Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical assignment
Version 1.4b

Protecting Corporate Laptop by home use – Case Study
Niko Makovecki
July 9, 2003

ABSTRACT:

How to mitigate increased vulnerability when connecting with my corporate laptop to cable Internet at home? That was essential challenge by upgrading my home Internet connection from dial-up line to cable Internet provider. Impact of GSEC study on my behavior was great. Numerous questions but only few answers, that is true story by all of us when we find us on security battlefield.

By dial-up connection with speed thru 56 Kb, with short-term connection to Internet and with changing IP address by each call is the vulnerability also great but lower like by broadband permanent cable connection. I used remote dial-up access for connecting to corporate network. When I went to Internet thru this connection I was behind corporate firewall and protected with same degree of security like at work. With broadband connection at home it is likely to access Internet thru this connection and no more thru dial-up remote access to corporate network. New challenge is also to connect to Corporate network thru Internet. So real need is to protect corporate laptop by home use and access to Internet. For this goal I implemented old Pentium PC with Freesco software router and firewall.

SITUATION BEFORE:

I am employed as system administrator and part of my duties is also in security sphere. To achieve better response time, to improve administrators possibilities to connect to corporate network and to enable homework we made a decision to acquire laptops. So my laptop goes with me everywhere. I call frequently from home to company network to check system state, to gain access to company data or to supervise availability of services on company network. Even if I connect to Internet thru this connection is my laptop protected behind company's firewall.

My company is connected to internet with leased line 128 Kb. Basic protection is 3Com NetBuilder router with integrated firewall. To improve security we don't allow incoming traffic thru firewall with exception of e-mail – SMTP protocol to fixed IP address and port 25. Mail server is MS Exchange 5.5. Complete incoming and outgoing mail traffic is scanned with F-Secure Anti-Virus for MS Exchange. All workstations and mobile computers are equipped with F-Secure Anti-Virus for Workstations. All servers are also equipped with F-Secure Anti-Virus for Servers. Every half hour poll BackWeb agent F-Secure site for new virus strings or program versions. Every installation of antiviral software is updated through central management server in frame of half hour after arriving of new virus strings from principal's site. For Internet access is employed MS Proxy server. Internet access has

to be approved from highest company's management. Internet access is limited to approved internal IP addresses and to approved users.

Company's platform on workstations is mainly Windows NT and Windows 2000 Pro. There are left some Windows 98 on some workstations because of incompatibility of some employed software with Windows NT and Windows 2000. All users have to log on to NT domain. We implement login scripts and roaming profiles for all users. Company has established policy of acceptable use of company's information system and of information capacities. Separate are rules for acceptable use of electronic mail. According to this policies and rules users shouldn't threatening security of company's information system with their activities. Especially users are not allowed to install any programs on corporate computers without special permission of IT department. Goal of these rules is for all to ensure trouble free functioning of information system. Important aspects are also to mitigate possible negative impact of installing of unknown programs in corporate environment and to improve reliability of information system and accessibility of information resources.

New impact is implementation of mobile computers in company's informatics technology. Since now, use of mobile computers was limited only to system administrators also for home use and for connecting to corporate network from outside. Base of this network are Windows NT servers and for connection we use Windows remote access over dial-up line. Although this type of connection is some threat to company's security, is it's use acceptable and under sufficient control. Connection is established with callback from corporate computer. Therefore are phone numbers of callback lines and modems known only to system administrators. Each administrator has predefined home telephone number from which can he dial company's modem. After callback the administrator is connected to company's network as have I mentioned before and therefore protected with same degree of security just as he would be connected direct to company's network.

On my Laptop is installed operating system Windows XP Pro. For virus protection is implemented F-Secure Anti-Virus for Workstations. On this computer have I also a lot of software and tools for administering and supervising of network and other information and technical resources. Between them are Ethereal for network supervising and for testing vulnerabilities on other computers also NmapWin. Part of my working duties is also administering Linux server. Therefore open source community is not total stranger for me. When I ordered cable connection at home, the greatest challenge for me was: "How to protect my business laptop when connecting to Internet?« In some articles there was mentioned Freesco – FREE ciSCO – free replacement for commercial routers.

Some questions on which I will try to answer are:

1. How to protect system administrator's home network and corporate laptop?
2. Price aspect for home use – Why Freesco and could Freesco be right answer? How to install Freesco?
3. How to examine suggested solution? Can some tools from Security Essentials Toolkit help me by this?
4. What to suggest for protecting corporate laptops of other administrators? How to protect mobile computers of other ordinary users when they are on the road? Is this protection with personal firewall?

