Global Information Assurance Certification Paper

Track 4 Practical – Exam Question Option

The company where I work does not yet have a security policy, firewall, or anything that would allow us to go through the process of an incident in the "proper" way, and since I've started work there, there was only one issue that could even be called an incident, and it was not handled in a manner anything like what is taught in Track 4. I know no one else that works with a computer network here in Japan. So Option 1 would be quite difficult or impossible to complete. I have no personal experience with any hacker exploits other than the ones covered in class, except for occasionally receiving e-mails with suspicious-looking attachments. I considered trying to examine a copy of the recently proliferating "FW:" virus, but I realized that there probably wasn't 10 pages of information that I could get out of it. So in the end I felt that Option 3 was the best way for me to demonstrate my knowledge of the subject matter.

Each section corresponds to one of the books, and the page number within that book is noted after the question is parentheses. The questions are in the order that the references occur in the books, and the correct answer is denoted with "*" after it.

4.1 Incident Handling

1. The four basic steps of enterprise-level incident handling are: (p. 1, also 25-28)
   - A) Contact, Plan, Recover, Defend
   - B) Detect, Defend, Repair, Recover
   - C) Detect, React, Defend, Recover*
   - D) Defend, React, Backup, Restart
2. What is the best thing to have a user do if their computer is involved in an incident? (p. 17)
   - A) Contact you and don't touch anything*
   - B) Check the logs for unusual activity
   - C) Reboot
   - D) Run his virus scanning software
3. The best type of backup to make during the handling of an incident is: (p. 18)
   - A) None; backups are only useful if made before the incident occurs
   - B) A full, file-structure based backup
   - C) An incremental backup
   - D) A binary backup*
4. Which of the following is not one of the six phases of good incident handling? (p. 32)
   - A) Identification
   - B) Lessons Learned
   - C) Research*
   - D) Recovery
5. What is the simplest single action you can take to improve your legal standing in case of an incident? (p. 37, esp. notes)
   - A) Incident handling team training
   - B) Assign an official security "boss"
   - C) Post warning banners on your servers*
   - D) Use out-of-band communications

6. When is the best time to decide whether to involve law enforcement or to "run silent"? (p. 38)
    A) Before any incidents happen, as part of policy*
    B) When the first signs of an incident are detected
    C) When you know the scope of an incident
    D) After things are under control and cleaned up
7. One important way that an incident response team should be like the police force is: (p. 43)
    A) There should be a separate office for them, with a management structure
    B) They should have a uniform of some sort when handling an incident, to be easily identified
    C) In case of a large incident, a command post at the scene should be set up, to report back to a central location*
    D) There should be sheriffs and deputies
8. How should passwords to critical services be handled? (p. 49)
    A) Each member of the trained incident response team should know the passwords for critical systems
    B) Only the system administrator should know the password, for security purposes, and it should not be written down
    C) The system administrator should tell one assistant the password, in case he's not there during an incident
    D) The passwords should be written down and put them in a safe place like a sealed envelope, so that whoever handles the incident can access them if necessary*
9. How many ways of communication should you have? (p. 54)
    A) One, so that everyone knows what means to use
    B) Two, one as a backup in case of failure
    C) Three - this is an area important enough to have two backup means
    D) As many as is practical - you can never have too many*
10. When should a user report something unusual to incident handling personnel? (p. 61)
    A) As soon as he notices it*
    B) After he observes it for a little while and is sure it is really something to worry about, to avoid false alarms
    C) After checking with a coworker to verify that what he is seeing needs investigation
    D) Users should report to their system administrator, never to the incident handling team directly
11. Considering the six primary phases of handling an incident (could list the phases here if you think it is too hard without it), when should a backup be run? (p. 65 notes)
    A) Only before incidents occur, not during an incident
    B) Before the containment phase*
    C) Before the eradication phase
    D) After the recovery phase
12. Where should evidence be gathered and kept? (p. 69)
    A) Nearby the system where it was gathered, to be able to compare it with new log entries, etc.

