# Global Information Assurance Certification Paper

**Practical assignment for Advanced Incident Handling and Hacker Exploits certification**

*Steve Riley*
*15 June 2000*

## Incident Handling

1. When beginning an incident handling exercise, you want to act as fast as possible at the first sign of a possible intrusion. *(IH_emergencyresponse.pdf, p.3)*

___ True.
**_x_ False.**

2. Why is it a good idea for more than one person to witness an event or to have correlating logs from two separate sources? *(IH_emergencyresponse.pdf, p.5)*

A. The first person's memory may not be completely accurate.
**B. It increases validity of the observations in any potential court action.**
C. Multiple observations are required by law in some states in order for evidence to be admissible.
D. Some logging software will fail to record certain events.

3. Information about attacks should be shared because: *(IH_emergencyresponse.pdf, p.8)*

A. Attackers themselves share information.
B. Having personally published information about an attack is important in the information security industry.
C. It expands the body of knowledge available to other intrusion detection experts.
**D. A and C only.**
E. None of the above—attacks should be kept secret in order to minimize an organization's legal liabilities.

4. Notes of an incident should include: *(IH_emergencyresponse.pdf, p.12)*

A. Only who, what, and how.
B. Where, why, which, and how many.
**C. At least who, what, when, and where.**
D. Pretty colors and fonts, to demonstrate your word processing prowess.

5. Which is the most difficult to answer?

A. How.
B. Why.

C. Where.
D. When.
**E. Who.**

6. Tools to use for determining the owner of a system include (choose two): *(IH_emergencyresponse.pdf, p.15)*

**A. whois.**
**B. nslookup.**
C. hostname.
D. ipconfig.
E. traceroute.

7. When called to the scene of an incident, as soon as you begin working on an affected system: *(IH_emergencyresponse.pdf, p.19)*

**A. You essentially own the system and anything that happens is your fault.**
B. The system remains under its original ownership; you're only examining it for evidence.

8. The six steps of incident handing are, in the proper order: *(IH_section2.pdf, p.5)*

A. Identification, preparation, containment, eradication, recovery, lessons learned.
**B. Preparation, identification, containment, eradication, recovery, lessons learned.**
C. Preparation, identification, eradication, containment, recovery, lessons learned.
D. Preparation, identification, containment, eradication, lessons learned, recovery.

9. Why are warning banners on systems important? *(IH_section2.pdf, p.8)*

A. It's always a good idea to give users yet another reason to resent your IT department.
B. Like home burglar alarm stickers or signs, warning banners will usually scare off most attackers.
C. Banners can absolve your organization of legal liability.
**D. Warning banners explicitly spell out your organization's privacy policy.**

10. Because attacks happen so quickly, an incident handler should immediately begin examining affected systems, regardless of whether an organization's security policy provides such authorization. *(IH_section2.pdf, p.9)*

___ True.
**_x_ False.**

11. Desire and technical skill are sufficient for someone to join an incident handling team. *(IH_section2.pdf, p.14)*

___ True
**_x_ False**

12. Incident response teams should include: *(IH_section2.pdf, p.15)*

A. Technically-oriented on-site handlers.
B. A command post with communications and management support.
C. A corporate security officer to make any necessary decisions.
**C. Only A and B.**
D. A, B, and C.
E. Only A and C.
F. None of the above.

13. Who is the best person to create a checklist describing how to back up or bring down a system? *(IH_section2.pdf, p.17)*

**A. The system administrator.**
B. The vendor consultant.
C. A third-party consultant specializing in system security.
D. Someone from the organization's incident response team.

14. The "clue closet" is: *(IH_section2.pdf, p.19)*

A. A wallet-size list of the six steps of incident handling.
B. Procedures for backing up a system and containing evidence.
C. A secure location for storing evidence for later forensic analysis.
**D. An incident handler contact list and call tree information.**

15. Sometimes it may be necessary to write down critical passwords and encryption keys, especially if this information needs to be shared with an incident handler. This is acceptable as long as the passwords and keys are stored securely. *(IH_section2.pdf, p.20)*

**_x_ True.**
___ False.

16. Which methods of communication are good for encouraging employees to report suspicious activity? *(IH_section2.pdf, p.22)*