5. How to assure faster and secure access to corporate network – which obstacles have to be surpassed? What should I suggest to management – how to protect corporate network when employees connect to corporate network thru Internet? What about VPN?

REALIZATION OF CABLE CONNECTION AT HOME:

Technicians from Internet provider installed Cable connection at my home. Unusual to me was, that they needed MAC address from network card that will be connected to cable modem. Obviously this was some kind of protection and to assign fixed IP address for my connection.

In Article "Build a floppy based router/firewall with Freesco" from Jim McIntyre in TechRepublic (URL: http://www.techrepublic.com/article.jhtml?id=r00220020924mci01.htm - access is free but one have to be registered user of TechRepublic) I found some very exciting information. Also opinions in discussions were quite positive. So I decide to give closer look at Freesco. Home site of Freesco project is http://www.freesco.org. I test version 0.3.1 since latest version is 0.3.2 and has implemented some patches to kernel – so this latest is the recommended download.

Freesco is - according to Summary on http://sourceforge.net/projects/freesco:
"FREESCO, a router for networks with static routing. Freesco is based on the Linux operating system and incorporates many of the features of a full operating system into software that fits on a single 1.44 meg floppy diskette.«

Freesco was developed as an alternative to proprietary, commercial and sometimes expensive products offered by Cisco, 3-Com etc. Some features of Freesco from home site (URL: http://www.freesco.org/?L=Overview):
"With Freesco, you can make:

- a simple bridge with up to 3 Ethernet segments
- a router with up to 3 Ethernet segments
- a dialup line router
- a leased line router
- an Ethernet router
- a dial-in server with up to 2 modems
- a time server
- a dhcp server
- a http server
- a print server (requires TCP/IP printing client software)

Freesco also incorporates firewalling and NAT which are resident within the Linux kernel to help protect you and your network. All of these features can be used in conjunction with each other or individually. "

For Internet access I have planned old PC with Pentium 166 MMX processor, 32 MB memory, installed Windows 95 and two network cards – one SMC 8216C in one and 3com 509B-TPC in other, floppy drive 1.44 MB, and Hard drive 850 MB. After installation of cable modem we, with technician from Internet provider, made first test

under Windows 95 and PC has successfully established connection to Internet over cable modem.

In next step I have set up Freesco on PC. First I copied program to diskette and afterward checked settings of Freesco. Boot was very slow so logical choice was to transfer program from floppy drive to hard drive. After changing settings bootgui in MSDOS.INI to "no", normal start was without Windows – only command prompt. Next step was editing autoexec.bat with inserting line "C:\router.bat". My PC is booting now direct in Freesco router.

When I was configuring Freesco I choose Ethernet router. In Network card settings I entered I/O and IRQ for both network cards. After that it was time to define network settings for both networks. For network 0 – external network - I chose Interface name "eth0" and defined that this network will use DHCP client and will configuring it's settings according data received from internet service provider.

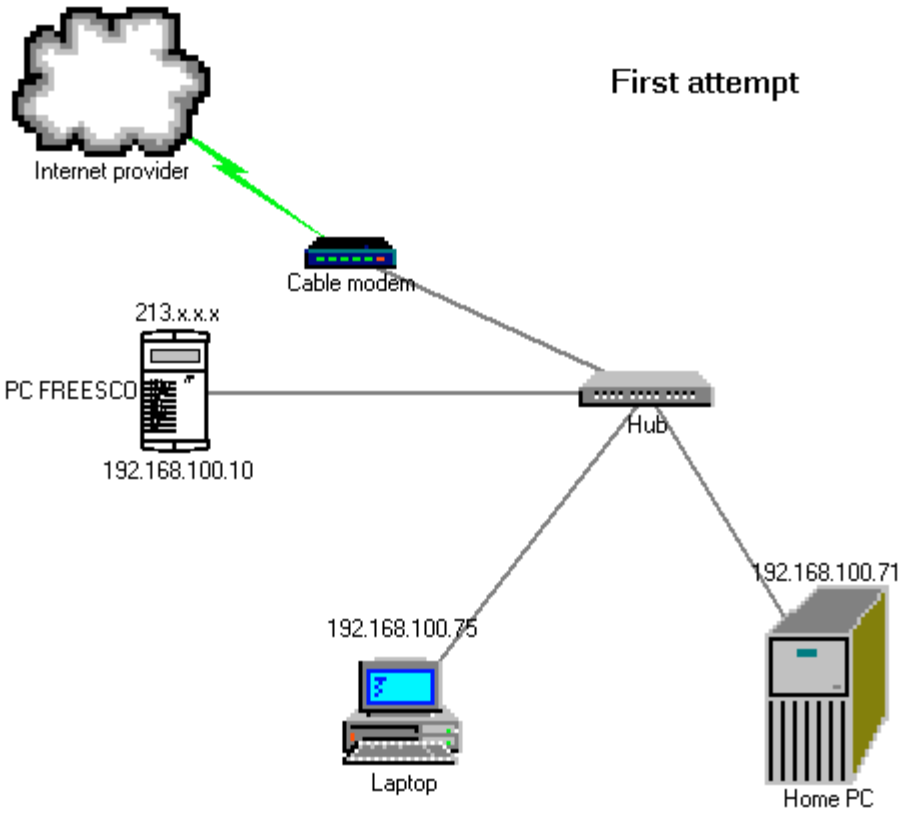
For network 1 I choose interface name "eth0" then IP Address 192.168.100.10 and network mask 255.255.255.0. Such setting of network mask can be too generous for home network – 256 available network addresses are too much, but I simple copied setting from corporate setting. So I don't need to change IP settings on my laptop each time when I connect to home network. DHCP pool for DHCP server on internal network was 192.168.100.20 to 192.168.100.25.

