116, 117
97. The goals of using a bastion host for mail routing include all of the following, except: a. inbound mail goes to the bastion first. b. inbound mail is delivered on the bastion. c. outbound mail from internal hosts is relayed to the bastion. d. bastion delivers to remote domain. b is the correct answer.	6.4	125
98. The most secure way to operate a DNS server is to: a. run it in a chroot environment. b. run it as user nobody. c. only permit encrypted connections. d. enable DNS+ security features. a is the correct answer.	6.4	94
99. The purpose of using the Secure Socket Layer (SSL) with the "Apache" web server is to: a. provide strong authentication and encryption. b. integrate Apache with PGP. c. allow one time passwords in conjunction with "wu-ftp". d. avoid cache poisoning. a is the correct answer.	6.4	55
100. A cache poisoning DNS server attack involves: a. appending extra information to a DNS response. b. a buffer overflow corrupting the cache. c. misconfiguring the DNS cache. d. bad data in the SOA record. a is the correct answer.	6.4	69

Question	Section	Page
101. On Linux, Pluggable Authentication Modules (PAM) can be used for all of the following, except: a. increase RPM logging. b. change password encryption. c. impose access limits. d. impose resource limits. a is the correct answer.	6.5	22
102. On Linux, the PAM service config files use control flags that can have any of the following values, except: a. secure b. optional c. required d. requisite a is the correct answer.	6.5	23
103. On Linux, all of the following are PAM Config files, except: a. srm.conf b. access.conf c. limits.conf d. time.conf is the correct answer.	6.5	24
104. On Linux, system logs are managed with the package: a. sysklog b. swatch c. logcheck d. logger a is the correct answer.	6.5	29
105. To maintain maximum security for system logs: a. use a standalone log server. b. run syslog in a chroot process jail. c. encrypt log files. d. store log files in nonstandard directories. is the correct answer.	6.5	35

Question	Section	Page
106. On Linux, using Ctl+Alt+Del to reboot can be prevented by modifying: a. /etc/inittab b. /etc/system c. /etc/keyboard d. LILO a is the correct answer.	6.5	18
107. On Linux, it's possible to enable or disable startup scripts with the command: a. chkconfig b. init c. mv d. configure a is the correct answer.	6.5	20
108. On Linux, use the "chage" command to a. change password expirations. b. rotate log files. c. change the GECOS field in /etc/passwd d. change time/date information in the inode. a is the correct answer.	6.5	28
109. On Linux, system logfiles are rotated automatically by a. logrotate b. logger c. logcheck d. rotalog a is the correct answer.	6.5	31
110. On Linux, the correct date and time can be set: a. manually using the date command. b. automatically using ntpdate c. automatically using xntp d. all of the above d is the correct answer.	6.5	38, 39

Question	Section	Page
111. On Linux, use RPM's "freshen" option to a. only install update packages currently installed. b. only install updates to the kernel. c. install updates for all available packages. d. update the RPM index, so it accurately reflects packages installed on the system. a is the correct answer.	6.5	50
112. On Linux, inetd should be a. turned off if possible to enhance security. b. always be on, as the system won't run without it. c. configured to run with security enabled. d. none of the above. a is the correct answer.	6.5	63
113. "tcp-wrappers" will control access to and log activity associated with: a. inetd b. init c. netstat d. ipchains a is the correct answer.	6.5	64
114. On Linux, "tcpdchk" can be used to: a. verify tcp-wrappers config file syntax. b. enable or disable tcp-wrappers. c. check the tcp-wrappers log file and report hacking attempts. d. determine whether tcp-wrappers has been hacked. a is the correct answer.	6.5	68
115. On Linux, inetd should be used to control Internet daemons for all the following services, except: a. telnet b. sendmail c. DNS d. Samba a is the correct answer.	6.5	70

Question	Section	Page
116. To find network ports that are actively listening for connections, use: a. netstat b. vmstat c. portstat d. inetd a is the correct answer.	6.5	71
117. NFS: a. is a widely used network file sharing protocol. b. uses weak, easily spoofed authentication c. both a and b d. neither or b c is the correct answer.	6.5	75
118. On Linux, workstations shouldn't need to export NFS directories, since: a. workstations should be running the NFS client, not the NFS server. b. the Linux workstation release of NFS is a newer revision with enhanced security. c. they're exported automatically. d. NFS doesn't work on Linux workstations. a is the correct answer.	6.5	76
119. On Linux, a printing option that is available that supports authentication with Kerberos and PGP is: a. LPRng b. lpr/lpd c. lp/lpsched d. impressario a is the correct answer.	6.5	81
120. On Linux, "Samba" is: a. the daemon that provides NT file and print sharing. b. an audio CD player. c. an addon to NFS. d. an NT emulator. a is the correct answer.	6.5	83