A. Fax.
B. Voice phone.
C. E-mail.
D. Web address.
**E. All of the above.**

17. Since most local law enforcement agencies are busy with their regular duties, it's best not to try to work with them in advance of an actual incident. *(IH_section2.pdf, p.26)*

___ True.
**_x_ False.**

18. A jump bag should include vendor-distributed OS media, since part of the containment process includes nuking and reinstalling the operating system. *(IH_section2.pdf, p.27)*

___ True.
**_x_ False.**

19. Alerting of an actual incident should be done by whom and when: *(IH_section3.pdf, pp.2-3)*

A. Anyone suspicious of an incident; immediately upon suspicion.
B. The organization's security officer; after the incident response team calls a meeting.
**C. The designated handler; early enough to react.**
D. The help desk staff; after verification of an attacker's presence.

20. During an incident, it's important for handlers to take the time to communicate to the help desk, to system administrators, and occasionally to users. *(IH_section3.pdf, p.4)*

**_x_ True.**
___ False.

21. Initial assessment of whether an event is an actual incident should include (choose three): *(IH_section3.pdf, p.8)*

**A. Checking for simple mistakes.**
**B. Examining available evidence in detail.**
C. Watching logs for a few minutes to see if anything else happens.
**D. Thinking of whether there are any other possibilities.**
E. Tracerouting back to any suspicious IP addresses.

22. Before beginning the containment process, system backups should already be done; if not, they should be the first thing the handler should do. *(IH_section3.pdf, p.10)*

**_x_ True.**
___ False.

23. Maintaining a low profile when containing an incident is important. Ways to do this include: *(IH_section3.pdf, p.16)*

A. Using ping and traceroute to try to locate the source of the attack.
**B. Following standard regular operations procedures (like doing the nightly backup).**
C. Neither—maintaining a low profile isn't that important.

24. Occasionally it may be necessary to leave an affected system running. If so, trust relationships can become a point of additional vulnerability. Which trust relationship is probably the most important one to watch? *(IH_section3.pdf, p.19)*

A. Between the organization and its business partners.
B. Between the affected system, all systems it connects to, and all systems they connect to.
C. Between the affected system and all internal users.
**D. Between the affected system, the system administrator's computer, and other systems he/she is responsible for.**

25. Possible ways of improving defenses include: *(IH_section3.pdf, p.24)*

A. Reloading the computer's operating system.
B. Changing the computer's name and IP address.
C. Strengthening router ACLs and firewall rules.
D. Porting the machine's function to a different operating system.
E. All of the above.
**F. B, C, and D only.**
G. A, B, and C only.

26. Running a scanner such as nmap can help identify areas of eradication. Good systems to scan include: *(IH_section3.pdf, p.25)*

A. The affected system only, running nmap on the system itself.
B. The affected system only, running nmap from another system on a hub the affected system is connected to.
**C. The affected system (from another system on a hub the affected system is connected to) and its network neighbors (from another system on that network).**
D. Scanning your own network is never a good idea because it might be a violation of policy.

27. Eradicating viruses is fairly simple, because there are tools for Windows and Unix that will take care of this automatically. *(IH_section3.pdf, p.26)*

___ True
**_x_ False**

28. How can file integrity software help locate compromised code? *(IH_section3.pdf, p.29)*

A. As long as it's installed, it will notify of compromised code automatically.

**B. Compare the results of running it on the affected system to the results of running it on a known good system.**
C. Most compromised code is so well crafted that file integrity software can't detect it anymore.

29. After you've finished restoring the system to full integrity and patched all compromise vectors, your work is done and you can put the system back into production. *(IH_section3.pdf, pp.30-31)*

___ True
**_x_ False**

30. In the follow-up report (choose three): *(IH_section3.pdf, pp.34-35)*

A. Everyone on the incident response team contributes to the report; consensus is necessary.
**B. The primary incident handler writes the report; consensus should be a goal but not a requirement; objections should be noted.**
C. Organizational policy that hindered the response should be omitted from this report.
**D. Organizational policy that hindered the response should be included in this report.**
**E. The executive summary should illustrate the organization's cost savings provided by having a response policy.**
F. The executive summary should describe who attacked the system and how he/she was punished.

## Hacker Exploits, part 1

1. Confidentiality is: *(Network exploits, 22 March, book 1, p.9)*

A. Ensuring that data isn't modified by an unauthorized party.
**B. Ensuring that unauthorized access is prevented.**
C. Ensuring that authorized users aren't denied service.

