Multiple Choice Test
for SANS LevelTwo GIAC Incident Handling Certification
by Brent Stackhouse

Following each question is the book id (4.1 = Computer Security Incident Handling, 4.2 = Computer and Network Hacker Exploits: Step-by-Step, Part 1, and 4.3 = Computer and Network Hacker Exploits: Step-by-Step, Part II), page number(s), and correct answer letter.

1. The six critical steps of incident handling, in order, are:
   A. Prepare, Detect, Eradicate, Contain, Lessons Learned, Recover
   B. Approve, Remove, Improve, Debrief, Simplify, Maintain
   C. Detect, Contain, Remove, Recover, Lessons Learned, Improve
   D. Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned
   * 4.1, p. 32, D
2. Most incidents are not reported by:
   A. Help Desk personnel
   B. Incident Handlers
   C. End Users
   D. Systems Administrators
   * 4.1, p. 5, B
3. In the event that data from an incident is used in court, it's a good idea, during the incident, to:
   A. Eat a quick snack
   B. Work quickly
   C. Take good notes
   D. All the above
   * 4.1, p. 12, C
4. In an incident, full backups should be done:
   A. As soon as possible
   B. After a situation has been completely assessed
   C. When the incident has been resolved
   D. Not at all - full backups should already be available
   * 4.1, p. 18, A
5. One of the pitfalls of incident handling is:
   A. Unrealistic expectations
   B. Restoring from backups that are already compromised
   C. Working with people
   D. All the above
   * 4.1, p. 20, B
6. One of the "Seven Deadly Sins" of incident handling is:
   A. Failure to apply lessons learned
   B. Failure to contain or eradicate
   C. Failure to take notes

D. All of the above
* 4.1, p. 23, D

7. _____ is important when handling an incident:
   A. Testing
   B. Checking
   C. Encrypting
   D. Communicating
   * 4.1, p.25, D
8. When experiencing a Denial-of-Service attack from the Internet, it's a good idea to:
   A. Tighten perimeter defenses
   B. Remove the attacked host from the Internet
   C. Strike back with your own DOS attack
   D. Open up more firewall ports so that the ports under attack aren't as saturated
   * 4.1, p. 27, A
9. "Presumption of Privacy" means:
   A. Users' activities are their business, not the company's
   B. Privacy is a constitutional right
   C. The level of privacy, if any, that a user has on a given company's network or host
   D. Encryption is required on that system
   * 4.1, p. 37, C
10. Policies are:
   A. Only good if they're kept very general
   B. For large companies only
   C. Best decided before an incident instead of during one
   D. Official only when notarized
   * 4.1, pp. 38, 39, C
11. System administrators should not be:
   A. Involved at all in incident handling
   B. Discouraged from reading log files
   C. Allowed access to a compromised system
   D. All of the above
   * 4.1, p. 45, B
12. During an incident, communication to _____ is encouraged:
   A. Your manager
   B. Your security officer
   C. Your Help Desk
   D. All of the above
   * 4.1, p. 60, D
13. Along with communication, the following item(s) are important in the Identification phase of an incident:
   A. Alerting only when sure of the existence of an incident
   B. Information correlation or fusing
   C. Maintaining situational awareness
   D. Both A and B

E. Both B and C
* 4.1, p. 61, E

14. Signs of an incident do not include:
A. Unexplained user accounts
B. Accounting discrepancies
C. Unexplained attempts to write to system files
D. User obtaining root access
* 4.1, p. 62, D

15. When arriving on the scene of an incident, you should:
A. Wait until backups complete before contacting the command center
B. Generate a list of potential witnesses
C. Treat your arrival time as time zero of the incident
D. Assume the information you were given prior to arriving is accurate
* 4.1, p. 68, B

16. When assessing a potentially compromised system, you should:
A. Assume all system binaries are intact
B. Use basic network tools like ping, telnet, and ftp to gather information on a suspected intruder's IP address
C. Discontinue normal system activities as soon as possible
D. Use pristine binaries and your own backup program from your jump kit
* 4.1, pp. 76, 77, D

17. When establishing quarantine boundaries, it's a good idea to:
A. Disconnect all systems on the subnet that the compromised system is on
B. Determine and certify the trustmodel
C. Contact all users on the affected systems
D. A and B
E. B and C
* 4.1, p. 80, B

18. During the eradication phase of incident handling, it's best to:
A. "Nuke from high orbit."
B. Determine the cause of the incident and take action to prevent it from recurring
C. Restore from backups immediately
D. All of the above
* 4.1, p. 82, B

19. Validating a system includes:
A. Asking for a test plan and baseline documentation
B. Getting the system owner to sign that the system is back in full operation
C. Having the support vendor certify the machine as operational
D. B and C
E. A and B
* 4.1, p. 89, E

20. Which of the following are ineffective for defending against malicious code?
A. Monitoring for abnormal outbound traffic
B. Creating a strong configuration management process

C. Server-based anti-virus scanners
D. None of the above
* 4.1, pp. 112 - 115

21.Examples of Denial Of Service attacks include:
A. Smurf
B. Out-of-Band
C. Mail bombing
D. All of the above
* 4.1, pp. 124 - 126. D

22.It is not a good idea when dealing with espionage to:
A. Maintain a small core team
B. Perform target analysis of important information assets and monitor them
C. Shut down all access to the firewall
D. Establish a war room containing copies of the evidence
* 4.1, pp. 130 - 137, C

23.When dealing with unauthorized use, an incident handler should not:
A. Gather evidence from logs, e-mail, and other sources
B. Confront the intruder
C. Recommend policy changes to restrict unauthorized use
D. Ever involve the HR department
* 4.1, pp. 159, 165, B

24.Expert Witness is:
A. A great UNIX tool
B. The best backup tool for Win9x/NT
C. Identical to Tripwire
D. An evidence-gathering tool for FAT file systems
* 4.1, p. 185, D

25.The U.S. Department of Defense standard for safe file deletion:
A. Is 7 wipes, each of which puts random information in the physical location of the file
B. Is 36 wipes, each of which puts random information in the physical location of the file
C. Uses Windows Defragmenter
D. Employs polarity reversal for each sector on the disk
* 4.1, p. 205, A

26.Steganography is:
A. A form of handwriting that uses codewords
B. Hiding files inside other files
C. The process of charting forensics evidence
D. Outdated and only works on IBM mainframes
* 4.1, p. 214, B

27.Depending on the type of system, good forensics commands are:
A. ls -lart, ps -ef, df, find
B. netstat -a, rpm -V filename

C. strings, od, diff
D. All of the above
* 4.1, pp. 227 - 229, D

28.Signs of a sniffer being on your network include:
A. Your firewall logs a lot of traffic to port 135
B. All the routers hang
C. A network card is in promiscuous mode
D. Log files randomly disappear from NT servers
* 4.1, p. 142, C

29.Malicious code examples do not include:
A. Infinite loops
B. Viruses
C. Root kits
D. Easter eggs
* 4.1, p. 106, A

30.Central reporting of incidents can be encouraged by:
A. Rewarding users that report
B. Educating users as they're hired
C. Removing users' computers from the network that don't report
D. A and B
E. A and C
* 4.1, p. 56, D

31.Pick the following false statement about exploits:
A. Does not have to be computer based
B. Is a security hole or takes advantage of a security hole
C. Anything that can be used to compromise a machine
D. Refers only to Internet-connected servers
4.2, p. 8, D

32.Exploits are attacks against:
A. Confidentiality
B. Irrefutability
C. Integrity
D. A and B
E. A and C
* 4.2, p. 9, E

33.Which of the following is not an attack against availability:
A. Denial of Service
B. Disabling user accounts
C. Having the ability to change data
D. Disabling applications from running
* 4.2, p. 12, C

34.An attack over the Internet would involve:
A. Shoulder surfing
B. Unlocked terminals

C. Application hijacking
D. Session hijacking
* 4.2, p. 14, D

35. The following can be exploited:
A. Inference channels
B. Covert channels
C. Services
D. Ports
E. All the above
* 4.2, p. 20, E

36. Which of the following statements about Denial Of Service attacks is true?
A. Are always deliberate
B. Always renders a system permanently unusable
C. Only affect UNIX systems
D. Can be hindered by restricting access to critical accounts and resources
* 4.2, p. 32, D

37. Buffer overflows are not caused by:
A. Buffer trojans
B. Poor programming
C. A lack of error checking
D. Sending unexpected data
* 4.2, p. 33, A

38. Which of the following are not used in password exploits?
A. Automated cracking programs
B. Dictionary attacks
C. L0pht AntiSniff
D. Brute force attacks
* 4.2, p. 34, C