B) Under the charge of each remote command post, so that it is near the related system but is not likely to get lost

C) All together for the entire incident, in a locked container*

D) None of the above

13. Should you talk with your ISP during an incident? (p. 73)

A) No - you don't want to give away the fact that you have a weakness

B) No - you don't want them to change anything while you are gathering evidence

C) Maybe, but they're not likely to be much help

D) Yes - many ISPs are very good at dealing with incidents and might be able to help with recovery*

14. If an incident is in progress when the time comes for a routine backup, what should you do? (p. 76)

A) If possible, let the backup happen as normal*

B) Backup only systems not effected by the incident

C) Delay the backup until after the containment phase

D) Don't disrupt the process with such scheduled functions until after the whole incident is over and things are cleaned up

15. Which of the following is true? (p. 79)

A) It is important to determine whether a user did something wrong, and take appropriate action as soon as possible, like informing their supervisor.

B) After enough evidence is gathered that it becomes clear that someone internal made a mistake that caused an incident, it should be reported.

C) Fault should never be an issue in incident handling - it is not your job to blame anyone for things going wrong.*

D) All incidents are caused by hackers - by definition, it isn't amybody's fault internally.

16. Which of the following is necessary to do successful eradication? (p. 82)

A) Knowing how many systems were damaged

B) Knowing what caused the incident*

C) Top management approval for changes to the firewall configuration

D) The IP address of the attacker

17. After you have restored a system that was contaminated, what is an important step before turning it back over to the owner? (p. 89)

A) Use it yourself for about a week to make sure it's okay

B) Monitor the user for a while in case it was something he did that caused the failure the first time

C) Get the owner to sign saying that the machine is in working order again*

D) Train the owner in incident handling techniques

18. When writing the reports, how should the team resolve disagreements about what happened? (p. 93)

A) The appointed primary incident handler should have the last word

B) Majority vote

C) Try to reach a consensus among the handlers who were involved*

D) There shouldn't be disagreement - facts are facts

19. The documents passed on to upper management should: (p. 94)
    A) Be complete with details about the incident - leave out nothing
    B) Include the actual changes made to the firewall
    C) Be only a concise summary in non-technical language*
    D) Upper management doesn't need a report unless their individual client PC was involved
20. Which of the following is not an example of malicious code? (p. 106)
    A) Port scans*
    B) Root kit binaries
    C) Hostile applets
    D) Disk based surveys
21. Those who conduct espionage are usually: (p. 129)
    A) Competitors (business-wise or militarily)
    B) Full-time spies
    C) Part of the organization being spied on*
    D) None of the above
22. Which of the following is not typical of attempts to steal passwords? (p. 140)
    A) It is probably done during off-hours
    B) It uses a non-normal source host
    C) The same password is often tried on several systems
    D) It is typically done by sniffing, because guessing passwords is so easy to detect*
23. If your disk light flashes with the same rhythm as the light on your hub for network traffic, a likely cause is: (p. 142)
    A) You are getting many warning e-mail messages from your IDS
    B) You have a sniffer*
    C) Someone is installing a backdoor on your system
    D) None of the above
24. An arrest is: (p. 149)
    A) Accusing someone of a crime
    B) Something you can, and should do if you have reasonable evidence that you know who committed the crime
    C) Depriving a person of their freedom*
    D) Something only employed police officers are allowed to do by law
25. Which of the following is not an example of abusive email? (p. 158)
    A) In-house spam
    B) Hate mail
    C) Using foul language in email messages*
    D) In house chain letters
26. Which is not true about sexually explicit web access at work? (p. 166, 167)
    A) It can lead to addiction

B) Can become a factor in a sexual harassment case
C) Often something everybody knows but no one talks about
D) Is a serious problem, but only the employee is legally liable, not the company itself*

27. What is NTLast? (p. 180)
    A) A tool that helps an NT machine withstand a DoS attack
    B) A hacker tool that provides the most recently logged on userid and password
    C) A tool that keeps a copy of the last version of the registry and status of various system files before configuration changes are made
    D) A tool that can provide a list of recent successful and/or failed logons*
28. Which of the following is not true about SafeBack? (p. 186 notes)
    A) It does a raw data dump from disk to file*
    B) It contains safeguards against tampering
    C) It only runs from a DOS boot
    D) Its sales are restricted to security personnel that may be involved in forensics
29. To tell if you have the virus Picture.exe, look for: (p. 204 notes)
    A) A file called "picture.exe" in your windows/system directory
    B) A file called "note.exe" in your windows directory*
    C) A new macro in Word called "picture"
    D) An extra graphic that displays when your system boots
30. Which is true about forensics on Unix systems? (p. 225)
    A) There are a variety of tools available as open-source that should be used in combination
    B) Without Tripwire, decent forensics is not possible*
    C) Unlike other applications for Unix, the only good forensics tools cost money
    D) None of the above