2. Integrity is: *(Network exploits, 22 March, book 1, p.9)*

**A. Ensuring that data isn't modified by an unauthorized party.**
B. Ensuring that unauthorized access is prevented.
C. Ensuring that authorized users aren't denied service.

3. Attacks against availability are often the most difficult to defend against. *(Network exploits, 22 March, book 1, p.12)*

**_x_ True.**
___ False.

4. Session hijacking: *(Network exploits, 22 March, book 1, p.14)*

**A. Works because authentication happens only at the beginning of a session but is good for the entire session.**
B. Doesn't work because logon information is usually encrypted or hashed.

5. As long as someone identifies him/herself as a representative of your organization's IT group, it's okay to give out your password over the phone even if you didn't make the initial call. *(Network exploits, 22 March, book 1, p.19)*

___ True.
**_x_ False.**

6. Which of the following application and port pairs is known for being vulnerable to a very high number of exploits? *(Network exploits, 22 March, book 1, p.21)*

A. http on 80/tcp.
B. telnet on 119/tcp.
C. nntp on 119/tcp.
**D. smtp on 25/tcp.**
E. smtp on 23/tcp.

7. One way to exploit the trust between two machines is to spoof IP packets such that: *(Network exploits, 22 March, book 1, p.30)*

**A. The source address of outgoing packets is changed to make the packets appear to have originated from within the attacked network.**
B. The source address of outgoing packets is changed to make the packets appear to have originated from some other network.

8. Does session hijacking also involve denial of service? *(Network exploits, 22 March, book 1, p.31)*

A. No.
B. Yes, to the destination machine.
**C. Yes, to the machine which originally made the connection.**

9. Is it necessarily always a good policy to have a minimum password length? *(Network exploits, 22 March, book 1, p.36)*

A. Yes—minimum lengths disallow short passwords that are often easy to obtain via brute force.
**B. No—minimum lengths can speed up some brute force attacks because they eliminate part of the potential key space.**

10. Asymmetric encryption uses two identical keys, differing only in that one is designed for encryption and the other is designed for decryption. *(Network exploits, 22 March, book 1, p.39)*

___ True.
**_x_ False.**

11. Why is password cracking useful? *(Network exploits, 22 March, book 1, p.43)*

A. Auditing password strength.
B. Administrators should keep a list of all user passwords.
C. Recovering forgotten or unknown passwords.
D. Migrating users to other platforms.
E. A, B, and C only.
**F. A, C, and D only.**

12. Which two weaknesses allow for L0phtCrack to work so well? *(Network exploits, 22 March, book 1, p.44)*

A. Having a graphical interface makes it too easy to use.
**B. NT passwords are divided into two seven-character pieces before being hashed.**
**C. NT doesn't add salt to the password before computing the hash.**
D. The hash algorithm is well known.

13. The SYSKEY hotfix for Windows NT (choose two): *(Network exploits, 22 March, book 1, p.66)*

A. Provides a way to enforce password policies.
**B. Is included in Service Pack 3.**
C. Eliminates the seven-character division of NT passwords.
D. Disables LANMAN and NTLMv1 authentication.
**E. Allows for 128-bit ("strong") encryption of password information stored in the registry.**

14. Most modern Unix operating systems don't, by default, prevent or make it difficult for attackers to read (but not necessarily comprehend or utilize) the password file. *(Network exploits, 22 March, book 1, p.69)*

**_x_ True.**
___ False.

15. Crack can crack Unix passwords by: *(Network exploits, 22 March, book 1, p.70)*

**A. Performing its work against the password file.**
B. Watching logon traffic over the network.
C. Both of the above.

16. A shadow file (choose two): *(Network exploits, 22 March, book 1, p.85)*

A. Stores real IDs with bogus passwords in /etc/passwd and real passwords in /etc/shadow.
B. Stores bogus IDs and passwords in /etc/password and real IDs and passwords in /etc/shadow.
**C. Stores IDs in /etc/password and real passwords in /etc/shadow.**
**D. Has restricted read access.**
E. Is hidden from casual snooping.

17. One-time passwords are essentially uncrackable because there really is no password to guess. *(Network exploits, 22 March, book 1, p.88)*

**_x_ True.**
___ False.

18. GetAdmin is: *(Network exploits, 22 March, book 1, p.94)*

**A. An NT exploit that can attach to any process and set a global flag.**
B. An NT buffer overflow that adds the logged in user to the system's local Administrators group.

