Global Information Assurance Certification Paper

Securing A Wireless LAN: A Case Study
GSEC Practical Assignment, Version1.4b, Option 2

By: Richard Park
Date: September 25, 2003

Abstract

A wireless LAN extends the network to the end user. Wireless LANs are a popular method of providing network connectivity without deploying fixed wiring to the workplace. Wireless LANs increase employee productivity by allowing network access without being physically tied down to their desk. It allows employees to get network access in locations such as meeting rooms where fixed wireless connections may not exist.

When our wireless LAN was first deployed, very few laptops had wireless adapter cards so the wireless LAN was very seldom used. In the past 6 months, there has been an increase in the number of people visiting the building as well as the number of PCs that have wireless adapter cards. As the number of wireless connections increased from an average of 4 users a day when initially deployed in 2001 to 20 users a day in the spring of 2003, the higher the risk became that our wireless LAN would be used by people visiting our office who were not employees of our company. There was also a higher risk that someone could use our wireless access to attack other systems on the wireless LAN and the Internet.

My role was to select and implement appropriate security to secure our existing wireless LAN. This paper describes the decisions made in selecting the appropriate security to secure our wireless LAN and identifies the steps used in implementing the chosen security into our wireless LAN.

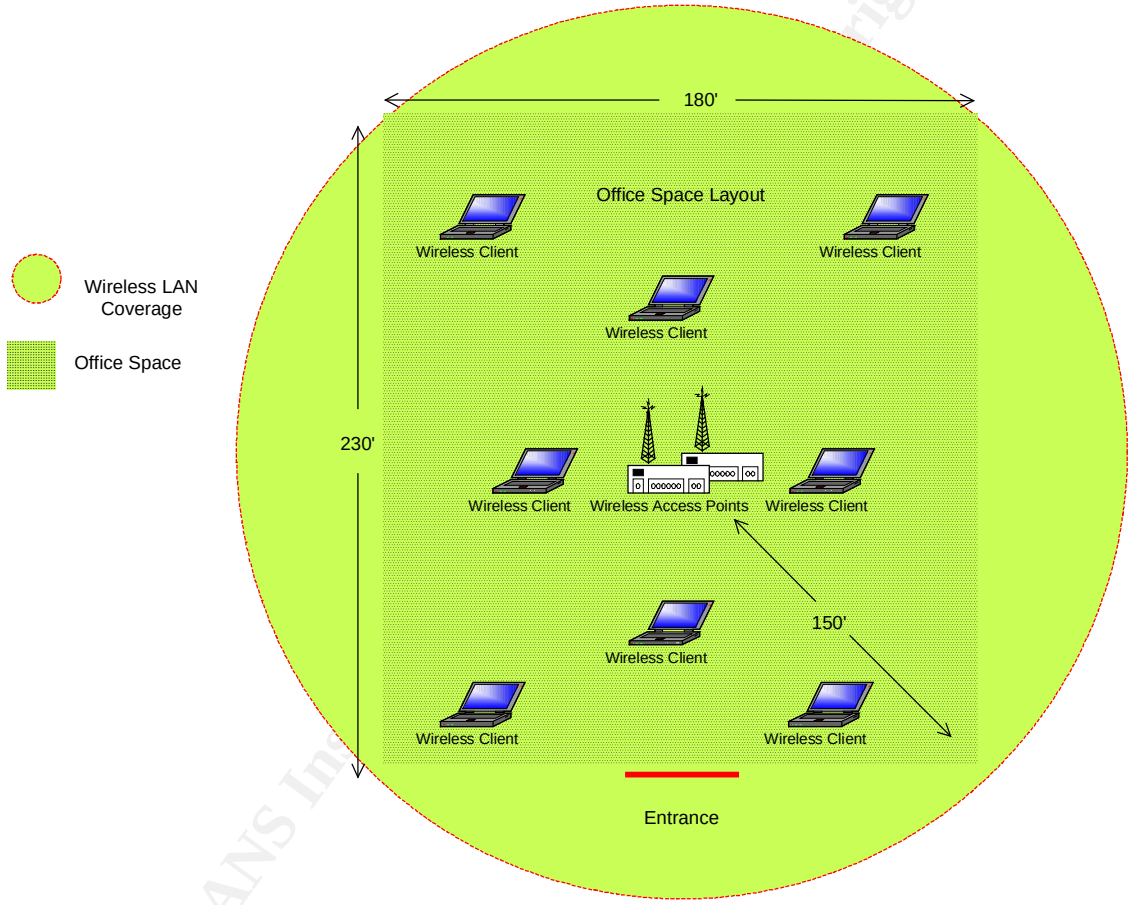
Existing Deployment

One of the corporate security policies currently in place is that wireless LANs attached to the internal corporate network are prohibited. This policy is in place to stop employees from setting up their own wireless LANs that have direct access into the internal corporate network. In order to comply with this policy, our wireless LAN was connected to the Internet. Employees can access the internal corporate network by using the company's IPSec VPN remote access service once on the Internet. By connecting our wireless LAN to the Internet, we can make use of this existing IPSec VPN service to gain access into our internal corporate network and still comply with corporate security policies.

2 Cisco Aironet 350 series access points were placed at the center of our rectangular shaped workplace. This also happens to be where our lab is located. The lab is a closed room where access is restricted by a locked door with a card

access reader. There are 8 lab employees who have access cards that allow access into this lab.

Access to the wireless LAN is open to anyone with a wireless card that supports the IEEE 802.11 protocol. The only restriction to this access point is a physical one in which the wireless access must be established within 150 feet of the access points. Beyond the150 feet, wireless access can still be established but the signal quality can be weak at times. With the existing deployment, one can be outside the 4 physical walls of the office space and get access to our wireless LAN as depicted in the diagram below:



Selecting the Right Security

In order to select the right security to be implemented into our wireless LAN, an analysis was performed on the following types of security:

- physical security
- access security policies
- authentication/encryption

Physical Security

