Global Information Assurance Certification Paper

Tim Lund

SANS2000 San Jose

GIAC Advanced Incident Handling and Hacker Exploits

Curriculum Practical Assignment for SNAP San Jose

1. An exploit:

   A. Has to be computer based

   B. **Is anything that can be used to compromise a machine**

   C. Cannot involve social engineering

   D. Always occur at the application level

   Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 8

2. The three main areas of security are:

   A. Physical, Social & Environmental

   B. Host, Network & Media

   C. **Confidentiality, Integrity & Availability**

   D. Hardware, Software & Data

   Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 9

3. An example of an attack against confidentiality is:

   A. Changing an account balance

   B. **Gaining unauthorized access**

C. Executing a buffer overflow

D. All of the above

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 10

4. An example of an attack against integrity is:

A. **Changing an account balance**

B. Gaining unauthorized access

C. Executing a buffer overflow

D. None of the above

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 11

5. An example of an attack against availability is:

A. Gaining read access to sensitive information

B. **Denying access to resources**

C. Having the ability to change data

D. All of the above

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 12

5. A Buffer overflow:

A. Requires taking over an existing session.

B. Requires fooling another system into thinking you are a different machine

C. Requires overloading resources so no one else can use them

D. **Requires from sending data to a program that it is not expecting**

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 33

5. To protect against CPU Hog:

A. **Give Task Manager level 16 priority**

B. Run the web server with a user account having minimal permissions

C. Disable access to port 135

D. Limit portmapper access from the internet

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 119

5. Which is not an NT DOS exploit:

A. RPC Locator

B. **Red Button**

C. Win Nuke

D. SSPing

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 135

5. Hack A Tack is:

A. A buffer overflow exploit

B. A Denial of Service exploit

C. A password exploit

D. **A remote trojan exploit**

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 279

5. The result of sechole is:

A. Adds a user to the administrators group

B. 100% utilization of the target host

C. **Allows a non-administrative user to gain debug-level access on a system process.**

D. Allows a non-administrative user to read the registry and view shares

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 103

5. The aglimpse exploit:

A. Allows stack data to be overwritten by user data on an NT server

B. **Allows execution of arbitrary commands on a Unix server**

C. Allows any world readable directory to be viewed by a remote user

D. Allows a user administrative privileges on an NT server

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 176

5. Which of the following is **not** true:

A. Most passwords are trivial to guess

B. Most passwords are rarely changed

C. Many systems have accounts with no passwords

D. **Some passwords cannot be cracked**

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 24 & 36

5. The land exploit works by:

   A. Sending an ICMP packet to a broadcast address

   B. Sending only TCP SYN packets to create half-open connections

   C. **Sending a TCP SYN packet with the same target and source address and port number**

   D. Sending an oversized ICMP packet.

   Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 251

5. The ping of death exploit works by:

   A. Sending an ICMP packet to a broadcast address

   B. Sending only TCP SYN packets to create half-open connections

   C. Sending a TCP SYN packet with the same target and source address and port number

   D. **Sending an oversized ICMP packet.**

   Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 235

5. The smurf exploit works by:

   A. **Sending an ICMP packet to a broadcast address**

   B. Sending only TCP SYN packets to create half-open connections