19. SecHole is: *(Network exploits, 22 March, book 1, p.104)*

A. A Unix exploit that can be used to create several kinds of security holes.
B. A Unix buffer overflow that is executable from a CGI-based web page.
**C. An NT exploit that can be detected if an application calls DebugActiveProcess.**

20. CPUHog could easily be prevented from consuming all resources if Windows NT would: *(Network exploits, 22 March, book 1, p.116)*

A. Allow task manager to run at a priority higher than 16.
B. Provide a way to limit CPU usage by user.
C. Automatically decrease the priority of the higest-priority processes when other applications become CPU starved.
**D. All of the above.**

21. WinNuke sends what kind of data to which service: *(Network exploits, 22 March, book 1, p.126)*

A. Floods of SYN packets to http.
**B. Any packet with the URG flag to NetBIOS.**
C. Any packet with a specially-crafted sequence number to the RPC locator.
D. Floods of RST packets to SMTP.

22. When RedButton connects to a remote computer, it can: *(Network exploits, 22 March, book 1, p.143)*

**A. Identify the administrator account even it's been renamed; list all of the shares.**
B. Not identify the administrator account; list and connect to all of the shares.
C. Identify the administrator account; list only the administrative shares.
D. Identify the administrator account; list and connect to all of the shares.
E. Not identify the administrator account; connect only to administrative shares.

23. You can exploit a flaw in what service on which port by doing what? *(Network exploits, 22 March, book 1, p.146)*

A. RPCSS.EXE; 135; telneting and sending a specific string of characters.
B. RPCSS.EXE; 137; telneting and sending a specific string of characters.
**C. RPCSS.EXE; 135; telneting and sending any random short string.**
D. LSASS.EXE; 135; telneting and sending any random short string.
E. LSASS.EXE; 137; telneting and sending a specific string of characters.

24. You can protect your web server from attacks against aglimpse by (choose two): *(Network exploits, 22 March, book 1, p.185)*

A. Changing the permissions so that only root has write access to httpd's configuration files.
**B. Not running httpd as root.**
C. Replacing the aglimpse script with wglimpse.
**D. Replacing the aglimpse script with webglimpse.**
E. Running the web server on a hidden port.

25. Campas is: *(Network exploits, 22 March, book 1, p.188)*

**A. A CGI script that can provide a means to carry out an attack.**
B. A CGI script that carries malicious code.
C. A CGI script that screens out most bad input but has a few known vulnerabilities.
D. A CGI script that passes commands to the web server when those commands are bracketed by "%a".

26. One way to protect ToolTalk from attacks is to: *(Network exploits, 22 March, book 1, p.204)*

A. Only allow TCP connections (no UDP) to ToolTalk.
B. Create a tooltalk.rc file and add the IP addresses of trusted systems. This effectively disables access from other systems.
**C. At the firewall, filter incoming SYN packets addressed to high ports.**
D. Disable the ToolTalk service.

27. Strong authentication, like that provided by Kerberos or SecurID cards, is one way of reducing IMAP's vulnerability. *(Network exploits, 22 March, book 1, p.214)*

**_x_ True.**

___ False.

28. Which of the following are correct (choose two)? *(Network exploits, 22 March, book 1, pp.234, 243)*

**A. Ping of Death sends one very large ICMP packet to the target.**
B. Ping of Death sends several large, highly fragmented ICMP packets to the target.
C. SSPing sends one very large ICMP packet to the target.
**D. SSPing sends several large, highly fragmented ICMP packets to the target.**

29. A Land attack is: *(Network exploits, 22 March, book 1, p.251)*

A. Sending a large number of SYN packets to a target, creating many half-open connections.
**B. Sending a packet where the source address and port number are the same as the destination.**
C. Sending forged ICMP packets to a broadcast address, causing the victim machine to be overwhelmed with replies.