The first part of my physical security analysis was to decide if the existing location of the 2 wireless LAN access points (Cisco Aironet 350s) were in fact physically secure. Because the wireless access points were inside a room where access was limited to the 8 lab employees who had access, I felt that the equipment was physically secure. There was thought to place the wireless access equipment inside a lockable rack but I felt this was excessive considering that network equipment in the lab like switches and routers were not locked up. It would be most unlikely that a malicious person who was able to gain access into the lab would take or attack the two wireless access points when there were more expensive equipment to take or attack.

The second part of my physical security analysis was to look at who had access into the office space where the wireless LAN signal propagated. To enter our building an access card is required. This access card is given to all employees residing at this location. The other way to gain access into our building was to have a residing employee grant access to a visitor. Applying additional access restrictions into the building was not a viable option.

The last part of my physical security analysis was to make sure that the area of coverage from the wireless access points provided good to excellent signal quality strength in the office space yet minimize the signal quality outside the office. Using the Cisco Wireless Client "Status" utility on my PC I was able to get good to excellent link status at the 4 corners of my office space. Outside the office space, I was able to get good to poor link status which is what I wanted. So the signal strength of the wireless access points were already optimally set to allow access inside the office and minimize access outside the 4 walls of our office space.

Access Security Policies

Our company has multiple office buildings located within the city and outside the city. It is common to have employees within the same division working out of different buildings. We have a large number of employees who would like to have network access while at our workplace. Our wireless LAN usage can be classified into the following categories:

1. employees from the same division whose primary place of work is other than this office space
2. employees from the same division whose primary place of work is this office space but they also require network access while away from their wired LAN
3. employees from other divisions
4. non-employees

The decision was made to have a policy whereby we would allow wireless access to those in categories 1 and 2. This would allow us not to be liable for the

actions of people who are not in our division or even employed by our company. A security policy stating that "wireless LAN access was restricted only to those employees belonging to the same division" was sent out to all employees in our division.

In order to restrict access to only those employees who meet the above criteria, authentication base on username and password would allow access to these employees only and restrict all others. So, the next logical step was to choose the right authentication method.

Authentication/Encryption

When it came down to authentication/encryption, there were 3 options available:

- IPSec VPN
- WEP
- LEAP

Part of the decision making process was to try and make use of existing equipment in the lab like our Cisco Access Registrar which is a Radius server from Cisco. If possible, we would also like to reduce additional cost by minimizing the procurement of additional hardware or software.

IP Security protocol (IPSec) consists of the following separate protocols[1]:

- Authentication Header (AH): provides authenticity.
- Encapsulating Security Payload (ESP): provides confidentiality by encrypting packets with encryption algorithms.
- IP payload compression (IPcomp): provides a way to compress packets.
- Internet Key Exchange (IKE): provides key negotiation.