   C. Sending a TCP SYN packet with the same target and source address and port number

   D. Sending an oversized ICMP packet.

   Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 259

5. The syn flood exploit works by:

   A. Sending an ICMP packet to a broadcast address

   B. **Sending only TCP SYN packets to create half-open connections**

   C. Sending a TCP SYN packet with the same target and source address and port number

   D. Sending an oversized ICMP packet.

   Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 269

5. Encryption which transforms plain text to irreversible cipher text is:

   A. Symmetric encryption

   B. **Hash functions**

   C. Asymmetric encryption

   D. All of the above

   Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 39

5. Symmetric encryption uses:

   A. **A single key**

   B. A public and private key

   C. A hash function

   D. None of the above

   Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 39

5. Win Nuke sends:

A. 10 characters to port 135 followed by a carriage return

B. A gratuitous ARP

C. In band data to port 135

D. **Out of band data to port 139**

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 123

5. A good password policy should **not** include:

A. Require passwords to contain at least one alpha, one number and one special character

B. Require the password change interval to be less than the time to brute force a password

C. **Allowing users to re-use the previous 5 passwords**

D. Restricting users from using birthdays as passwords

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 36, 64 * 65

5. The fastest method for cracking passwords is:

A. Hybrid attack

B. **Dictionary attack**

C. Brute force attack

D. Land attack

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 42

5. A salt is:

   A. A type of brute force attack

   B. An encrypted password

   C. **A random string meant to randomize a password**

   D. Required by NT passprop utility

   Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 44

5. Implementing SYSKey:

   A. Creates a new key called PASSFILT

   B. Requires passwords contain at least 6 characters

   C. Works only on domain controllers

   D. **Allows 128 bit encryption**

   Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 66

5. The IMAPD exploit:

   A. Allows any world readable directory to be viewed by a remote user

   B. Sends out of band data to port 135

   C. **Issues an AUTHENTICATE command larger than 1024-bytes**

   D. Utilizes an HTTP Get method

   Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 209

5. Which is **not** a denial of service attack:

A. Smurf

B. Land

C. Fraggle

D. **Campas**

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 188 & 233

5. A CGI program is:

A. Executed by the client

B. Most secure when run with root privileges

C. **Executed by the server**

D. Always hacker proof

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 189

5. The maximum packet size for TCP/IP is

A. 8 bits

B. **65536 octets**

C. 20 octets

D. 256 k

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 237

5. Red Button Works by remotely logging onto

A. **A target machine without authentication**

B. A target machine by hijacking an active session

C. A unix workstation

D. A target machine by spoofing an ip address

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 136

5. Which of the following is not a version of passwd?

A. npasswd

B. anlpasswd

C. **npasswd+**

D. passwd+

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 90

5. Which is **not** a category of exploit

A. Over the Internet

B. Locally

C. Off-line

D. **IP Service**

Computer and Network Hacker Exploits: Step-by-Step, Part 1 pg. 13

5. An example of a vulnerability scanner is:

A. Nmap

B. **Nessus**

C. THC-Scan

D. Firewalk

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 38

5. With the nessus architecture, the client and server can never:

A. Be on different networks

B. Run on the same machine

C. **Run on windows 98**

D. Send encrypted information

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 40

5. ___ is a packet sniffer:

A. **Tcpdump**

B. Hunt

C. Nessus

D. Nmap

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 67

5. Session hijacking utilizes:

A. DNS cache poisoning

B. Incrementing packet TTLs

C. ARP **spoofing**

D. UDP scanning

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 75

5. An example of a distributed DOS attack is::

A. Targa

B. Smurf

C. Fraggle

D. **Trin00**

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 114

5. Ack storms can result from:

A. DNS cache poisoning

B. **Session hijacking**

C. Tribe Flood Network 2000

D. Trin00

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 74

5. Rootkits do not:

A. **Allow an attacker to gain root access**

B. Allow an attacker to gain backdoor access into a system

C. Allow an attacker to sniff the network

D. Allow an attacker to replace critical system programs with modified versions

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 141

5. A trojan horse is

   A. A program that targets technology

   B. **A program that looks innocuous, but is really sinister**

   C. A program that targets hardware

   D. A program that only affects other applications

   Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 126 & 127

5. The remove program allows an attacker:

   A. To change data in the process accounting files

   B. To change data in the SECURITY.LOG FILE

   C. To change data in the APLICATION.LOG File

   D. **To change data in the lastlog file**

   Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 168

5. An example of a port scanner is:

   A. **Nmap**

   B. Nessus

   C. THC-Scan

   D. Firewalk

   Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 25

6. Defenses for covering tracks does not include:

   A. Using a separate server for logging

   B. Using write-once media for logging

   C. Encrypting log files

   D. **Shutting of logging**

   Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 171

5. Knark:

   A. Runs at the application level

   B. Can be detected by tripwire

   C. **Is a trojan kernel module**

   D. Runs on several versions of unix

   Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 151 & 152

5. The reverse www shell does **not**:

   A. Support authenticating through a web proxy with a static password

   B. **Support HTTPS**

   C. Require the placement of a daemon on an internal host

   D. Provide an attacker a command line shell

   Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 172

5. Which of the following is **not** used in IP address spoofing:

   A. Exploit Trust

   B. Change Address

   C. **Packet Fragmentation**

   D. Source Routing

   Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 47

5. TFN communicates between the client and server by:

   A. Using fragmented ip packets

   B. **Using ICMP_ECHO reply packets**

   C. Using HTTP GET method

   D. Using ICMP_ECHO request packets

   Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 108

5. Which of the following is **not a defense against Knark**

   A. Don't let the attacker get root in the first place

   B. Use LCAP

   C. Build a monolithic kernel

   D. **Use cryptographic hashes of key system files**

   Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 159 & 160

5. To Defend against being a part of a distributed denial of service attack:

A. Install host-based intrusion detection on internet systems

B. Use network-based intrusion detection to discover Trin00 default ports

C. Keep systems patched

D. **All of the above**

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 115

5. Which of the following is not normally affected by a rootkit installation:

A. ls -l

B. ps -ef

C. **echo ***

D. ifconfig -a

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 146 & 148

5. Back orifice 2000 default port is:

A. UDP port 31337

B. **Does not have a default port**

C. TCP port 11000

D. UDP port 31338

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 129

5. An example of a war dialer is:

A. Nmap

B. Nessus

C. **THC-Scan**

D. Firewalk

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 19

5. Loki provides shell access over:

A. **ICMP**

B. HTTP

C. IMAP

D. None of the Above

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 175

5. Source routing is used in which exploit:

A. IP fragmentation attacks

B. Session hijacking attacks

C. **IP address spoofing attacks**

D. Denial of service attacks

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 55

5. Which service is **not** commonly used for reconnaissance:

A. ARIN

B. Whois

C. DNS

D. **None of the above**

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 15

5. THC-Scan:

A. Performs TCP stack fingerprinting

B. **Dials a sequence of telephone numbers to locate modem carriers.**

C. Performs vulnerability scans on remote systems.

D. Searches a target for open ports

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 18

5. Which tool is the Swiss Army knife of tools:

A. Nessus

B. Nmap

C. Knark

D. **Netcat**

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 91

5. To defend against loki:

A. Use static ARP entries on servers & network gateways

B. Configure routers and servers to reconfigure packets before making filtering decisions

C. Filter source routed packets on network gateways

D. **None of the above**

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 177

5. To cover an attackers tracks on NT an attacker would have to, at a minimum:

A. **Delete SECEVENT.EVT**

B. Modify SYSTEM.LOG

C. Change the datestamp on APPLICATION.LOG

D. All of the above

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 169

5. IP fragmentation attacks:

A. Do not work against firewall hosts

B. Do not work against routers

C. Do not work against intrusion detection software

D. **Work against all three**

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 59

5. Sniffers are useful in executing a:

A. Smurf attack

B. **Island Hopping Attack**

C. Trin00 attack

D. None of the above

Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg. 67

5. To defend against DNS cache poisoning:

   A. Use a version of BIND, which does not allow multiple responses for other domains

   B. Implement a split-split DNS architecture

   C. Use a version of BIND, which has difficult-to-predict Query IDs

   D. **All of the above**

   Computer and Network Hacker Exploits: Step-by-Step, Part 2 pg.