30. A Smurf attack is: *(Network exploits, 22 March, book 1, p.259)*

A. Sending a large number of SYN packets to a target, creating many half-open connections.
B. Sending a packet where the source address and port number are the same as the destination.
**C. Sending forged ICMP packets to a broadcast address, causing the victim machine to be overwhelmed with replies.**

## Hacker Exploits, part 2

1. That there are fewer types of systems today: *(Network exploits, 23 March, book 2, p.12)*

A. Is a good thing, because security professionals can focus all their knowledge and understanding toward a limited number of well-known systems, making it easier to keep these systems secure.
**B. Is a bad thing, because reduced biodiversity increases our vulnerability.**

2. It is generally safe to identify machines that face the Internet with names that indicate their function. *(Network exploits, 23 March, book 2, p.15)*

___ True.
**_x_ False.**

3. THC-Scan is: *(Network exploits, 23 March, book 2, p.21)*

A. A tool used to find marijuana stashes in your organization.

B. A war dialing program with a feature that allows it to bypass PBX scan detection algorithms and dial without stopping.
**C. A war dialing program with the ability to spread the dialing work among multiple machines.**

4. Nmap can often identify the operating system of the machine it is scanning by: *(Network exploits, 23 March, book 2, p.28)*

**A. Sending various forms of illegal packets and comparing the responses against a database.**
B. Issuing certain undocumented calls that force an IP stack to reveal OS information.
C. Nudging some well-known ports, looking for any kind of identifiable response.

5. Stealth scans often go undetected because: *(Network exploits, 23 March, book 2, p.27)*

A. Most firewalls block unsolicited inbound ACKs.
B. Nmap is available only for Unix, which is used primarily by seasoned hackers who know how to hide. New hackers only use Windows, for which there currently is no version of Nmap.
C. Stealth scans don't wait for the SYN-ACK return from their target.
**D. Most systems don't log a connection until the three-way handshake completes.**

6. Firewalk can determine the rules of which kind of firewall: *(Network exploits, 23 March, book 2, p.33)*

**A. Packet filter.**
B. Proxy.
C. Both.
D. Neither.

7. Vulnerability scanners such as Nessus: *(Network exploits, 23 March, book 2, p.38)*

A. Incorporate heuristic algorithms (similar to those used by anti-virus programs) to scan for known and unknown vulnerabilities.
**B. Scan only for known vulnerabilities based on signatures.**

8. Alice and Bob are communicating. Eve attempts to step in. In a source route spoof: *(Network exploits, 23 March, book 2, p.57)*

**A. Eve crafts packets to make them appear as if they came from Alice and can intercept packets from Bob on their return to Alice.**
B. Eve must fly blind for a while since all replies will be directed toward Alice.
C. RSTs from Alice provide clues to Bob that some traffic isn't really from Alice.

9. Why is authentication based on IP address not a good idea? *(Network exploits, 23 March, book 2, p.57)*

A. IP addresses are easily spoofed.

B. Address authentication doesn't really indicate who is doing something—only which machine is being used.
C. In a DHCP environment, IP addresses are transient.
**D. All of the above.**

10. Fragrouter is tool that: *(Network exploits, 23 March, book 2, p.63)*

A. Performs router DOS attacks by flooding a router with packet fragments.
B. Maps an internal network by sending packet fragments through most firewalls.
**C. Attacks an internal network by using packet fragments to sneak data past firewalls.**

11. The best way to defend against network sniffers is to: *(Network exploits, 23 March, book 2, p.69)*

A. Install L0pht's AntiSniff tool.
**B. Use switched Ethernet on exposed network segments, particularly the DMZ.**
C. Add ingress and egress filters to the DMZ router's ACL.
D. There is no way to defend against sniffing.

12. Hunt avoids ACK storms by exploiting a vulnerability in: *(Network exploits, 23 March, book 2, p.76)*

**A. Gratuitous ARP.**
B. Unsolicited ARP.
C. Gratuitous RARP.
D. Unsolicited RARP.

13. Which is the better way to securely manage your infrastructure? *(Network exploits, 23 March, book 2, p.79)*

A. Install an additional NIC in every device and build a separate, secure management network. Tightly control who has access to this network and religiously monitor all logs.
**B. Use protocols with strong authentication and encryption such as ssh, SSL telnet, or a VPN.**

14. In DNS cache poisoning: *(Network exploits, 23 March, book 2, pp.85-87)*

A. An attacker alters a victim's DNS server so that its cache file contains incorrect root hints, thus redirecting all recursive queries to the attacker's DNS server.
B. An attacker alters a victim's local resolver cache, redirecting certain lookups to the attacker's machine.
**C. An attacker alters the cache of a victim's DNS server so that certain lookups are resolved to the attacker's machine.**