Question	Section	Page
121. On Linux, Samba is configured using the file: a. smb.conf b. samba.conf c. nt.conf d. audio.conf a is the correct answer.	6.5	84
122. Bastille Linux is: a. a set of scripts for securing a Linux system. b. a version of Linux marketed in France. c. a Linux-based firewall product. d. Linux network backup software. a is the correct answer.	6.5	104
123. The TARA security tool is based on: a. Tiger b. SATAN c. YASSP d. TITAN a is the correct answer.	6.5	111
124. Rules for scanning a network include all of the following, except: a. post the results where they can be seen. b. test the scanner on an isolated network. c. post a notice that the scan is going to happen. d. get management approval prior to performing the scan. a is the correct answer.	6.5	113
125. On Linux, secure operation: a. depends upon having the disks divided into multiple partitions. b. depends upon having the disk configured as one, mangeable partition. c. disk partitioning styles is not really a factor. d. disks should be partitioned using the “secure” option. c is the correct answer.	6.5	8

Question	Section	Page
126. When performing the initial build of a secure machine, make sure the machine is: a. not connected to a network. b. connected to a network for using Jumpstart. c. connected to a network only while downloading configuration files. d. connected to the network. a is the correct answer.	6.6	13
127. When building a secure Solaris system, start by installing the _____ OS cluster. a. core b. end-user c. developer d. full a is the correct answer.	6.6	17
128. When building a secure Solaris system, after the initial OS installation: a. download and install the latest patches. b. no patches will be required if the OS version is current. c. install the latest patches that came on the OS CD-ROM. d. wait for the latest patch CD-ROM to arrive in the mail. a is the correct answer.	6.6	23
129. On Solaris, by default, system daemons use a umask of a. 000 b. 022 c. 067 d. 077 a is the correct answer.	6.6	30

Question	Section	Page
130. On Solaris, to disable the listener on serial ports, the following line: sc:234:respawn:/usr/lib/saf/sac –t 300 should be removed from the file a. /etc/inittab b. /etc/inetd.conf c. /etc/gettytab d. /etc/ttys a is the correct answer.	6.6	36
131. On Solaris, to setup sendmail securely: a. delete the Solaris sendmail, and download , install, and securely configure the most currect version of sendmail. b. use the standard, Solaris sendmail installation. c. use the secure, Solaris sendmail installation. d. download, install, and securely configure "smrsh",and use it along with the standard, Solaris sendmail installation. a is the correct answer.	6.6	40
132. On Solaris, if the /usr file system is mounted "ro", the only way to add new files to /usr is to: a. use the command "mount –o remount,rw" b. modify "/etc/vfstab" and use the command "reboot" c. use the command "shareall" d. a and b d is the correct answer.	6.6	44
133. On Solaris, problems with the "nosuid" option for the /etc/vfstab file include all of the following, except a. nosuid can poisen the NFS cache. b. nosuid implies nodev. c. nosuid can't be specified for the root file system. d. nosuid can't be used for an anonymous FTP server chroot environment. a is the correct answer.	6.6	45

Question	Section	Page
134. After Solaris has been securely installed, system administrators should be able to securely login over the network using: a. ssh only b. ssh and telnet c. ssh, telnet, and rsh d. telnet only a is the correct answer.	6.6	49
135. After Solaris has been securely installed, access to the root account should be available: a. via su b. via console login c. via remote login d. a and b d is the correct answer.	6.6	62
136. On Solaris, unwanted user accounts that are recommended to be deleted include all of the following, except: a. nobody b. uucp c. smtp d. listen a is the correct answer.	6.6	63
137. On Solaris, to create the initial log file, it's necessary to use the command: a. touch /var/log/authlog b. syslogd –l /var/log/authlog c. syslogd -init d. a and b a is the correct answer.	6.6	67
138. On Solaris, the "sar" command can gather data about all of the following, except: a. user login times b. CPU utilization c. disk and file I/O d. system calls a is the correct answer.	6.6	70

Question	Section	Page
139. On Solaris, problems associated with running process accounting include all of the following, except: a. it's possible for processes to opt out of being accounted. b. a potential 10-20% performance degredation. c. 40 bytes of data logged per process can accumulate quickly. d. if a process doesn't terminate, it's never logged. a is the correct answer.	6.6	76
140. On Solaris, it's possible to disable the "Stop-A" keyboard halt sequence by placing: "KEYBOARD_ABORT=disabled" in the file: a. /etc/default b. /etc/keyboard c. /etc/system d. /etc/pam.conf a is the correct answer.	6.6	80
141. On Solaris, it's possible to create set default "umask" values in the file: a. /etc/profile b. /etc/.login c. /etc/system d. a and b d is the correct answer.	6.6	81
142. On Solaris, if EEPROM security mode is set to full, and the EEPROM password is lost, the password may be recovered : a. only by installing a brand new EEPROM. b. with the eeprom-reset command. c. by removing and reinstalling the current EEPROM. d. by pressing and holding the system reset button for 10 seconds. a is the correct answer.	6.6	82

Question	Section	Page
143. On Solaris, to prevent removeable media with SetUID programs from being introduced to the system, add the lines: mount hsfs –o nosuid mount ufs –o nosuid to the file: a. /etc/rmmount.conf b. /etc/vfstab c. /etc/mtab d. /etc/mount.conf a is the correct answer.	6.6	84
144. On Solaris, the most secure way of preventing users from using .rhosts style authentication is to: a. configure it in /etc/pam.conf b. educate your users why .rhosts files are insecure c. create a cron job to run at midnight which deletes .rhosts files d. configure it in /etc/hosts.equiv a is the correct answer.	6.6	86
145. On Solaris, usage of "cron" can be controlled with the file: a. cron.allow b. cron.deny c. cron.conf d. a and b d is the correct answer.	6.6	87
146. On Solaris, file system mount options include all of the following, except: a. secure b. ro c. nosuid d. remount a is the correct answer.	6.6	44

Question	Section	Page
147. On Solaris, by default, a system with two network interfaces will: a. act as a functioning router. b. act as a functioning router, but only for local subnets. c. not route data between the two interfaces. d. only route data as requested between the two interfaces. a is the correct answer.	6.6	33
148. On Solaris, to disable default routing behavior, use the command: a. touch /etc/notrouter b. ndd –set /dev/ip ip_forwarding 0 c. route -f d. a or b d is the correct answer.	6.6	33
149. On Solaris, to run the client-side of DNS securely: a. use the standard Solaris resolver. b. delete the Solaris resolver, and download , install, and securely configure the most currect version of BIND. c. use the secure Solaris resolver. d. use “tcp-wrappers” to maintain secure access to the Solaris resolver. a is the correct answer.	6.6	39
150. On Solaris, there are several security scripts available on the Internet, including all of the following, except: a. SolarSecure b. fix-modes c. YASSP d. TITAN a is the correct answer.	6.6	102, 106, 111
151. NTP service provides all of the follow features, except: a. provides timestamped system log feature. b. provides network time synchronization. c. resists bogus time data. d. supports mutual server authentication. a is the correct answer.	NTP	4

Question	Section	Page
152. Using NTP service is important for all the following reasons, except: a. keeps cron running without errors. b. consisitent time for log file timestamps c. required by security tools, e.g., SecureID, Kerberos d. avoid problems with NFS filesharing used in distributed development environments a is the correct answer.	NTP	5
153. XNTP is: a. NTP version 3 b. a divergent version of NTP c. NTP modified for use with X Windows d. NTP version 4 a is the correct answer.	NTP	6
154. NTP distributes time using: a. a hierarchy of primary and secondary servers. b. Open Shortest Path First (OSPF). c. a broadcast, average, and vote protocol. d. a two-level, master-slave server relationship a is the correct answer.	NTP	9
155. A _____ 1 NTP server gets time fromand atomic/GPS clock. a. stratum b. level c. cumulus d. master a is the correct answer.	NTP	11
156. NTP's ongoing report of inaccuracy of the system clock is called: a. drift. b. time shift. c. synchronization error. d. time factor. a is the correct answer.	NTP	12

Question	Section	Page
157. An NTP server can be configured to use their own system clock if their connection to the external clock source fails. This feature is called a: a. pseudo clock b. system clock c. atomic clock d. redundant clock a is the correct answer.	NTP	19
158. Advantages to using routers as NTP servers include all of the following, except: a. easy global configuration updates. b. routers are at predictable addresses. c. networks are often a centrally managed resource. d. provides time seamlessly to the network. a is the correct answer.	NTP	21
159. NTP should be started: a. by a startup script. b. by inetd. c. by routed. d. manually. a is the correct answer.	NTP	27
160. The name of the NTP configuration file is: a. ntp.conf b. time.conf c. xntprc d. time_config a is the correct answer.	NTP	29
161. SSH is a replacement for all for all of the following, except: a. smrsh b. rsh c. rlogin d. rcp a is the correct answer.	SSH	2

Question	Section	Page
162. SSH can be configured to integrate with all of these security tools, except: a. SSL b. Kerberos c. SecurID d. SOCKS a is the correct answer.	SSH	7
163. SSH can use all of the following authentication methods, except: a. Blowfish b. host-based trust files c. RSA-based authentication d. Kerberos a is the correct answer.	SSH	8, 9, 10
164. Secure SSH port forwarding is also known as a: a. tunnel b. loop c. warp d. straw a is the correct answer.	SSH	14
165. SSH initializes a secure connection using: a. RSA public/private key encryption. b. Kerberos. c. host-based trust files. d. symmetric key encryption. a is the correct answer.	SSH	17
166. The issue associated with using RSA encryption with SSH is one of: a. patents. b. robustness. c. algorithm speed. d. cryptographic strength a is the correct answer.	SSH	17, 26, 52

Question	Section	Page
167. "sshd" uses the config file: a. /etc/sshd_config b. ~/.ssh/config c. /etc/sshd.conf d. /usr/local/sshd/sshd.config a is the correct answer.	SSH	31
168. "ssh" uses the config file(s): a. /etc/sshd_config b. ~/.ssh/config c. /etc/sshd.conf d. a and b d is the correct answer.	SSH	31
169. "ssh": a. can be compiled with tcp-wrappers, for tight integration. b. should be run-independently-from tcp-wrappers. c. interferes with the operation of tcp-wrappers. d. precludes using tcp-wrappers. a is the correct answer.	SSH	39
170. "ssh" can be used to replace rsh by: a. replacing the "rsh" binary with the "ssh" binary. b. changing "rshd" to "sshd" in inetd.conf c. renaming "rsh" as "ssh" d. a and b a is the correct answer.	SSH	22
171. Problems with standard UNIX passwords include all of the following, except: a. passwords are too easy to change. b. passwords can be captured by a sniffer. c. encrypted passwords are stored online. d. 8-character password length is too limited. a is the correct answer.	One Time Passwords	4

Question	Section	Page
172. Using a One Time Password system has all of the following features, except: a. the remote machine doesn't know the users re-usable secret password. b. a new password is generated for every login session. c. the new password is no good after it has been used once. d. the user has a re-usable secret password. a is the correct answer.	One Time Passwords	5
173. "Two-factor authentication" involves "something you know" with a. something you have. b. how much you weigh. c. something you don't know. d. the current NTP time. a is the correct answer.	One Time Passwords	7
174. Most commercial OTP systems are either "challenge/response" or: a. synchronous. b. NTP-based. c. kerberos-based. d. asynchronous. a is the correct answer.	One Time Passwords	8
175. Freely available OTP solutions include: a. S/Key b. OPIE c. Passwd+ d. a and b d is the correct answer.	One Time Passwords	11
176. The typical problems faced when deploying OTP solutions include all of the following, except: a. no more external access b. integrating OTP systems with applications. c. user resistance. d. maintaining OTP-modified software. a is the correct answer.	One Time Passwords	12, 13

Question	Section	Page
177. OPIE stores encrypted user secrets is the file: a. /etc/opiekeys b. ~/.secrets c. /etc/opie.conf d. ~/.opiekeys a is the correct answer.	One Time Passwords	17
178. OPIE user secrets are good: a. until the counter decrements to zero. b. until the expiration date is reached. c. until they are changed. d. until the host secret is changed. a is the correct answer.	One Time Passwords	17
179. On a UNIX client system, OPIE replaces all of the following binaries, except: a. netscape b. login c. ftp d. su a is the correct answer.	One Time Passwords	18
180. On a UNIX server system, OPIE runs: a. with replacements for login and in.ftpd b. as opied c. as a replacement for inetd d. b and c a is the correct answer.	One Time Passwords	19, 20
181. Kerberos is all of the following, except a. a session encryption protocol b. trusted 3rd-party authentication protocol c. designed for TCP/IP networks d. shared secret DES key encryption a is the correct answer.	Kerberos	3

Question	Section	Page
182. Kerberos is based on: a. symmetric-key cryptography. b. asymmetric-key cryptography. c. public/private-key cryptography. d. OTP technology. a is the correct answer.	Kerberos	3
183. Using Kerberos on a network requires all of the following, except: a. NFS b. NTP c. DNS d. KDC a is the correct answer.	Kerberos	7
184. The process of initially authenticating a user to Kerberos is: a. kinit b. klogin c. ksetup d. login a is the correct answer.	Kerberos	18
185. Network services that use Kerberos require users to authenticate themselves by presenting credentials in the form of a: a. ticket b. password c. OTP d. public key a is the correct answer.	Kerberos	11
186. After the initial Kerberos authentication process, the user is passed a _____, which prevents them from having to re-authenticate when using Kerberized network services a. ticket granting ticket b. ticket c. OTP d. private key a is the correct answer.	Kerberos	22

Question	Section	Page
187. A Kerberos authentication server is the master key distribution server for a given: a. realm b. domain c. cluster d. subnet a is the correct answer.	Kerberos	26
188. Cross-realm Kerberos authentication is: a. configurable. b. automatic. c. not possible. d. insecure. a is the correct answer.	Kerberos	26
189. In symmetric key cryptography: a. the same key is used for both encryption and decryption. b. different keys are used for encryption and decryption. c. the public key is used for encryption, the private key for decryption. d. the private key is used for encryption, the public key for decryption. a is the correct answer.	Kerberos	9
190. A Kerberos Principal is a. a Kerberos user or service. b. a Kerberos server. c. a user or service in possession of the Kerberos private key. d. any stratum 1 Kerberos server. a is the correct answer.	Kerberos	8
191. The purpose of an incident investigation is to answer all of the following questions, except: a. why b. what c. where d. when a is the correct answer.	UNIX Forensics	9

Question	Section	Page
192. Commonly trojaned UNIX programs include all of the following, except: a. netscape b. ls c. telnet d. libc a is the correct answer.	UNIX Forensics	12
193. Since collecting evidence after a security incident disturbs the system, the first thing to do is: a. record the most volatile evidence. b. make a backup. c. interview the system administrator. d. turn the system off. a is the correct answer.	UNIX Forensics	35
194. Of the following list of computer evidence, which is the most volatile: a. memory b. network connections c. processes d. filesystem a is the correct answer.	UNIX Forensics	36
195. After a security incident, evidence about the local network can be collected using any of the following commands, except: a. /var/log/network b. netstat c. lsof d. firewall logs a is the correct answer.	UNIX Forensics	42

Question	Section	Page
196. After a security incident, evidence about the process system can be collected using any of the following commands, except: a. vmstat b. ps c. ls /proc d. lsof a is the correct answer.	UNIX Forensics	40
197. After a security incident, evidence about the file system can be collected using any of the following commands, except: a. file b. dump c. tar d. dd a is the correct answer.	UNIX Forensics	47, 48, 49
198. Proper handling of evidence includes of all the following, except: a. perform all analysis only on the original evidence. b. take good notes. c. label, sign, seal, and date evidence. d. create backup copies of all evidence. a is the correct answer.	UNIX Forensics	50
199. File integrity can be assessed using all of the following tools, except: a. Swatch b. Tripwire c. Sherpa d. RPM a is the correct answer.	UNIX Forensics	57, 58

Question	Section	Page
200. The steps for computer forensics include all of the following except: a. Determining motive b. Collection and handling c. Event reconstruction d. Evidence inspection and analysis a is the correct answer.	UNIX Forensics	104

Last Updated: October 24th, 2017

Upcoming Training

SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**