After few attempts there was positive answer from pinging our corporate Internet site from PC router. Evidently all configurations and connection was successful and functional.

FIRST ATTEMPT:

All devices were connected to hub. So all traffic can be captured to determine possible problems. Symbolic Network diagram is presented on PICTURE 1. In this attempt it was problem whit IP traffic. PC with FREESCO installed can get connection to Internet, but not to other devices on internal network.

To determine where is the problem there was best choice to use Ethereal and to see all traffic on network. After capturing traffic some time analysis was clear. In capture log there were lot of packets with ARP protocol. Those packets came from outer network and they arrived thru modem from external network interface. Some packets with ICMP (Echo (ping) request) and DHCP protocol were more interesting. From those packets I saw that PC with Freesco offer DHCP services on network interface that was provided for external network. And DHCP client has sent configuration requests from network interface that was provided for internal network. From Ethereal capture I have realized which network interface on PC Freesco was used for which communication. After realizing wrong configuration in interfaces I had to change assignment between physical network cards and logical network interfaces in Freesco. Test with ping from Laptop to Internet provider or corporate home site was successful after applying new configuration and restarting Freesco.

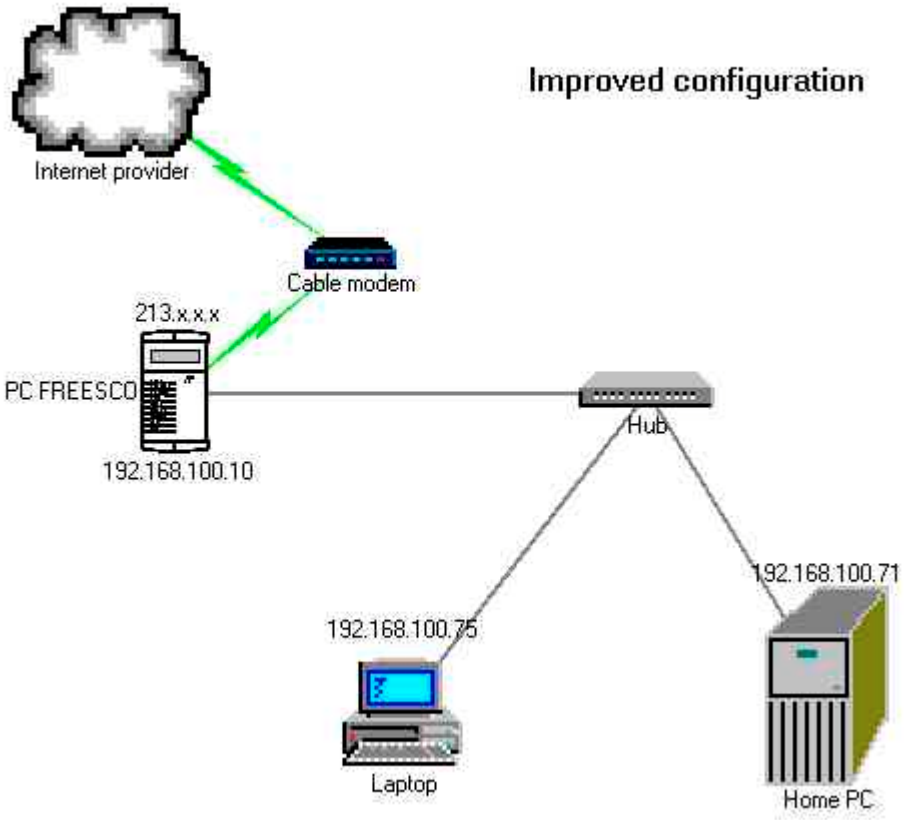


PICTURE 1 – First attempt

Closer look at captured file has brought me some concerns about exposure and vulnerability of entire home network. Most of packets came over cable modem from external interface. The majority of their protocol was ARP and source address was from external network. If those packets come to laptop, then is it exposed to all threats from external network? After all, this configuration is too much insecure and I have to improve it.

IMPROVED CONFIGURATION:

To achieve expected functionality of router, device has to be between external and internal network. Obviously cable modem has to be connected to external network card on PC with Freesco and not to hub. Network diagram after changing connection is presented on PICTURE 2 – Improved configuration:



PICTURE 2 - Improved configuration

Once again the checking of traffic on internal network with Ethereal was taking place. New captured result was much better. There were no more packets from external network with ARP protocol. The only packets with ARP protocol came from internal network, from laptop. There were ARP requests in packets to resolve IP addresses of network printers. There were also some packets with NETLOGON protocol – SAM logon requests from client. Such behavior was normal and expected from Windows XP. In corporate network we have network printers and each workstation is part of NT domain. Connecting to other network – in this case home network – Windows XP machine tries to find out network printers and domain controller. Since there was no packets originating from external network that trying to start connection, reasonable conclusion was that router handles its role well.