IPSec used in a Virtual Private Network (VPN) provides both authentication and encryption. For our deployment, IPSec VPN would be established from the user's PC to the VPN server. The VPN server would issue the IP address upon successful authentication of the end user. Authentication would most likely be based on username and password. Data traffic would be encrypted from the PC to the VPN server. This option was not selected because we would have to purchase a VPN server which we did not have in the lab.

Wired Equivalent Privacy (WEP) is part of the 802.11 standard[2]. WEP provides link-layer protection from attacks like eavesdropping on wireless LANs.
How Secure is WEP? Many articles can be found on the Internet discussing the weaknesses and vulnerabilities of WEP. These problems include cryptographic attacks, man in the middle attacks and traffic injection from unauthorized clients[3].

[1] http://www.netbsd.org/Documentation/network/ipsec/#ipsec_breakdown
[2] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549087,00.html
[3] http://www.cs.umd.edu/~waa/wireless.html

However, the purpose of WEP is to provide the level of security found in wire LANS. Since our wireless LAN connects to the Internet, WEP provides adequate security for our needs. There is no point having a highly secure wireless LAN that can withstand all types of vulnerability attacks when, in fact, the network connection is to the Internet which, itself, is not secure at all.

So, it looked like WEP would provide the security we needed for our wireless LAN. However, WEP key management was something that I was looking to avoid since it would be a manual process. Fortunately, Cisco supported a proprietary protocol called Lightweight Extensible Authentication Protocol (LEAP) that was based on the Extensible Authentication Protocol (EAP)[4]. Beside authentication, LEAP dynamically manages the WEP key assignment during authentication so we would only need to manage usernames and passwords. The other reason for selecting LEAP was that we could make use of an existing Cisco Access Registrar, a Radius server, which supports LEAP.

LEAP is supported on the following wireless cards[5]:

- Cisco client cards
- Apple Airport cards

The following is a list of all RADIUS servers that currently support LEAP[6]:

- Cisco Secure Access Control Server (ACS)
- Cisco Access Registrar (CAR)
- Funk Steel Belted RADIUS
- Interlink Merit

The disadvantage of using LEAP is that it is a protocol that was developed by Cisco and is not supported by many vendors. We found that wireless network cards from Linksys and internal wireless network devices from IBM do not support LEAP and could not authenticate to the Cisco Access Registrar. In order to solve this problem, employees who required access to the wireless LAN had to purchase Cisco Aironet 350 wireless cards. There were 3 employees out of 30 who had to purchase new Cisco Aironet cards. So, the additional cost to implement LEAP was $500. This came well within our budget to limit costs.

Implementation

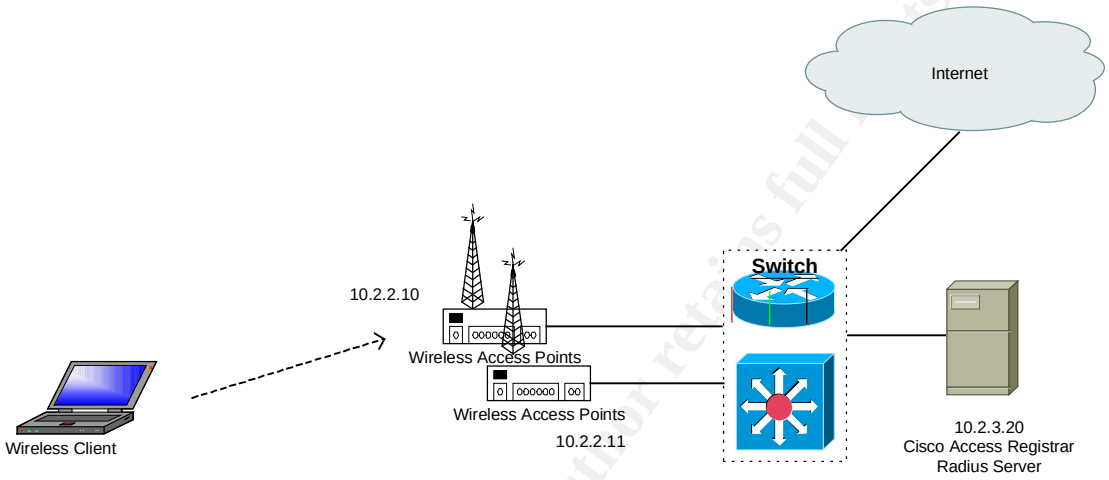
The equipment required to setup LEAP authentication on our wireless LAN is listed as follows:

- 2 Cisco Aironet 350 wireless access points
- 1 Sun server 420R with

[4] http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_online_exclusive09186a00800a5cab.html
[5] http://www.cisco.com/en/US/products/hw/wireless/ps430/products_tech_note09186a008019fea2.shtml#LEAPRADIUS
[6] http://www.cisco.com/en/US/products/hw/wireless/ps430/products_tech_note09186a008019fea2.shtml#LEAPRADIUS

    - 1GB memory and 10GB disk space
    - Cisco Access Registrar 3.0r1
- IBM ThinkPad T23 with
    - Windows 2000
    - Aironet 350 wireless LAN adapter
    - Cisco Aironet Client Utility version 5.05

The diagram below illustrates the network layout of the equipment listed above:



The following section identifies the implementation steps used to setup LEAP authentication on our wireless LAN.

Access Points

The two Cisco Aironet 350 access points have to be configured to use LEAP authentication. The information required for this configuration are:

- 2 shared secrets between each access point and the Radius server
- SSID
- IP address and port of the Radius server

The steps to configure the access points will not be described here since Cisco does a very good job in their configuration document. Please see the configuration document at http://cisco.com/en/US/products/hw/wireless/ps458/products_configuration_guide_chapter09186a008007f788.html#1053749 for the step-by-step instructions on configuring the access points to use LEAP authentication.

Radius Server

Install Cisco Access Registrar 3.0r1 on a Sun 420R server running Solaris 2.8. Log into Cisco Access Registrar by entering the command “aregcmd”. Enter the administrator’s username and password.

Add the two wireless access points as clients in Cisco Access Registrar by entering the following commands:

```
% cd /radius
% cd clients
% add CiscoAP1
% cd CiscoAP1
% set ipaddress 10.2.2.10
% set secret trust34n2o4q
% cd ..
% add CiscoAP2
% cd CiscoAP2
% set ipaddress 10.2.2.11
% set secret dump3e48w3r1
```

The next step is to create user profiles in Cisco Access Registrar. For each username, enter the following commands into the userlist. In this example, the username is “smith” and password is “as2wed22tt”.

```
% cd /radius
% cd userlist
% cd default
% add smith
% cd smith
% set password as2wed22tt
```

Set the authentication and authorization services in Cisco Access Registrar to use LEAP by entering the following commands:

```
% cd /radius
% set default authenticationservice wireless
% set defaultauthorizationservice wireless
% cd services
% add wireless
% cd wireless
% set type eap-leap
% set userservice local-users
% save
% reload
```

Client

Insert the Cisco 350 wireless network card into the IBM ThinkPad T23 PC card slot. Install Aironet client version 5.05 on the IBM ThinkPad T23 running Windows 2000.

Start Aironet client utility 5.05. Click on “Profile Manager” and click the “add” button. Enter a name for this profile. Click on the “Network Security” tab and

select LEAP as the network security type. Click on the “Configure” button. Select “Use Saved Username and Password” and enter the assigned username and password. Click the “OK” button twice. Click the “Apply” button. Click the “OK” button again.

Click on the Aironet client utility “Status” icon and your PC should be associated to the wireless LAN. You should also have good to excellent link quality.

Verification

To verify that authentication is taking place, packets were captured between the wireless access point and the Radius server during the authentication process. Using the “snoop –vx0 –d qfe0 port 1645” command on the Sun server running the Cisco Access Registrar, I was able to capture the following packets when my PC established a wireless connection:

```
Using device /dev/qfe (promiscuous mode)
ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 1 arrived at 13:55:49.79
ETHER:  Packet size = 195 bytes
ETHER:  Destination = 8:0:20:d9:2:ad, Sun
ETHER:  Source      = 8:0:20:ff:3b:e8, Sun
ETHER:  Ethertype = 0800 (IP)
ETHER:
IP:   ----- IP Header -----
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         xxx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 181 bytes
IP:   Identification = 32845
IP:   Flags = 0x0
IP:         .0.. .... = may fragment
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 59 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = 595f
IP:   Source address = 10.2.2.11, 10.2.2.11
IP:   Destination address = 10.2.3.20, RadiusServer
IP:   No options
IP:
UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 2247
UDP:  Destination port = 1645
UDP:  Length = 161
UDP:  Checksum = 68A9
```

