Global Information Assurance Certification Paper

Candidate: Kevin Clarke

Assignment Version: Track 1 – GIAC Security Essentials (GSEC) v1.4

Title: An evaluation of Firewall considerations and steps an organisation should follow to build an Internet Solution to protect their Internet presence.

1.0 Abstract

This paper has been written to illustrate the reasons why organisations choose to rely solely on a firewall to protect their entire network infrastructure. The paper also illustrates why a firewall should be considered as only one of the first steps in network security for an organisation. Taking these areas into consideration I have made recommendations for further systems that can be used to develop an organisations security solution.

The paper concludes to show that security solutions should not rely on single systems, again echoing my belief in why a firewall shouldn't be used as the only system. Finally the paper is completed with the four elements that need to be considered by an organisation when implementing their security solution.

2.0 Why?

Many organisations choose to only implement a firewall to protect their network infrastructure against attacks. The key reasons for this are outlined below.

2.1 Media

Most people responsible for Internet Security are use to reading about firewalls in different areas of the media, whether it is from a website or in a trade magazine. Due to this media coverage firewalls are considered as mandatory when building a security solution. I agree it is an essential building block when constructing an Internet security solution, but it should be seen as just one of the stages and not as a complete solution.

Firewalls are widely accepted by the media and industry as being a developed Security system when compared to other systems, such as Intrusion Detection (IDS). No doubt in time other systems such as IDS will be considered mandatory as firewalls are today by people building Internet security solutions.

Companies retailing firewalls, i.e. Checkpoint and Cisco, are well known within the Security arena due to their extensive media coverage. This influences potential purchasers and helps to build trust with the brands.

2.2 Budget

A budget affects the choice of security systems applied to a network because the majority of organisations have a limit on how much they can spend. This results in the IT Manager looking at systems that can provide the organisation with value for money but at the same time meets his security goal of having a secure network. A firewall is

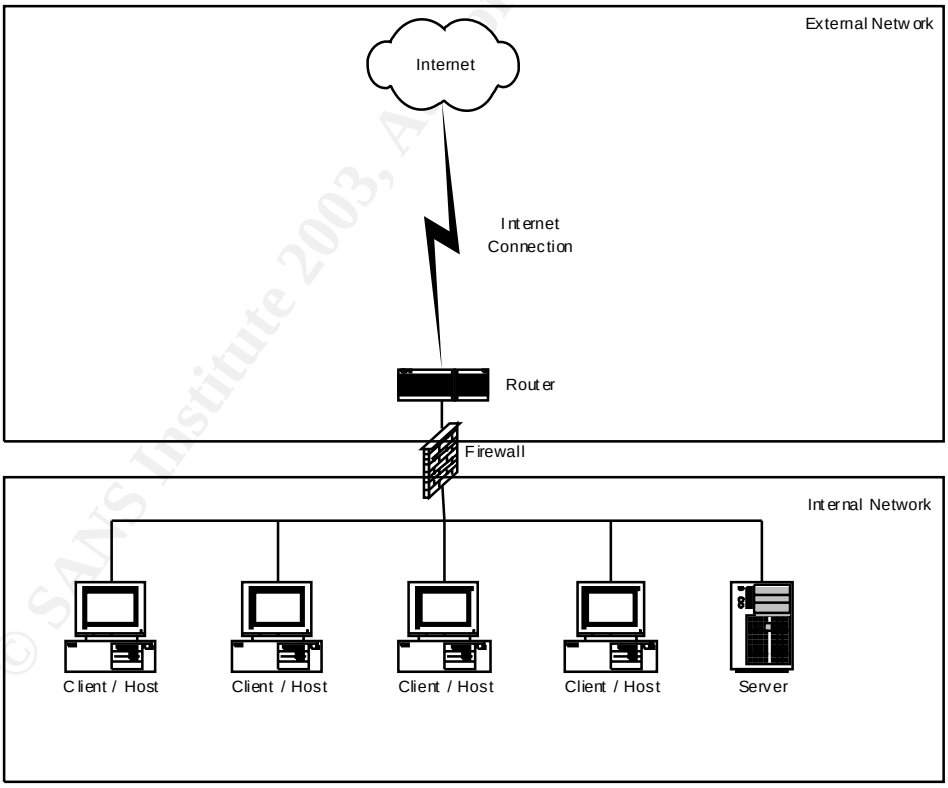
appealing in this situation as it provides protection for the entire network for a single fee. This is obviously attractive to an organisation in today's market where general spending on IT is considerably more conservative.

2.3 Simplicity

Simplicity is a key reason organisations choose to only implement a Firewall for network infrastructure protection. Many organisations networks are now business critical and cannot be interrupted, therefore installation of a firewall providing a blanket security solution with minimal disruption is appealing. Alternatively it may be more secure to protect each host on an individual basis but this usually results with a heavy investment in labour for the initial set-up and ongoing management.

Figure 1 illustrates a firewall providing the gateway for the internal network to reach the external network (the Internet) and therefore it is ideally placed to govern traffic between the two networks to provide a protected internal network.

Figure 1: Basic Network Topology



3.0 Infrastructure Analysis

When an organisation decides to implement a security solution to help protect their network and digital assets they need to decide which areas require protection. These areas can be divided into the following categories; data , resources and company reputation, which are now discussed in further detail.

3.1 Data

The most valuable company data is customer and employee records. Therefore these areas require careful consideration when managing digital assets and the access given to them. For example if a company cannot keep accurate customer records then billing can become an issue, you cannot bill a customer without knowing which products and services they have purchased.

Employee records are equally important, as it could be very disruptive for a company if the payroll records were made public. Imagine the embarrassment for senior managers of a company if the employees found out how much the Managing Director was being paid or what bonus the Sales Director had received. [1]

3.2 Resources

Reviewing figure 1, page 4, focus shifts to resources and the effect on the internal network if the Internet connection was unavailable. This situation could be experienced through unnecessary or unwanted traffic consuming the Internet connection, potentially leaving the internal network without email and Internet access. Nowadays due to Internet services becoming business critical for many organisations, serious downtime could result in substantial financial penalties caused by loss of trade. [1]

3.3 Company Reputation

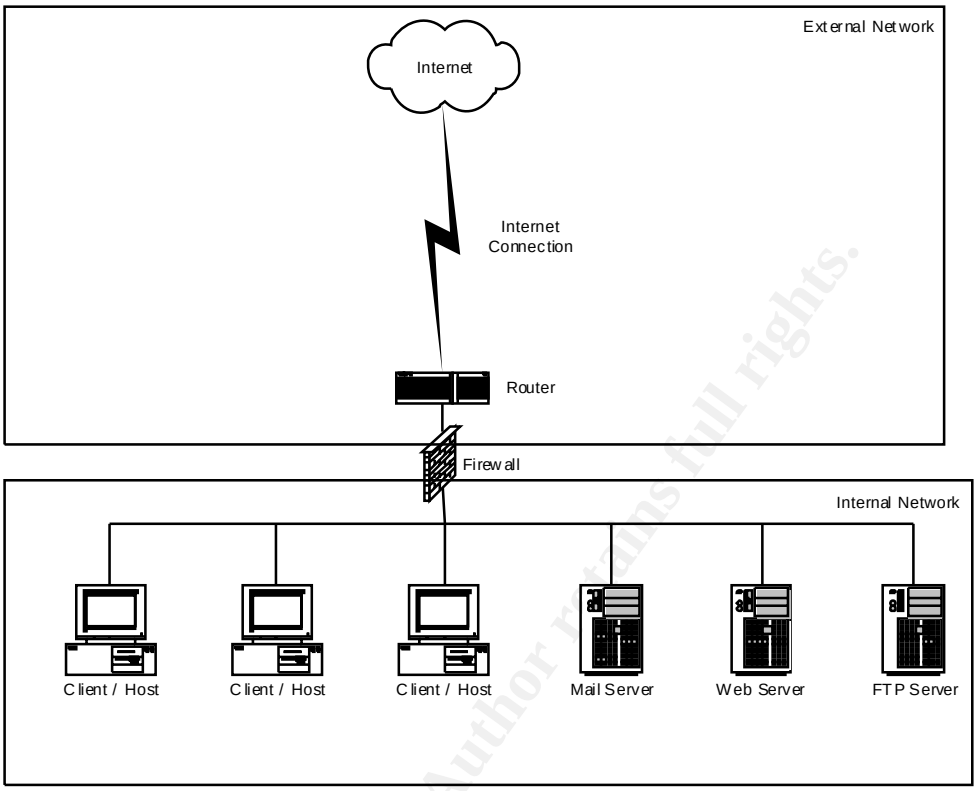
Image and reputation of an organisation needs to be protected due to the potential vulnerability of an Internet presence. If a companies IT infrastructure is exploited then it can have disastrous consequences for the company's reputation. For example if a company's website was attacked and defaced with some distasteful content, this could seriously impact their credibility. [1]

4.0 Systems and Services

Once the analysis stage has been completed and areas of vulnerability have been discovered, systems and services used by the organisation have to be reviewed. In many cases an organisations systems and services can be updated to provide high levels of security.

Let's take the example of a medium sized organisation running a mail server, web server and FTP server, which all require access from the Internet. This is illustrated in figure 2, page 6.

Figure 2: Basic Network Topology with Public Services



As you can see from figure 2 the servers are hosted on the internal network along with the internal client machines. This means that if one of the publicly available servers is exploited, potentially the attacker could gain access to the rest of the internal network. Several methods can be used to help prevent this, the first and arguably the most important is to attempt to secure each public service.

As the servers require public access, the firewall has to be configured to allow access for each service to be able to function; in effect this punches holes through your securely configured firewall, placing greater responsibility on the individual servers to be secure. I will now progress to detail examples of potential server vulnerabilities and address how to secure them.

4.1 Mail Server

Many organisations run their own mail server to provide mail services to their users, an essential service for the majority of organisations. Taking figure 2 as an example, the mail server is running Microsoft Windows NT with Microsoft Exchange 5.0. As well as the operating system and Exchange service being old versions, Exchange 5.0 is publicly known as vulnerable to being an open relay. This means anybody could use this mail server to send email, ideal for people who wish to send out unsolicited email (spammers). To secure this server it is recommended to upgrade the operating system to Windows 2000 and upgrade the Exchange service to the latest version, Microsoft

Exchange 2000. Alternatively Microsoft Exchange 2003 is due to be released in the near future. [3]

4.2 Web Server

Figure 2, page 6, details a network hosting a web server. In this example the web server is a Windows 2000 server running Apache 2.0.44. According to mitre.org cve CAN-2003-0017 this version of apache has several possible vulnerabilities and according to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0017 the server could allow a remote attacker access to certain files. To fix this vulnerability and various other minor vulnerabilities it would be recommendable to upgrade to 2.0.45. [5]

4.3 FTP Server

In addition to the Mail and Web servers this organisation is running an FTP server. In this example the FTP server is a LINUX Redhat Server running wu-ftp v2.4. This wu-ftp version contains a vulnerability which allows regular and anonymous users to gain root privileges. The vulnerability exploits a problem with the signal handling when the FTP server receives an unexpected pattern of commands, this results in the user gaining root privileges. As this is a problem with the programming it can only be fixed by applying a relevant security patch or upgrading to a different FTP service. [2]

4.4 Need or Nice?

Whilst reviewing the systems and services a disciplined approach has to be taken to consider whether a system or service is a business requirement or just a "nice to have". If it is the latter then it is usually a good idea to remove the service, as less services generally mean less possible vulnerabilities. An attacker can't exploit a service that isn't installed.

4.5 Architecture

Once you have tightened the security of the individual servers it is also worth considering a separate network for them. Many firewalls support additional interfaces to allow organisations to physically separate networks. A firewall will have at least two interfaces; one for the internal network and one for the external network. When a third interface on a firewall is configured it is usually due to the requirement of hosting public services, the third network interface is commonly referred to as a demilitarised zone (DMZ) or service network. DMZ networks allow organisations to remove the risk of hosting public services by providing physical separation. As a public service is usually required to be accessed by un-trusted sources this is usually one of the easiest ways for a malicious hacker to break into a network. If the attacker discovers a vulnerability on one of the public services and compromises the server, they may be able to use this to gain access to the rest of the network, particularly troublesome if the public server resides on the internal network. However if the public server is hosted on the DMZ the

attacker still needs to break the firewall before they can gain access to the internal network.

5.0 Selecting a firewall

Once you have decided what to protect and improved areas of potential weakness as covered in sections 3.0 and 4.0, the next step is to choose a firewall. This needs careful consideration as the cost of a firewall varies from a few hundred to several tens of thousands of pounds. Below are two examples of Internet Security companies that retail firewalls. There are many more security organisations that manufacture firewalls that you may also wish to consider before making your final decision.

Checkpoint firewall-1 is considered by many as the leading firewall on the market today, it can run on several platforms including NT, Solaris and Nokia. Firewall-1 is based on a licensing model that depends on the number of hosts the firewall is expected to protect, the licenses are broken down in 25, 100, 250 and unlimited node protection. The more nodes you wish to protect the higher the cost. Most firewall-1 implementations are now being built on one of the reliable Nokia server models. The Nokia hardware range covers the majority of requirements quite successfully, providing the necessary number of network interfaces, throughput, memory and processing power.

WatchGuard Systems is another Internet Security company that has until recently concentrated on providing security for SME organisations. In my experience the WatchGuard Firebox III appliance range covers approximately 90% of SME security requirements. The Firebox is an appliance based firewall which means it is a hardware device built to run the WatchGuard firewall software only. Recently WatchGuard has released a new appliance range of firewalls called Vclass. This range of firewalls provides more network interfaces, higher throughput levels, increased memory and superior processing power than the Firebox range and therefore helps WatchGuard to compete with the higher end firewalls.

When selecting a firewall three key requirements needing appraisal (along with other elements) are network interfaces, manageability and resiliency. These are discussed below:

5.1 Network Interfaces

Two network interfaces (NIC) are needed as a minimum when running a firewall for an organisation; one for the un-trusted network and one for the trusted network. For any public services being hosted a choice is needed if you are going to require a NIC for a DMZ or service network. Future requirements need to be considered including the potential for secondary internal networks or additional DMZ facilities

5.2 Manageability

When selecting a firewall you need to think about the operational management up on installation. Questions to address include; does the

firewall support company monitoring systems?, when you want to make a rule change will you be able to use a Graphical User Interface (GUI) or a command line? Focusing on these questions will result in a firewall suitable to your circumstances.

5.3 Resiliency

Once your organisation has become dependent on its Internet connection for business critical services, what would happen if your firewall failed? This question prompts consideration of high avail ability options for your firewall. For example some firewalls support automatic failover so if the primary firewall fails the secondary firewall takes over the network protection and continues supporting the live connections. Alternatively a preconfigured firewall may be sufficient, allowing you to keep a preconfigured cold swap firewall in the cupboard, which could be connected in place of the primary firewall if it failed. This would mean down time between the firewalls being swapped over, but would usually be considerably cheaper than an automatic failover option.

6.0 Additional Security Systems

So you have installed your firewall and everything seems to be working as expected. You have a firewall that is being actively managed and regularly patched and updated to ensure your network is protected from the latest threats. Attention now turns towards upgrading your security solution to help increase protection against determined malicious Internet hackers.

This section outlines technologies and tools a vailable to step up your protection, it is by no means a conclusive list but provides enough information for beginning to think about the next step.

6.1 Intrusion Detection System (IDS)

IDS is probably the next system a company would purchase if they felt they were at a high risk from attack. IDS is a signature based defence system that works by monitoring all of the network traffic looking for suspicious activity.

IDS can be explained through the simply analogy of IDS as the equivalent of a burglar alarm on a house. A burglar alarm uses sensors to detect suspicious movement and upon making a detection alerts the owner through sounding the alarm. This is the same principle with IDS as it uses sensors placed strategically on the network to monitor for suspicious activity. If one of the sensors makes a detection it alerts the administrator, for example through sending an email.

Depending on you specific requirements there are two different types of IDS; host based or network based. Host based systems monitor a single computer whilst network based systems monitor an entire network or a section of a network. Host based systems rely on the system or event logs of the machine it is residing on. When an entry is

made into one of the logs the host based IDS cross matches it with a database of attack signatures. If the log entry or entries match an attack signature the host based IDS can take several actions such as sending an email, initiating an SNMP trap, terminate the user login, etc.

Network based systems rely on the raw data packets being sent across the network. The raw data is analysed by the IDS to look for attack signatures. If the IDS can match a raw data pattern with an attack signature then the system is triggered to raise an alert, this can include but is not limited to sending an email, changing the firewall rule set, logging to a console, etc.

6.2 Vulnerability Scanning

As soon as you establish an Internet presence, whether going live with your website or connecting your network to the Internet you are highly likely to be probed by a potential attacker. These attackers will generally run automated tools against you to discover weaknesses and potential loopholes in your Internet presence. They will then use this information to help make targeted attacks against you.

So why not get hold of some of these tools and run them against your network before someone else does. This will put you in the malicious hackers shoes and help you to highlight your vulnerabilities. You can then use this information to make the necessary changes; this could include patching your systems, altering your firewall configuration or changing your network topology. There are some excellent open source tools available which are more likely to be used by malicious attackers due to there free availability on the Internet. Some of the commercial tools can be expensive and therefore are less likely to be used by an attacker, however many if not all of the commercial tools are usually available on an evaluation or trial basis.

Some well known commercial tools include a product called Retina, produced by eEye. Retina was recently voted as the best network security scanner by the readers of Information Security magazine. The scanner is acknowledged for producing accurate results as well as its speed of use. Another example of a commercial scanner is Internet Scanner, available from a company called Internet Security Systems (ISS). It is very easy to use and is complemented by additional scanners from ISS which are called Database scanner and System scanner. [9, 10 & 11]

The two most widely used open source tools are Nmap and Nessus. Nmap, written by Fyodor is an excellent Port Scanner, available on almost every platform including Linux and NT. It can carry out many more tests than usually required of port scanners, including OS fingerprinting, TCP and UDP port scanning, simultaneous multiple host scanning and a wide range of advanced scanning techniques. [6]

Nessus is one of the more popular vulnerability scanners, mainly due to it being regularly updated on a daily basis by an active group of

developers and its plug-in architecture. This architecture allows you to write your own security tests in C or its own scripting language called Nessus Attack Scripting Language (NASL). However there are more than 1200 plug-ins already for Nessus with more being produced in response to new security vulnerabilities. Nessus operates a client server model which requires a LINUX or UNIX system for the Server element and an X Window or Windows platform for the GUI Client. The server is responsible for carrying out the scanning once it has taken its instructions from the client. Nessus can produce good reports which can be in various formats including HTML and TXT depending on requirements. If you are planning to use open source tools to help protect your network, Nessus is a necessity. [7]

6.3 Security Policy

A security policy complements security systems and procedures put in place by an organisation. If there is a document outlining the Information Security guidelines which employees can read and agree to, overall company awareness increases. This means the organisation has a workforce aware of Internet risks and can also assist with disciplinary issues, for example if Internet access is covered in the policy and an employee abuses the access, it is easier for the organisation to discipline the employee.

A security policy assists an organisation in identifying potential risks. This could be through outlining access points to the network, the firewall, Remote access dial in servers, private links to other offices and third party connections.

The above are just two areas a policy would cover, but as you can see just from the examples a security policy would benefit most organisations.

6.4 Additional firewall

It can be beneficial to consider implementing a second Internet firewall to achieve two main benefits. Firstly, if a vulnerability is discovered for your primary firewall, more than likely the same vulnerability will not work against your secondary firewall. Secondly, if you make a mistake in the rule set of one of the firewalls hopefully you won't have made the same mistake in the second firewall which means it is less likely that you will inadvertently exposed your network. You need to be careful when implementing a second Internet firewall as it can become complicated and therefore harder to manage.

You may also wish to implement an additional firewall to help protect internal networks, for example an organisation may wish to restrict access to the Finance systems.

7.0 Conclusion

This paper provides an insight into why companies choose only to implement a firewall, what digital assets need protection, how to review current systems and services, what to consider when selecting a firewall and finally how to use additional systems and tools to build upon your firewall implementation.

Internet Security requires constant attention, systems need to be regularly reviewed to ensure they are being protected from the latest threats. Whilst a firewall should give you a good basis of protection it is always best not rely on this one single system as protection. Try to build in additional security protection mechanisms to allow for failure. For example when using an ATM you must produce a bank card and enter your pin number prior to obtaining your money.

If after reading this paper, you only remember four elements when building an Internet security solution they are:

- Protect your assets
- Review current systems and services
- Elements to consider when selecting a firewall
- Additional building blocks for your security solution

Bibliography

1. CHAPMAN, D. B and ZWICKY, E. D (1995) Building Internet firewalls, United States: O Reilly. 1 – 17, 55 – 88,

2. SCAMBRAY, J, MCCLURE, S and KURTZ, G. (2001) Hacking Exposed Second Edition, United States: Osbourne / McGrawe -Hill. 349

Websites

3. "To prevent SMTP relaying with Microsoft Exchange Server". 04 Apr. 2003. URL: http://www.slipstick.com/exs/relay.htm (13 Apr. 2003)

4. "Welcome! – The Apache HTTP Server Project". URL: http://httpd.apache.org/ (13 Apr. 2003)

5. "CAN-200300017 (Under Review)". URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0017 (13Apr. 2003)

6. "Nmap – Free Stealth Port Scanner For Network Exploration & Security Audits. Runs on Linux/Wind". 19 Apr 2003. URL: http://www.insecure.org/nmap (13 Apr. 2003)

7. "Nessus". URL: http://www.nessus.org/doc/datasheet.pdf (13 Apr. 2003)

8. "eEye Digital Security" URL: http://www.eeye.com/html/Products/Retina/index.html (13 Apr. 2003)

9. "Enterprise Protection" URL: http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php (13 Apr. 2003)

10. "Enterprise Protection" URL: http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_database.php (13 Apr. 2003)

11. "Enterprise Protection" URL: http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_system.php (13 Apr. 2003)

Last Updated: July 26th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	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
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
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
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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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
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 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
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event