To verify configuration of router and protection of internal network there are multiple possibilities. My choice was to check external network interface on PC Freesco with tests initiated from internet site SecuritySpace.com owned by E-Soft Inc. Internet address is: http://www.securityspace.com/sspace/index.html. Security audit initiated from Securityspace was Basic Port Scan Vulnerability Test and result was "Number of open ports found by port scan:0". There was also warning, that 0 ports open is very god, but one should be aware of limitations: "Port scan did not include UDP ports" and that some vulnerabilities as trojans that "phone home" cannot be detected by port scan. Another warning was "You may not be protected from email viruses".

Such situation seemed acceptable to me. I know, that email viruses are great threat to each user and company. For email we have established corresponding policy and educated users how to act to mitigate threats from email viruses and other attacks that came thru email messages. In accordance with this policy, but independent from users actions is first barrier Anti-Virus on email server and second Anti-Virus on user stations. This is one sight of dependence in depth. If malicious program or attachment passes protection on email server there is another barrier on user workstation in form of Anti-Virus for workstations. This second barrier is functional also in case when one use email client to access external email server using web browser for email access.

Some trojans that "phone home" can be detected with use of suitable programs. One of those is Ad-aware from Lavasoft company. Program is free for non-commercial use and most usable information about this program can be obtained on: http://www.lavasoft.de/support/faq/. With Ad-Aware one can not only detect possible spyware or different kinds of advertising programs that are installed on his computer without his knowledge or approval but also remove these unwanted or dangerous programs from his computer. For this reason I accept also second warning and acknowledge that some additional actions has to be made.

NEXT STEP FOR PROTECTING MY CORPORATE LAPTOP:

After all checking I think that first step in improving security at home is achieved. My corporate laptop is now better protected by home use and also when accessing Internet resources from home trough cable connection. But (yes it is always some "but"), is this enough? Answer is clear - NO!

To see what is happening with my laptop I choose to install personal firewall. By searching different resources on Internet the most frequent answer was ZoneAlarm from Zone Labs. Why? It seems to me very likely that because of fact, that one version of this product can be obtained for free. Not to mention all good marks that this product get in different reviews and also all awards. On their home page: http://www.zonelabs.com/store/content/home.jsp there is one interesting statement: »A growing number of profit-driven hackers have learned that the surest way to your organization's assets is to target your unprotected PCs—in particular, remote and mobile PCs—with a customized attack.« This was another proof for me that one should newer underestimate security and that my concerns to protect corporate laptop were in place.