4.2 Exploits Part 1

1. Which of the following is not a main area of security? (p. 9)
    A) Availability
    B) Dependability*
    C) Integrity
    D) Confidentiality
2. Which of the following is not an exploit using the Internet? (p. 14)
    A) Spoofing
    B) Relaying
    C) Sniffing traffic*
    D) Coordinate attacks
3. Which of the following is not a commonly exploited port? (p. 21, other source also)
    A) 27*
    B) 80

C) 25
D) 53

4. What is IP Spoofing? (p. 30)
   A) Taking over an existing session
   B) Sending a packet with a false source port number
   C) Sending a packet with a false source address*
   D) Listening to traffic on a network

5. A denial of service attack is an attack on which area of security? (p. 32)
   A) Availability*
   B) Dependability
   C) Integrity
   D) Confidentiality

6. Which of the following is not a password cracking tool? (p. 34)
   A) Red Button*
   B) L0phtcrack
   C) John the Ripper
   D) Cracker Jack

7. What is a dictionary attack? (p. 35)
   A) Exploiting a vulnerability in the MS Office spell-checking tools
   B) Guessing passwords using only common words*
   C) Guessing passwords using a hybrid of dictionary words and numbers
   D) Deleting all the dictionary files on a computer

8. How long should you set your password change interval? (p. 36)
   A) 90 days
   B) 30 days
   C) Less than the time it takes to guess a password with a hybrid attack
   D) Less than the time is takes to guess a password with a brute force attack*

9. Which of the following is not a method of password cracking? (p. 42)
   A) Brute force
   B) Dictionary
   C) Decryption*
   D) Hybrid

10. To use L0phtcrack, you must have: (p. 55-56)
    A) Physical access to one of the computers on the network
    B) Administrative access to the server
    C) Either Administrative access to the server or visibility of the network traffic*
    D) Access to the registry on the server

11. Which of the following is not a defense against Crack? (p. 82-83)
    A) Make /etc/passwd readable only by root*
    B) Require alphas, numerics, and special characters in passwords

C) Use the shadow password feature
D) Use one-time passwords

12. Which of these exploits can be used against a Unix machine? (p. 92 & 259)
    A) Sechole
    B) RPC Locator
    C) Smurf*
    D) Net Meeting Buffer Overflow
13. What does Sechole actually do? (p. 103)
    A) Allows entry into the system without a password
    B) Makes modifications to the password file
    C) Grants a regular user to gain debug-level access on a system process*
    D) Grants administrator access through a backdoor
14. Which is not true about a denial of service attack? (p. 115)
    A) It makes a system unusable for legitimate users
    B) It allows hackers into a system*
    C) It can be caused accidently
    D) It can be done against routers
15. What can be done to defend an NT host against CPU Hog? (p. 119)
    A) It cannot be defended against at the host level
    B) Apply the new patch from Microsoft, and then install the service pack
    C) Set the priority of the Task Manager to 16*
    D) Unbind NetBios if it is not needed
16. Which of the following does Red Button provide? (p. 143)
    A) Administrator level privilege
    B) The name of the administrator account*
    C) The opportunity to modify the registry
    D) The ability to crash the machine
17. To run RPC Locator, you would: (p. 156)
    A) Install the software and double-click the icon
    B) Run “rpcloc.exe” from a command line
    C) Telnet to port 135 and type random characters*
    D) This tool is not publicly available
18. What is a buffer overflow? (p. 160)
    A) When the memory of the computer completely fills up
    B) When data coming in from the network exceeds the capability to process it
    C) When data input to a program exceeds what was expected by the developer*
    D) None of the above
19. If you get a buffer overflow on a Windows PC, what are you likely to see? (p. 163)
    A) Your machine will freeze with no message
    B) A dialog box saying that a program has performed an illegal operation*

C) The blue screen of death
D) Nothing immediately; the machine will appear to be running normally

20. CGI exploits are related to which network service? (p. 177)
    A) ftp
    B) sendmail
    C) dns
    D) http*
21. Which of the following is a buffer overflow exploit? (p. 159, 197, 207)
    A) NetMeeting Exploit
    B) ToolTalk
    C) IMAPD Exploit
    D) All of the above*
22. Which of the following is not a defense against IRIX Wrap? (p. 223)
    A) Removing Outbox software from the server
    B) Make the cgi-bin directory writable only by root*
    C) Make the Outbox program writable only by root
    D) Install vendor patches
23. Why are some versions of the sample program PHF vulnerable to exploits? (p. 225)
    A) User inputs are not properly validated*
    B) By default it runs as root
    C) It opens port 80 on non-http servers
    D) None of the above
24. Which of the following is not a defense against the PHF exploit? (p. 231)
    A) Do not run web servers as root
    B) Remove the PHF program
    C) Run swatch to check logs
    D) Filter packets destined for port 80 with "/../" in the contents*
25. Which of the following is not a denial of service attack? (p. 233)
    A) SSPing
    B) Land
    C) Aglimpse*
    D) Smurf
26. What is a Ping of Death? (p. 234)
    A) A spoofed ping sent to a broadcast address so that a flood of answers comes back
    B) A ping packet with a very large payload*
    C) A ping packet with destructive code in its payload
    D) None of the above
27. The source address of a land attack packet is: (p. 253)
    A) Localhost (127.0.0.1)
    B) The address of the host the hacker wants to attack

C) The same as the destination address*
D) The broadcast address of the local network

28. A variant on Smurf is: (p. 259, 263)
    A) Frums
    B) Fraggle*
    C) Blue Guy
    D) None of the above
29. What do you need to configure to defend against SYN Flood attacks? (p. 275)
    A) The router*
    B) The inetd.conf file
    C) The hosts.deny file
    D) You can't defend against it; you can only watch for unusual traffic
30. What does Hack A Tack enable the hacker to do? (p. 287)
    A) Get passwords
    B) Send messages as if from that machine
    C) Force a shutdown of the machine
    D) All of the above*

4.2 Exploits Part 1

1. Which of the following is not a trend happening currently to favor hackers? (p. 11, 12)
    A) Fierce competition between independently working hackers*
    B) Hacker conferences
    C) High quality, easy-to-use hacker tools on the Internet
    D) Fewer system types results in one bug compromising many systems
2. About how many phone numbers can be war-dialed per hour on a single-modem machine? (p. 20)
    A) 10-15
    B) 30-50
    C) 100-125*
    D) 180-240
3. How can you defend against war dialing? (p. 23)
    A) War dial against your own network
    B) Activate scanning detection in your PBX
    C) Unplug all your modems
    D) All of the above*
4. Which of these cannot be done using Nmap? (p. 26-29)
    A) Determining which ports are open
    B) Bounce a scan off a ftp server to hide the source
    C) ICMP scan*
    D) Identify hundreds of operating system versions
5. Firewalk is used to: (p. 32)

A) Find software vulnerabilities in a firewall
B) Find ports that a firewall allows through*
C) Find a way to disable a firewall
D) Find a way to sneak past a firewall's intrusion detection

6. Which of the following is not a vulnerability scanner? (p. 38, 39)
   A) CyberCop
   B) SATAN
   C) Nessus
   D) Gravedigger*
7. By spoofing by simply changing the IP address on your machine, you cannot: (p. 48)
   A) Hide your identity
   B) Initiate DoS attacks
   C) Get responses from servers*
   D) None of the above – you can do all these
8. Which of the following is not important to defend against spoofing? (p. 57)
   A) Disallow source routing
   B) Make sequence numbers truly random
   C) Have your external servers on a screened network*
   D) Avoid trust relationships outside the firewall
9. For the "tiny fragment" trick to work, what should be in the second fragment? (p. 61)
   A) The source IP address
   B) The source port
   C) The destination IP address
   D) The destination port*
10. What exploit does the "fragment overlap" attack use? (p. 62)
   A) The port number is rewritten*
   B) The incongruent offset numbers confuse the firewall
   C) The incongruent offset numbers confuse the server
   D) The server waits forever for the rest of the packet
11. What is the safest firewall type against fragment attacks? (p. 64 and various)
   A) Packet-filtering routers
   B) Packet-filtering firewalls
   C) Proxies*
   D) Host hardening
12. What Ethernet interface feature is used by sniffers? (p. 66)
   A) Switching
   B) Promiscuous mode*
   C) Dual-homed host
   D) Network address translation
13. Which of the following is not a session highjacking tool? (p. 75,77)

A) Hunt
B) Juggernaut
C) TTYWatcher
D) IPSnatch*

14. Which of the following is not a defense against Internet session hijacking? (p. 73, 79)
    A) Strong authentication*
    B) Encryption
    C) Using ssh instead of telnet
    D) VPNs
15. What is DNS cache poisoning? (p. 85-87)
    A) Sending many unresolvable recursive DNS queries to fill up the DNS's memory
    B) Using a buffer overflow exploit to rewrite a DNS's entries
    C) Sending false answers to a recursive DNS server regarding IP/name pairs*
    D) Use the DNS port's caching feature to launch other code on the server
16. Which of the following platforms does NetCat not run on? (p. 91)
    A) Linux
    B) NT*
    C) Solaris
    D) OSF
17. What does the "cat" in NetCat refer to? (p. 91)
    A) It works like the Unix cat command*
    B) It sneaks under IDS systems – like a cat
    C) It is used to join two IP sessions together – to concatenate them
    D) Clever Address Tool
18. A major characteristic of NetCat is: (p. 91-99)
    A) An easy-to-use GUI
    B) Setup is automatic for most systems
    C) Small and simple, so you can use it for almost anything*
    D) Can forge any ICMP message
19. Targa is: (p. 104)
    A) A sophisticated port scanning tool
    B) A bundle of several DoS attacks*
    C) A network sniffing and sorting application
    D) A handy tool for spoofing source addresses
20. In Tribe Flood Network, the clients talk to the servers using: (p. 111)
    A) telnet
    B) echo requests and echo replies
    C) just echo replies*
    D) NetCat
21. Trin00 is: (p. 113)

A) A newer variant on TFN
B) Works on more platforms than TFN
C) Similar to TFN but doesn't use ICMP*
D) Unrelated to TFN

22. What tool is used to edit cookies? (p. 121)
    A) A web browser
    B) A hacker tool such as Internet Exploder
    C) regedit
    D) any text editor*
23. Which of the following will not help to insure the integrity of hidden form elements? (p. 123)
    A) Encrypt them
    B) Use a timestamp in the variable
    C) Require a password from the user*
    D) Use long session Ids
24. Which of the following is not a backdoor? (p. 127, 139)
    A) SecHole*
    B) BO2K
    C) NetSpy
    D) NetBus
25. The RootKits tool suite is considered: (p. 141)
    A) A backdoor
    B) A Trojan horse
    C) Both of the above*
    D) Neither of the above
26. What is a good defense against RootKits? (p. 149)
    A) Good protection for the root account
    B) Tripwire
    C) PGP signatures
    D) All of the above*
27. How does Knark hide from view? (p. 151)
    A) It replaces ls and other commands with its own versions
    B) It makes the kernel lie to any command that might detect it*
    C) It resides in a user directory, which is not normally monitored with tools like Tripwire
    D) All the code resides outside the server, but utilizes a weakness in Unix to gain control
28. Which method cannot stop a hacker with root access from altering Unix log files? (p. 171)
    A) Put the files in a directory that is not root-readable*
    B) Encrypt the logs
    C) Send the logs to another machine
    D) Write the logs on write-once media
29. Reverse WWW Shell is written in: (p. 174)

A) VBS
B) C
C) Perl*
D) Java

30. What does Loki shell access traffic look like to a firewall? (p. 176)
A) Web access
B) Mail messages
C) DNS queries and answers
D) Pings*

Last Updated: May 26th, 2017

Upcoming Training

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	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
Mentor Session - SEC504	Reston, VA	Jun 13, 2017 - Aug 01, 2017	Mentor
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 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
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
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 Sacramento SEC504	Sacramento, CA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Ottawa SEC504	Ottawa, ON	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Annapolis SEC504	Annapolis, MD	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Phoenix SEC504	Phoenix, AZ	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Des Moines SEC504	Des Moines, IA	Jul 24, 2017 - Jul 29, 2017	Community SANS
Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
Community SANS Raleigh SEC504	Raleigh, NC	Aug 07, 2017 - Aug 12, 2017	Community SANS
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event