39. Password cracking is not a useful administrative tool for:
A. Tracking user activity
B. Migrating users
C. Recovering forgotten passwords
D. Auditing the strength of passwords
* 4.2, p. 43, A

40. L0pht Crack does not feature:
A. Hybrid cracks
B. SMB packet capture
C. Custom character set
D. Support for UNIX
* 4.2, p. 46, D

41. Ways to protect against password cracking on NT:
A. Have password policy
B. Disable LAN Manager authentication
C. Use L0pht Crack to automatically generate passwords

D. A and B
E. A, B, and C
* 4.2, p. 61, D

42. Passwords do not:
A. Control access
B. Determine access level
C. Potentially create back doors for future access
D. Serve as a first line of defense
* 4.2, p. 69, B

43. Which is true about Crack?
A. Already compiled
B. Works on both NT and Unix
C. Requires lots of CPU time
D. Large amount of disk space
* 4.2, p. 72, C

44. The following utility is needed to view Crack run output:
A. Output
B. Reporter
C. Reader
D. Crack.out
* 4.2, p. 75, B

45. General guidelines for passwords would not include:
A. Accounts are locked after three attempts
B. Passwords change every 90 days
C. Must contain one alpha, one number, and one special character
D. Cannot use previous five passwords
* 4.2, p. 83, B

46. Protect against UNIX Crack by:
A. Avoiding shadow passwords
B. Enforcing a strong password policy
C. Automatically generating passwords
D. Increasing security on /etc/passwd to 777
* 4.2, p. 82, B

47. The Get Admin exploit:
A. Grants normal users administrative rights
B. Grabs the Administrator password from network traffic
C. Disabled all administrative accounts
D. Occurs only on old versions of UNIX
* 4.2, p. 93, A

48. SecHole grants the following to an attacker:
A. Administrator access via Netbios overflows
B. Access to Primary Domain Controller registry images
C. Debug-level access on a system process
D. Web page access via CGI vulnerabilities

* 4.2, p. 103, C

49. Which are not DOS attacks?
   A. Red Button
   B. CPU Hog
   C. Win Nuke
   D. RPC Locator
   * 4.2, p. 135, A

50. The NetMeeting Buffer Overflow attack allows an attacker to:
   A. Immediately compromise an entire NT domain
   B. Gain root access on a Solaris box
   C. Execute arbitrary code on a client's machine
   D. Generate anonymous e-mail from MS Outlook on several machines
   * 4.2, p. 159, C

51. CGI (Common Gateway Interface) Attacks:
   A. Always use port 81
   B. Only affect Netscape products
   C. Allows an attacker to execute arbitrary commands on the web server
   D. Allows an attacker to deny service to an Internet domain
   * 4.2, p. 176, C

52. Which is not true about CGI programs?
   A. Susceptible to buffer underflow attacks
   B. Executed by the web server
   C. Requested by a usually unauthenticated client
   D. Its process has all the privileges of the web server that called it
   * 4.2, p. 179, A

53. Campas is:
   A. The last name of the author of HTTP
   B. A hacker program
   C. A functionality-adding program distributed with NSCA httpd server 1.2
   D. A DOS attack
   * 4.2, p. 188, C

54. The ToolTalk Buffer Overflow is:
   A. A Solaris attack only
   B. An attack that exploits the ToolTalk RPC service
   C. An attack that exploits an inadequate boundary check, allowing stack data to be overwritten
   D. A and B
   E. B and C
   * 4.2, p. 197, E

55. Hack A Tack does not do the following:
   A. Hide its presence in the Windows NT process list
   B. Install a program called expl32.exe in \windows\system\
   C. Place a key in the registry to run itself on startup
   D. Register in the process list as Explorer32

* 4.2, p. 281, A

56.The land Denial-of-Service attack:
   A. Has an IP packet with the same value for source and destination addresses
   B. Has an IP packet with the same value for source and destination ports
   C. Exploits vulnerabilities in some TCP/IP stack implementations
   D. All of the above
   * 4.2, p. 253, D

57.SSPing uses:
   A. ICMP for a Denial-of-Service Attack
   B. IP for a Denial-of-Service Attack
   C. TCP for a Buffer Overflow Attack
   D. ICMP for a Buffer Overflow Attack
   * 4.2, p. 244, A