I downloaded and installed Zone Alarm on my corporate laptop. By home use I found some services and programs on my computer for which I was not aware before and they wanted to access private network or Internet. When connecting to corporate network at work I discovered some bad configurations on other workstations. Some workstations wanted to access my laptop to use CD drive or to use printer that I used to share in the past. In such a role Zone Alarm acts not only as firewall but also like intrusion detection system and help me to fix some bad configurations and remove some potentially dangerous shares from my computer.

WAS EXPERIMENT SUCCESSFUL?

To answer on some of questions from beginning of this assignment:
To protect my home network and corporate laptop Freesco was right answer. It's flexibility and easy of use is great. Although I have not very much experience with Linux, firewalls and routers I was able to raise effective barrier for possible threats to my home network from external world. Freesco's setup utility is really great. Cost view of applying Freesco is also great. Instead of purchase of dedicated piece of hardware I was able to use my old PC and investment was minimal – only one additional network card. Some possibilities of Freesco are still open. I have configured DHCP server but my plan for the future is also configuring print server for home use.

Following my experiences with Freesco I can suggest Freesco to other administrators from my corporate. Each of us can improve security of his home network by applying PC with Freesco as router and firewall.

With use of Ethereal I discovered wrong configuration in network interfaces and was able to fix it. This tool was also very helpful when I inspected traffic in my home network and also in our corporate network.

To improve protection of very sensitive device, which administrator's laptop is, we have to apply some kind of personal firewall on this computer. I experimented with Zone Alarm and results were good. I discovered some services that try to connect to Internet and on other side some trials to connect to my laptop from other workstations on corporate network. This kind of protection is also suitable for protecting mobile computers of "ordinary" user when they are on the road. To achieve better control and with this also security and protection I would suggest in my enterprise use of F-Secure Distributed firewall. The main reason is in unifying platform. We already have F-Secure Anti-Virus applied and experiences with it are more than satisfying. The greatest thing is F-Secure Policy manager console that enable administrator not only to supervise workstations but also to set rules and to deploy this rules in form of obligatory policy to all workstations and servers. Furthermore, with right setting of alerting rules administrator is always informed about all incidents on supervised systems – from warnings caused by recoverable problems to security alerts caused by malfunctioning of antiviral protection or attempts from malicious programs to penetrate through protection and to possess the computer. With employment of F-Secure Distributed Firewall we can use the same management tool for this product and this is advantage that must be taken in sight when making long-term proposal.

TO DO OR LAST UNANSWERED QUESTION:

Last question, which I tried to answer, was How to assure faster and secure access to corporate network?

On central corporate location we plan to move from leased line 128 Kb to ADSL broadband connection 2, 4 or maybe 8 Mb. With this upgrade possibilities for faster connections for remote users would be great improved.

Beside of protection by home use – that was theme in this paper – to connect with corporate laptops we must consider at lest this aspects:

1. Anti-Virus protection – advisable is protection that is unaffected by user actions – desirable is central management with good reporting support.
2. Personal firewall for protecting corporate laptop when on road with same degree of configuration, protection and reporting possibilities like by anti-virus protection
3. Secure VPN connections on both sides – on central corporate location and on remote user side. On such a connection we can realize faster and still secure access to corporate network from home or while on business travel.
4. Good management, deployment and supervising tools. It is desirable also to have alerting possibilities so that each incident is reported to administrator.
5. Defining right policies to lead each user to acceptable behavior when using corporate desktop outside of corporate network.

CONCLUSION:

I am satisfied with first defense line by home use of corporate laptop, which is PC with installed Freesco. But this is only first line. Second line is personal firewall parallel with Anti-Virus protection. Very important is to establish suitable rules and policies to protect corporate information system and to educate users to act in accordance with this rules and policies.

All spheres of broadband connections to our corporate network, of secure connections between road warriors with mobile computers and corporate network stands before us to find suitable solutions and not to oversee which of important aspects of security.

REFERENCES:

Security Space http://www.securityspace.com
Freesco http://www.freesco.org and download also at http://sourceforge.net/projects/freesco
Tech Republic http://www.techrepublic.com
F-Secure http://www.f-secure.com
BackWeb http://www.backweb.com
Lavasoft – creators of Ad-aware http://www.lavasoft.de
Zone Labs – creators of Zone Alarm http://www.zonelabs.com
Klavs Klavsen "**Securing Remote Users VPN Access to Your Company LAN« URL:** http://www.sans.org/rr/papers/20/727.pdf
Daniel Crider "A 6-Layer Defense for an I.T. Proffesional's Home Network" URL: http://www.sans.org/rr/papers/26/621.pdf

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
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
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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