15. Netcat is an extremely useful tool, enabling many kinds of potential abuse. However, it is possible to detect the existence of Netcat using which commands: *(Network exploits, 23 March, book 2, pp.91-100)*

A. netstat.
B. A process viewing utility.
**C. Both.**
D. Neither.

16. Which packet type does TFN use for communication between the clients and the servers (zombies)? *(Network exploits, 23 March, book 2, p.108)*

**A. ICMP_ECHOREPLY.**
B. ICMP_ECHO.
C. UDP_ECHOREPLY.
D. UDP_ECHO.

17. Trin00 uses which three ports by default? *(Network exploits, 23 March, book 2, p.114)*

**A. 27665/tcp**
B. 27665/udp
C. 31337/udp
**D. 37444/udp**
E. 31335/udp
**F. 31335/tcp**

18. Is it sufficient simply to use SSL to encrypt the communications between a web client and server, or should stored state information (cookies, form elements) also be encrypted? *(Network exploits, 23 March, book 2, p.123)*

A. Just use SSL.
**B. Use SSL and encrypt state information.**

19. A Trojan horse is a program that: *(Network exploits, 23 March, book 2, p.126)*

**A. Pretends to be something useful but is actually quite dangerous.**
B. Allows an attacker to access a system, bypassing any security controls.
C. Usually can't be detected even by modern anti-virus tools.

20. Back Orifice 2000 is: *(Network exploits, 23 March, book 2, p.126)*

A. A Trojan horse.
B. A backdoor.
**C. Both.**

21. Back Orifice 2000 packets have a definite pattern that an IDS can detect. *(Network exploits, 23 March, book 2, p.137)*

**_x_ True.**
___ False.

22. Rootkits allow an attacker to obtain root access to a system. *(Network exploits, 23 March, book 2, p.141)*

___ True.
**_x_ False.**

23. How do rootkits hide themselves? *(Network exploits, 23 March, book 2, p.147)*

A. By modifying logs.
B. By installing Trojans.
C. By altering the command shell.
**D. Both A and B.**
E. Both A and C.

24. Knark takes advantage of which Unix feature to really harm a machine? *(Network exploits, 23 March, book 2, p.152)*

A. Remote command shells.
**B. Loadable kernel modules.**
C. Known portmapper holes.
D. Preinstalled C compilers.

25. Running tripwire against a knarked machine will reveal the existence of knark. *(Network exploits, 23 March, book 2, p.154)*

___ True.
**_x_ False.**

26. Which of the following can edit Unix binary logs (choose three)? *(Network exploits, 23 March, book 2, p.168)*

**A. remove.c.**
**B. wtmped.c.**
**C. wzap.c.**
D. editlog.c.
E. unwho.c.
F. logmod.c.

27. There are utilities for editing NT's log files. *(Network exploits, 23 March, book 2, p.170)*

___ True.
**_x_ False.**

28. Defending against attacks like reverse WWW shell involves POLP. What is POLP? *(Network exploits, 23 March, book 2, p.174)*

A. Privileges of lowest potential.
B. Practice of least privileges.
C. Practice of lowest privileges.
D. Principle of lowest privileges.
**E. Principle of least privileges.**

29. Loki can be thought of as: *(Network exploits, 23 March, book 2, p.175)*

A. Telnet over ICMP.
B. Telnet over DNS.
**C. Both.**
D. Neither.

30. Is it actually possible ever to evolve to a really secure world? *(Network exploits, 23 March, book 2, p.195)*

**_x_ Yes, if vendors decide that it's more important than short-term market gains.**
___ No, we never will.

Last Updated: July 25th, 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 New York City 2017 | New York City, NY | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Salt Lake City 2017 | Salt Lake City, UT | 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 |
| 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 |
| SANS London September 2017 | London, United Kingdom | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Mentor Session - SEC504 | Boston, MA | Sep 26, 2017 - Nov 07, 2017 | Mentor |
| SANS DFIR Prague 2017 | Prague, Czech Republic | Oct 02, 2017 - Oct 08, 2017 | Live Event |
| Mentor Session AW - SEC504 | Houston, TX | Oct 02, 2017 - Dec 11, 2017 | Mentor |
| 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 |