58.A Denial-of-Service Attack that uses large-sized ICMP packets is:
   A. Syn Flood
   B. SSPing
   C. Ping of Death
   D. ICMPack
   * 4.2, p. 234, C

59.Smurf attacks are not characterized by:
   A. A large amount of ICMP echo traffic being sent to IP broadcast addresses
   B. Spoofed addresses of a victim machine
   C. ACK bits being set on each packet
   D. None of the above
   * 4.2, p. 259, C

60.Good tips for protecting your site include:
   A. Inventory your current software and operating systems
   B. Relying on CERT for alerts about latest exploits
   C. Uniformly applying patches
   D. A and B
   E. A and C
   * 4.2, p. 306, E

61.To perform DNS Cache Poisoning, use:
   A. Netcat
   B. Knark
   C. Jizz
   D. Loki
   * 4.3, p. 83, C

62.Which tool is good for determining open ports through a firewall?
   A. nmap
   B. nessus
   C. netcat
   D. firewalk
   * 4.3, p. 32, C

63.Good defenses against IP Spoofing do not include:
A. Blocking incoming port 80 at the perimeter router
B. Replace r-commands (rsh, rcp, rlogin, etc.) with ssh or lsh
C. Utilize anti-spoof filters at routers and firewalls
D. Do not extend trust relationships outside of the firewall
* 4.3, p. 57, A

64.The best defense against sniffers includes:
A. Using L0pht Crack to ensure strong passwords
B. Using switched Ethernet on critical segments
C. Both A and B
D. None of the above
* 4.3, p. 69, B

65.IP Fragmentation Attacks are not useful for:
A. Avoiding detection by network IDS systems
B. Getting around packet filters in routers and firewalls
C. Scanning networks
D. Disrupting ARP tables
* 4.3, pp. 59, 63, D

66.IP Spoofing means:
A. Pretending to be a different IP address
B. Sending fragmented IP packets
C. Sending fragmented ICMP packets
D. Injecting memory interrupt calls into a system's memory remotely
* 4.3, p. 47, A

67.Which is not a Session Hijacking tool?
A. Hunt
B. Sniffit
C. IPWatcher
D. Juggernaut
* 4.3, pp. 76, 77, B

68.Netcat is used for:
A. Port scanning
B. Transferring data
C. Making connections to open ports
D. Replay attacks
E. All of the above
* 4.3, pp. 93 -94, 96 -97, E

69.Defending against Netcat would not include:
A. Shutting down unused ports
B. Registry lockdown
C. Including a timestamp and cryptographically signing all input for critical apps
D. Applying system patches
* 4.3, p. 100, B

70.Targa is used for:

© SANS Institute 2000 - 2005 Author retains full rights.

A. Denial-of-Service attacks
B. Buffer Overflow attacks
C. IP Fragmentation attacks
D. None of the above
* 4.3, p. 104, A

71. Tribe Flood Network's architecture is not:
A. Clients control the servers
B. Servers do the attacks
C. Peer-to-peer
D. Optimized for Denial-of-Service attacks
* 4.3, p. 107, C

72. The best ways to defend against Distributed Denial-of-Service attacks include:
A. Using both host and network intrusion detection
B. Removing Windows machines from exposed Internet network segments
C. Contacting upstream ISPs to ensure their routers are patched
D. None of the above
* 4.3, p. 115, A

73. Which is true concerning cracking WWW apps?
A. Very difficult to exploit
B. Attackers can usurp the session of another user
C. URL Session Tracking and Hidden Form Elements are not exploitable
D. Cookies are always read only
* 4.3, pp. 120, 121, B

74. Effective defenses against Web Application Cracks include:
A. Ensuring that the entire application is completely covered
B. Prevent accidental session ID collision by making them at least 10 characters
C. Encrypt cookie information
D. Apply timestamps within variables
E. All of the above
* 4.3, p. 123, E

75. Which is not true about Back Orifice 2000?
A. Open Source
B. Only controls Windows machines
C. No default port
D. Shows up in the task list by default
* 4.3, pp. 128, 129, D

76. Back Orifice does which of the following?
A. Change file mode on /etc/passwd and /etc/shadow
B. Randomly change Windows registry settings
C. Exploits Windows shares
D. Packet and application redirection
* 4.3, pp. 132, 133, D

77. Saran Wrap, Silk Rope, Speakeasy, and Trumpet all:
A. Work with Back Orifice 2000

B. Are Denial-of-Service tools
C. Generate large sniffer logs
D. Use 128-bit 3DES encryption
* 4.3, p. 136, A

78.When you defending against BO2K, you should not:
A. Check port 31337, even though it's not the default
B. Install the Microsoft BO2K service pack
C. Look for a "Remote Administration" service
D. Use network intrusion detection to look for BO2K packets
* 4.3, p. 137, B

79.Backdoor, NetBus, DeepThroat, and NetSpy are all:
A. Denial-of-Service attack programs
B. Type of RootKits
C. BO2K look-alikes
D. Free network scanners
* 4.3, p. 139, C

80.RootKits do the following:
A. Remove the root password
B. Install trojanized versions of command programs like find, inetd, ls, and netstat
C. Delete all log files
D. Gain root access on a UNIX box
* 4.3, p. 146, B

81.RootKit defenses include:
A. Running a Tripwire, ISS System Scanner or something similar
B. Changing the root account's name to something else
C. Changing all system binaries with chmod 777 /bin/*
D. All of the above
* 4.3, p. 149, A

82.Knark is a different kind of RootKit because it:
A. Deletes Tripwire logs when it finds them, thus preventing detection
B. Combines root cracking tools with standard trojan binaries
C. Allows all users to login without a password
D. Runs at the kernel level
* 4.3, p. 151, D

83.The best defense against Knark for sensitive systems is:
A. Utilize network and host IDS
B. Look for the presence of /usr/lib/.knark/
C. Build a monolithic module that disallows loadable kernel modules
D. Don't use Windows
* 4.3, p. 160, C

84.remove.c, cloak.c, and wzap.c are all:
A. RootKits
B. Trojans
C. Denial-of-Service attack tools source code

D. Binary log file editors
* 4.3, p. 168, D

85.Log File Alteration defenses do not include:
A. Using a separate server for logging
B. Run Tripwire hourly to check for any changes
C. Using write-once media
D. Encrypting your log files
* 4.3, p. 171, B

86.Reverse WWW Shell is insidious because:
A. It allows an attacker to access a machine with a command line prompt on your network from the outside
B. From a network perspective, t makes it appear that the victim machine is just surfing the web
C. None of the above
D. A and B
* 4.3, p. 172, D

87.The Principle of Least Privileges (POLP) is valuable in defending against:
A. Reverse WWW Shell
B. Loki
C. Knark
D. A and B
E. None of the above
* 4.3, pp. 174, 177, D

88.The following are not useful sites for hacker exploits:
A. www.hackernews.com
B. www.securify.com/packetstorm
C. www.technotronic.com
D. None of the above
* 4.3, pp. 197, 198, D

89.The following mailing lists are useful for security in general, including exploits:
A. Bugtraq
B. CERT
C. Hack Track
D. A and B
E. All of the above
* 4.3, pp. 202, 204, D

90.Netcat runs in either:
A. Client mode or Listen mode
B. Client mode or Server mode
C. Listen mode or Send mode
D. Attack mode or Passive mode
* 4.3, p. 92, A

Last Updated: May 23rd, 2017

Upcoming SANS Penetration Testing

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Madrid 2017	Madrid, Spain	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Virginia Beach SEC504*	Virginia Beach, VA	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Rocky Mountain 2017 - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017 - SEC542: Web App Penetration Testing and Ethical Hacking	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Thailand 2017	Bangkok, Thailand	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017 - SEC560: Network Penetration Testing and Ethical Hacking	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Milan 2017	Milan, Italy	Jun 12, 2017 - Jun 17, 2017	Live Event
Mentor Session - SEC504	Reston, VA	Jun 13, 2017 - Aug 01, 2017	Mentor
Community SANS Nashville SEC542	Nashville, TN	Jun 19, 2017 - Jun 24, 2017	Community SANS
Community SANS Albany SEC560	Albany, NY	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
Community SANS New York SEC542	New York, NY	Jun 26, 2017 - Jul 01, 2017	Community SANS
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Seattle SEC504	Seattle, WA	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS ICS & Energy-Houston 2017	Houston, TX	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Omaha SEC560	Omaha, NE	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC560	Augusta, GA	Jul 12, 2017 - Aug 23, 2017	Mentor