5. When handling an incident the handler should:

   A. Remain calm

   B. Take good notes

   C. Do not hurry

   D. **All of the above**

   Computer Security Incident Handling pg. 11

5. The second most common error in incident handling is:

   A. Failure to analyze lessons learned

   B. **Failure to make a good working backup**

   C. Failure to take complete notes

   D. Failure to secure the area

   Computer Security Incident Handling pg. 18

5. Which is a necessary step of contingency planning:

   A. Selecting contingency strategies

   B. Identifying critical functions

   C. Identifying critical resources

   D. **All of the above**

   Computer Security Incident Handling pg. 4

5. After detection the two main goals should be:

   A. Identify the source & place the system into service asap

   B. **Handle individual incidents & maintain an enterprise view**

   C. Contain the problem & backup the compromised host

   D. Create good notes & use out of band communications

   Computer Security Incident Handling pg. 8

5. A honey pot is:

   A. A backdoor application

   B. Slang for a system that has been hacked

   C. **A system that is designed to collect information about an attacker without yielding any useful data**

   D. An application exploit

   Computer Security Incident Handling pg. 83

5. An example of malicious code is:

   A. Viruses

   B. Easter Eggs

   C. Disk based surveys

   D. **ALL of the above**

   Computer Security Incident Handling pg. 106

5. The primary phases of intrusion detection are:

   A. Training, documentation, backups, identification, restoration

   B. Preparation**, identification, containment, eradication, recovery, lessons learned**

   C. Management, detection, notification, reaction

   D. Defense, detection, triage, treatment

   Computer Security Incident Handling pg. 32

5. The follow-up report draft should only be reviewed by:

   A. **All affected parties**

   B. The intrusion detection/handling team

   C. The companies security management

   D. The system owners

   Computer Security Incident Handling pg. 93

5. Malicious code may be detected by:

A. Enforcing a strong configuration management process which will highlight abnormal patterns

B. Network monitoring systems looking for inexplicable packets bound to internet

C. Virus scanners

D. **All of the above**

Computer Security Incident Handling pg. 112-115

5. The most common error incident handlers make is:

A. Failure to analyze lessons learned

B. Failure to make a good working backup

C. **Failure to take complete notes**

D. Failure to secure the area

Computer Security Incident Handling pg. 18

5. What can help protect against mapping techniques

A. Inverse mapping

B. **Split DNS**

C. Monitoring for abnormal outgoing traffic

D. Using a jump bag

Computer Security Incident Handling pg. 119

5. Signs of an incident include:

A. Social engineering

B. Scanning

C. Unusual time of usage

D. **All of the above**

Computer Security Incident Handling pg. 63

5. Which should **not** be in a jump kit

A. Small hub

B. Company phone book

C. CD's with binaries

D. **None of the above**

Computer Security Incident Handling pg. 52

5. An emergency communications plan should:

A. Use in band communications

B. Allow incident communications from the suspected system

C. **Avoid single threads**

D. Communicate to the largest group possible

Computer Security Incident Handling pg. 54

5. The key to gaining information superiority in a large scale attack is to:

A. **Establish solid information flow**

B. Involve a large core team

C. Keep incident communication to a minimum

D. Take steps to build a case

Computer Security Incident Handling pg. 74

5. What two categories can computer crimes be divided into:

A. Felony and misdemeanor

B. State and federal

C. Personal and commercial

D. **Criminal and civil**

Computer Security Incident Handling pg. 148

5. Search and seizure with a warrant can **only** occur when:

A. The suspect consents

B. If the employment policy explicitly requires it

C. The property is in plain sight or on the person arrested

D. **None of the above**

Computer Security Incident Handling pg. 150-151

5. An example of abusive e-mail is:

A. A meeting notice

B. **Several frivolous e-mails to one recipient**

C. Solicited advertisements

D. None of the above

Computer Security Incident Handling pg. 158

5. A war room is:

A. Another name for the data center

B. A media room available to the press

C. **A secure room with copies of evidence in the case**

D. Another name for the technical support center

Computer Security Incident Handling pg. 175

5. The Incident Handling Process can apply Forensic Techniques during:

A. Preparation

B. Identification

C. Eradication

D. **All of the above.**

Computer Security Incident Handling pg. 174

5. Performing an audit is **not** a useful way to:

A. **Identify a potential disgruntled employee**

B. Identify when an intrusion occurs

C. Identify the extent of the compromise

D. Control damage

Computer Security Incident Handling pg. A-7

5. S-Tools **cannot** be used to:

A. Hide multiple files in one sound/picture file

B. Encrypt messages

C. **directly access sectors of a disk**

D. Hide files inside files

Computer Security Incident Handling pg. 216-217

5. Steganography is:

A. Marking good disk clusters as bad

B. **Hiding files inside files**

C. Hiding data within TCP headers

D. All of the above

Computer Security Incident Handling pg. 215

5. An incident starts:

A. When the incident handler arrives

B. **When someone detects or suspects something is wrong**

C. When a security breach is planned by an attacker

D. When Law Enforcement Agencies become involved

Computer Security Incident Handling pg. 68

5. _____ is not an identified incident team role

   A. Team member

   B. In the Way

   C. Witness

   D. **None of the above**

   Computer Security Incident Handling pg. 43

5. To develop management support for incident handling capability:

   A. Collect news articles on computer break-ins

   B. Graphically illustrate an incident

   C. Collect historical support

   D. **All of the above**

   Computer Security Incident Handling pg. 41

5. A communications plan should **not**:

   A. Establish guidelines for interdepartmental cooperation

   B. Coordinate closely with help desks

   C. Allow skips in chain of command

   D. **None of the above**

   Computer Security Incident Handling pg. 57

5. In which phase does the incident handler begin to modify the system:

   A. Recovery

   B. **Containment**

   C. Identification

   D. Eradication

   Computer Security Incident Handling pg. 65

5. Almost every case of espionage prosecuted by the US Government has involved:

   A. A german national

   B. Computers

   C. **A trusted insider**

   D. A contractor

   Computer Security Incident Handling pg. 129

5. Methods of looking for an intruder, which should be avoided include:

   A. Ping

   B. Nslookup

   C. Telnet

   D. **All of the above**

   Computer Security Incident Handling pg. 76

Last Updated: July 24th, 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 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
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
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 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 Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
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
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
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
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
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