UDP:

```
 0: 0800 20d9 02ad 0800 20ff 3be8 0800 4500    .. ..... .;...E.
16: 00b5 804d 0000 3b11 595f cc65 3d0b ce2f    ...M..;.Y_.e=../
32: cdeb 08c7 066d 00a1 68a9 0134 0099 ebe1    .....m..h..4....
48: 2599 fbb8 3935 fa37 9d7f d540 cf80 0107    %...95.7...@....
64: 7270 6172 6b1a 1800 0000 0901 1273 7369    smith........ssi
80: 643d 7061 6c6c 6162 2d77 6c61 6e04 06cc    d=wireless-wlan...
96: 653d 0b1e 0e30 3034 3039 3633 3339 3837    e=...00409633987
112: 311f 0e30 3034 3039 3634 3236 3237 3420    1..004096426274
128: 0e41 5033 3430 2d33 3339 3837 3105 0600    .AP340-339871...
144: 0000 270c 0600 0005 783d 0600 0000 1306    ..'.....x=......
160: 0600 0000 014f 0c02 0200 0a01 7270 6172    .....O......smit
176: 6b50 1232 6837 5b1f 06d1 717b fda9 0663    hP.2h7[...q{ý..c
192: 9675 6e                                    .un
```

Looking at the above packets, the source IP address 10.2.2.11 belongs to the Cisco Aironet wireless access point and the destination IP address 10.2.3.20 belongs to the Cisco Access Registrar Radius server. This packet capture proves that LEAP is being used for authentication. Interestingly, both the username "smith" and ssid "wireless-wlan" are sent in clear text during authentication as expected.

Conclusion

Our wireless LAN went from having no security to good security by implementing security in the following areas:

- physical security
- access security policies
- LEAP authentication and WEP encryption

LEAP provides good security by making users authenticate with a username and password in order to access our wireless LAN. LEAP also provides a mechanism for exchanging WEP keys that are used for data encryption.

There has been recent work done by Microsoft, Cisco and Extundo on a new protocol called Protected Extensible Authentication Protocol (PEAP)[7] that has been submitted as an IETF draft document. PEAP addresses some of the weaknesses of EAP like protecting user identity and EAP negotiation. PEAP will most likely be supported by many vendors. We will be migrating from LEAP to PEAP once PEAP is supported on wireless network cards from vendors like Linksys and IBM.

[7] http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-06.txt

References

1. NetBSD, “NetBSD Documentation: NetBSD IPSec“, 23 September 2003, http://www.netbsd.org/Documentation/network/ipsec/#ipsec_breakdown

2. Bice, Bryan., “Wired Equivalent Privacy”, 31 March 2002, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549087,00.html

3. University of Maryland Computer Science Department, “Wireless Research: 802.11 Vulnerabilities”, http://www.cs.umd.edu/~waa/wireless.html

4. Cisco, Packet Magazine, “Under the Hood: Wireless Authentication”, http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_online_exclusive09186a00800a5cab.html

5. Cisco, Cisco Aironet 1200 Series, “LEAP and RADIUS Server”, 8 July 2003, http://www.cisco.com/en/US/products/hw/wireless/ps430/products_tech_note09186a008019fea2.shtml#LEAPRADIUS

6. Palekar, A., et all., “Protected EAP Protocol (PEAP)", 22 March 2003, http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-06.txt

7. Cisco, Cisco Aironet 350 Series, “Security Setup”, http://cisco.com/en/US/products/hw/wireless/ps458/products_configuration_guide_chapter09186a008007f788.html#1053749

8. Cisco, Cisco CNS Access Registrar, “Configuring Cisco Access Registrar”, http://www.cisco.com/en/US/products/sw/netmgtsw/ps411/products_installation_and_configuration_guide_chapter09186a008015472c.html

9. Cisco, Cisco Aironet 350 Series, “Bridge Hardware Installation Guide”, http://www.cisco.com/application/pdf/en/us/guest/products/ps460/c1099/ccmigration_09186a00800eec5d.pdf

10. Cisco, Cisco Aironet Wireless LAN Client Adapters, “Release Notes for Cisco Aironet Client Utilities, Version 5.05.001 for Windows 2002”, http://www.cisco.com/en/US/products/hw/wireless/ps4555/prod_release_note09186a00800df92a.html#83364

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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 Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS