Global Information Assurance Certification Paper

Intrusion Detection and Prevention – It's not just IDS vs. IPS

By Jason Duran

GSEC Practical Assignment, Version 1.4b, Option 1
October 15, 2003

Abstract

In today's society, we cannot experience a day that goes by without a new virus/worm being released, a new vulnerability being announced or a new patch that requires downloading to secure our operating systems, firmware and applications for which these vulnerabilities have been exposed. During these times of rapid change, users need to be educated, administrators need to be trained and have the ability to work with the technologies that can help secure a network environment.

In order to achieve confidentiality, integrity and availability, a defense in depth approach must be taken towards securing our environments. This approach is about intrusion detection and prevention, but entails much more than just the argument of IDS vs. IPS. This document is intended to answer the following questions: Why are Intrusions taking place at an alarmingly increasing rate? What kinds of threats and vulnerabilities exist? What kinds of tools, technologies, policies and good practices need to be in place? What initiatives are underway and need to be taken to help in securing Cyberspace?

1. Why are intrusions taking place at an alarmingly increasing rate?

A. Hackers

Let's start by defining a person who may attempt an intrusion. A **Hacker** was once defined as a skilled individual with an advanced knowledge of computers, networks and their operation. The dictionary definition of a hacker is "a computer user who attempts to gain unauthorized access to computers"[1]. There is a different understanding between the general public and the IT community. IT professionals like to categorize a hacker by dividing them into two groups and separate them only by determining their motivation and intentions.

The **White Hat Hackers,** also referred to as **"White Hats",** are those who find security vulnerabilities, exploits and security loopholes. Instead of using this knowledge in a negative way, they choose to publicly post the information they've obtained or contact a vendor to make them aware of a vulnerability relating to their product. This increases the community awareness and prompts vendors to release a security patch or fix. The **Black Hat Hackers, also referred to as "Black Hats"or "crackers"**, are those who also find vulnerabilities, exploits and security loopholes. However, their intentions are the opposite of the White Hats.

[1] Barber, p. 631

The Black Hats will use this knowledge for personal gain, to cause damage to systems and networks and release malicious code that may be used to compromise and expose weaknesses and vulnerabilities. A **Grey Hat Hacker** lies somewhere in between, playing both sides. And, because of this, is probably the most dangerous.

B. Black Hat's Motives

The motivation behind Black Hats' actions depends, of course, on the individual. However, most Black Hats are actually casual hackers motivated by the enjoyment of the challenge, curiosity, spam relays, the opportunity to spread worms and or take full control of others systems. They sometimes thrive on the ability to get away with stealing things that don't belong to them. Some common hacks pertain to software, subscriptions, music, movies, phone, internet account use, wireless access and phone use (phreaking). Many crackers have nothing better to do and may be categorized as outcasts with little or no friends, lacking social skills, and in need of a place to belong. Other motives include politics, organized crime rings, seeking financial gain, stealing of credit card numbers and trade secrets. Unfortunately, there is no end to the possible motives and the growth of the hacking community, threats and vulnerabilities continue. Today, it is even common for Black Hats to host their own conferences and on-line hacking challenges.

Increased attacks

There are many things that contribute to the fact that the number of attacks, threats and vulnerabilities are increasing at an alarming rate. The amount of users on-line and the speed at which they connect has increased exponentially over the years. The malicious tools that are available, complemented by the ease of the retrieval and use of these tools, is a huge concern threatening the security of Cyberspace. Businesses reliance on computers, email, networks and the internet has also been a factor in the heightened level of threats and vulnerabilities.

> According to statistics from Carnegie Mellon's CERT Coordination Center, the number of IT security incidents reported has steadily grown from 52,658 in 2001, to 82,094 in 2002, and in just the first quarter of 2003, there were 42,586 reports – setting the pace for the potential to double last year's numbers.[2]

[2] Trilling, p.1

2. What are some common threats vulnerabilities and attacks?

A **vulnerability** can be defined as a point of weakness at which a system or network is susceptible to an attack.

A **threat** is considered to be a person, item, tool or event that may be used to exploit a vulnerability. For example, if an office had no password policy in place or strong password enforcement of any kind, then a weak password would be considered a vulnerability. The threat would be that someone may find out about the vulnerability and use tools or processes that could exploit it.

"The majority of successful attacks on operating systems come from only a few software vulnerabilities. This can be attributed to the fact that attackers are opportunistic, take the easiest and most convenient route, and exploit the best-known flaws with the most effective and widely available attack tools.[3]"

Software vulnerabilities and exploits usually occur in cycles. First of all a hacker must find a vulnerability. What he/she does with the knowledge they've obtained is up to them. Eventually, the information will get to the vendor who will supply a patch for the vulnerability while announcing the type of systems affected, description, impact and solution. When the information becomes publicly available, Black Hats will write and publish scripts or programs that have malicious intent in exploiting the vulnerabilities. Coincidentally, when these worms, viruses, scripts and tools are written, even unskilled hackers, better known as **script kiddies**, are able to use them to cause potential damage.

A. Common Vulnerabilities

Policies – A potential weakness in an organization is a lack of a working Security Policy, documented procedures, standards or guidelines. Within a defense in depth strategy, everything starts and stops with the security policy. Support from management and a well documented policy and strategy need to be in place and adhered to. If a solid security policy is not in place, an organization increases their risk and challenge of properly securing their network infrastructure.

Passwords - Weak passwords, lack of encryption during authentication and a non-existing or out of date password policy can cause grief to any organization. Passwords can be used against a company by unauthorized persons and can be stolen in several ways including: social engineering, password cracking, and traffic sniffing.

Access Controls - If proper access controls are not in place on files, Firewalls, Intrusion Detection Systems, and other network resources, it will make it easier for an insider or external intruder to gain access to confidential information.

[3] Sans/FBI Top 20 List, p1

There are different security models to follow and several areas that require these ACL constraints. However, details on this subject is beyond the scope of this paper.

Operating Systems - Many operating system vulnerabilities exist, are later exposed, and aren't always patched in a timely manner. However, administrators must keep patches and hot fixes up to date; harden the operating system while still allowing the servers to perform only the services necessary for business use.

Applications – Application vulnerabilities are common and are probably most dangerous when they are exposed on a web server. Vulnerabilities within applications often become exposed and exploited requiring the vendor to create a patch or fix. Internet Explorer, SQL Server, Apache Web Server, and IIS are some of the most common applications that require continuous patching with vulnerabilities being continuously found. And, on some occasions, the vulnerabilities are of critical threat levels. Many applications are susceptible to buffer overflow attacks which are programmer errors and can be used to distract servers and allow an attacker to execute malicious code.

Protocol Level Vulnerabilities – Protocol vulnerabilities are widely exploited probably because of common use and routing over the internet. Protocols are primarily exploited during the scanning and probing process a Black Hat uses to determine versions of operating systems and application versions in your environment. Avoiding the use of, or taking extra controls and monitoring is necessary when considering SNMP, FTP, TFTP, SSH, DNS, and RPC.

Remote Access – Connecting remotely through the internet is a risky process and requires Integrity on the server and computer establishing the connection. One of the most overlooked items that I've seen when speaking about Remote Access systems, is the amount of trust that is placed on the remote computer. I personally would not allow any computer that is not centrally managed, to access a network remotely. Weak passwords, lack of solid encryption and a weak operating system on the remote host spell trouble for networks which allow remote access connectivity. VPNs, Secure Tokens, IPSec, RADIUS, and a combination of encryption services, protocols and devices should be evaluated and included in your remote access realm.

Internal Abuse – This, surprisingly enough, is one of the most common threats. Many of the internal threats come from people who have legitimate access and know where to get what they want. They can misuse resources by downloading and installing illegal software, initiating attacks, spamming or stealing anything for personal gain. Insiders have an upper hand on outsiders with better access to information and opportunity. They can also be a prime source of information leaks by doing the digging on the inside while passing it to those who can utilize the information obtained on the outside.

B. Types of threats and attacks

Attacks can be considered active or passive. For the most part, successful passive attacks such as packet sniffing and social engineering, will also result in active attacks.

Trojans and Backdoors - Trojans and backdoors are resident on a computer and provide "backdoor" methods for a hacker to get into a network. Trojans can be packaged inconspicuously in programs so that users cannot notice they have been infected. The amount of control and information that can be obtained could be very damaging to any organization. Trojans and backdoors are not always detected by common antivirus programs and updated Client IDS systems. Updated and varying methods of deploying and hiding this malicious functionality continues to keep hackers one step ahead of detection.

Virus – A virus attaches itself to a file or files, is incapable of self-replication and must instead be executed. Viruses can reside in memory, boot sectors, executables, macros, virtually any other type of file, and may be encrypted. A virus can include preventative measures to monitor a computer's activity, detect an initiated virus scan and contain the ability to fool the scanner into thinking that a different virus is resident. These are some common virus categories:

> **Stealth –** Stealth viruses must be run in memory and therefore can be detected. However, while active, stealth viruses can modify the information retrieved from dir and mem commands, and hide changes made to boot sectors and files.
>
> **Polymorphic –** A polymorphic virus can continue to change the way it appears when it infects different files. It is able to do this by using different forms of encryption and decryption each time. This, of course, makes for a difficult virus to completely detect and remove.
>
> **Bomb –** A bomb is a virus waiting to happen. It is a file that resides on a computer and is triggered by a certain time or event.

Worms – A worm can be created to perform the same type of malicious activity that a virus can. However, a worm is not considered a virus because it is capable of self-replication. Worms may pose the largest threat because of the speed of replication and the number of machines that can become infected by them. Worms of today can be multiplatform, polymorphic, metamorphic and exploit multiple vulnerabilities.

DOS (Denial of Service) – DOS attacks exploit TCP/IP and the way that the systems handle SYN requests. Ultimately, a successful DOS attack results in a total consumption of bandwidth and resources on a target system or network. DOS attacks can be launched by a single computer, or can be a distributed attack by multiple systems, better known as a DDOS.

Spam Relays – It is important that an email administrator deny relaying on their mail servers. An attacker may try to use your server for spam while changing the reply-to address to make it appear as though the messages are coming from your domain. Spammers will use robots to gather email addresses from the web or pay a few dollars for lists of thousands to millions of established address lists. Their intentions are simply to hope that you and others they email, will be one of a small percentage to respond to their get rich quick, or pornographic related offers. Blacklisted address databases are available on the internet and can be connected to for a small fee – an example of this is available at: http://mail-abuse.org.

Man in the Middle – A man-in the middle attack involves the interception of an ongoing session between two computers. This is a passive form of attack (packet sniffing) which turns active once the attacker injects information and impersonates one of the two computers, taking over one side of the conversation.

Alternative Data Streams (ADS) – This can be a very difficult type of file to detect. An ADS is a hidden file that can be associated with a clean file and is not seen while browsing data in explorer or via command prompt. Many people do not even know this exists as a part of the NTFS file system. ADS was originally created for compatibility with the Macintosh Hierarchical File System (HFS). Unfortunately, ADS can be used to hide .exe, .vbs, and other type of files which can be used to cause damage to a computer or log information. Because a hidden file is used to call other files, real-time antivirus protection can be useful in ADS detection. However, most files go unnoticed by current antivirus programs and other specialized Ads detectors such as LADS and CrucialADS should be evaluated.

Blended Threats – Blended threats use characteristics of worms, Trojan horses and viruses. A blended threat is one that uses multiple methods to attack and spread itself, causes harm and exploits known vulnerabilities.

Zero Day – Attackers often exploit known vulnerabilities which have been uncovered for an average of six months. However, we are getting closer to the day when an exploit comes out at the same time as a vulnerability, better known as a zero-day exploit. With less and less reaction time and a constant increase in the hacking community, we could see a series of highly successful zero day exploit attacks.

Rootkits – A rootkit is a collection of files developed to allow an attacker to take full control of a system without being detected. A rootkit integrates backdoors into existing programs and/ or the operating system. Depending on the rootkit, a number of registry entries, application files, and operating system files are replaced. Worse yet, there are rootkits that replace the kernel making it even more obscure. For more information on this subject, please visit http://www.megasecurity.org/Info/p55-5.txt.

3. What kinds of tools, technologies, policies and good practices need to be in place?

Security Policy - In order for security to work in an organization, it must begin with a solid security policy and support from upper management. A security policy dictates goals, responsibilities, and the direction of security practices within the company. The importance of the security policy cannot be overlooked as, if implemented properly, should provide a scope and direction for all security endeavors within the organization. A company must communicate this policy to its employees and make sure that it is updated and audited on a regular basis. Once the security policy is in place, standards, procedures and guidelines can be created, a Trusted Computing Base can be established, and movement towards defense in depth can commence. There are other related documents and policies that need to be in place such as a BIA, BCP, DRP email policy, remote access policy, and user policy. However, this exceeds the focus of intrusion detection and prevention.

Network Security

Firewall – A Firewall, which blocks incoming and outgoing data based on your policies and needs. There are many different types of Firewalls. However, when choosing a firewall, one should make sure that it is ICSA certified. For a list of ICSA firewalls, check out the website: http://www.icsalabs.com/html/communities/firewalls/newsite/cert.shtml.
There are software based Firewalls that can be installed on existing computers and hardware based which contain the same functionality but their sole purpose is to provide firewall functionality and related services.
Some types of firewalls include:

> **Packet Filtering –** A packet filtering firewall or screened router is an entry level firewall which provides network level packet routing. This can be used in combination with another firewall where it can be utilized to take some of the load off of a company's primary firewall. However, a packet filter is not recommended as a single source of traffic blocking if your intentions are to protect sensitive information. The main reason for this is: packet filtering firewalls are limited to access rules based on source and destination ip addresses.

Stateful Inspection – These firewalls also perform packet filtering, but look at all communication layers and offer better forms of security such as user authentication and the ability to pass data by application type. The session state information is stored in a table and is used, along with a list of rules, to allow or deny packets – this process in known as stateful inspection.

Proxy – Proxy firewalls add increased security at the application level and can cache websites, block urls and selected words or data. The entire packet is evaluated and because of this, many people feel that this is the most secure type of firewall.

No matter which type of firewall, or combination of firewalls you choose to operate, the most important things to make sure of are proper installation/configuration and constant monitoring.

Antivirus – Antivirus software is a must for any organization. If possible, antivirus software should be strategically placed on an internet gateway, an email server to scan incoming and outgoing attachments and messages, servers and client systems.

Encryption – Encryption should be used for network traffic, authentication and any type of communication local or remote where sensitive information may be transferred.

Network Intrusion Detection System (NIDS) – A Network Intrusion Detection System should be placed outside the firewall, on any DMZ in place, and on every segment of an internal network if possible. The benefits an NIDS is that it is another layer of detection when any malicious traffic gets past any defense mechanisms in place. In contrast, an NIDS cannot handle encrypted traffic, requires a great deal of time to properly configure for your environment, and can subject administrators to wasted time because of many false positives. Many alerts are reported by an NIDS, and this causes other serious attacks to slip through without being noticed. Because an NIDS has a promiscuous NIC card which listens to all passing traffic, it should be plugged into hub or a mirror port/scan port of a switch. In order for an NIDS to be more useful than hindering, it must be configured to suit its environment, and be monitored and updated regularly. If you do not have enough time to dedicate towards an NIDS, outsourcing services should be considered.

DMZ – A DMZ, which stands for demilitarized zone, provides another layer of protection from attack. Any server which provides internet services such as HTTP and SMTP should be placed in a DMZ. The DMZ is separated from your internal network in order to keep attackers away from network resources should the server hosting internet services become compromised.

Honeypot – A honeypot is a computer designed to allow a cracker to break in and have his methods and actions monitored. It should not have any production information on it whatsoever. Similarly, its main objective is to be used as a learning device. Information on the honeypot is captured and analyzed to find out more about attack points and tactics. There are free versions of honeypots and commercial applications as well. A honeypot should be placed in the DMZ of a Firewall outside of the internal network. For more information on honeypots, please visit http://www.tracking-hackers.com.

Vulnerability Test – Vulnerability tests should be performed on systems and networks as often as time allows. The vulnerability testing application chosen should provide testing on a full range of networks, switches, operating systems and applications. Good vulnerability scanners will report vulnerabilities on a wide range of services, categorize them by level of importance and provide information on how to fix or patch the weaknesses found.

Server Security

Servers should be patched, hardened, have policies in place for authentication, ACL's and event monitoring. Both physical and logical controls must be tight and in place for each and every server in production. Placement of these servers in the network design is also an issue and should be decided based on the services they intend to provide. The importance of these items cannot be overlooked and are ongoing responsibilities to audit and change as necessary. The minimal services should be installed on each server and a good backup system and policies must also be in place in case of an attack, crash or disaster.

Host based Intrusion Detection Systems (HIDS) – Host based Intrusion Detection Systems can be installed on servers that host sensitive information or provide services that are often vulnerable to attack. Depending on the product chosen, a host based IDS can report local changes to system files, policies, registry entries and user privileges. An HIDS does not require as much overhead as an NIDs because it only reports traffic related to the individual host computer that it resides on. Similarly, an HIDS can be utilized to detect attacks which are not detectable by an NIDS.

Intrusion Prevention System (IPS) – There is controversy involving the IPS and its definition and true services provided. However, it can possibly be defined as the evolving of an IDS, thereby using the same IDS signatures, while additionally preventing detected attacks. The IPS must be inline on the network and may block valid traffic if it reacts on false positives. The product itself need time to mature at which time, a true definition can be defined.

Encryption/authentication – Any communication transferred should be encrypted wherever possible. This includes network traffic, email, authentication, VPN for remote access, wireless, and any sensitive information that is hosted on the web. There are different algorithms, ciphers, types of encryption and management/cost factors involved. These along with confidentiality level required must be evaluated before deciding upon a suitable solution for each circumstance.

Tools of the Trade

Securing the infrastructure is more time consuming than in the past because increased layers of security are no longer a possibility, but a must in terms of network survival. It is important to be able to think like an attacker and look at points of entry, possible weaknesses and tools that provide you with valuable information. A security administrator should use tools and tactics as an environment testing process to make sure that appropriate countermeasures are in place to prevent and detect attacks. A few simple tools which I consider a good start in the creation of an administrator's toolkit are: Tripwire, Nmap, Nessus, Ethereal, Traceroute, Windump, HPING2, Dsniff, GFI Languard, L0phtCrack, Fport, Netstumbler, and Fragroute.

A good website to study up and download these tools is located at: http://www.insecure.org/tools.html.

Client Security

Clients should have limited access and local execution rights to the computers they use within an organization. The operating system must be hardened, patched and have appropriate levels of policies and auditing in place. I would not recommend running any client system without Antivirus, and a client Firewall/IDS system installed if internet access is required. Similarly, all of these items should be centrally managed and automatically updated wherever possible. This does not put the burden on a user or administrator to have to manually visit each and every computer whenever a new update becomes available. Other remote tools such as SMS or Update Expert should also be evaluated and considered to help with this process.

4. What initiatives are underway and need to be taken to help in securing Cyberspace?

The National Strategy to Secure Cyberspace – The National Strategy to Secure Cyberspace, is a vital initiative and a key component of the Nations overall Homeland Security plan. It was created because of the worldwide dependency on the internet and the importance of security relating to the interconnectivity of computers around the globe.

"The five national priorities are the creation of:

1. A National Cyberspace Security Response System

2. A National Cyberspace Security Threat and Vulnerability Reduction Program
3. A National Cyberspace Security Awareness and Training Program
4. Security Governments' Cyberspace
5. National Security and International Cyberspace Security Cooperation"[4]

The strategy is to be a continuously combined effort between the Government, Private Sector and citizens of the United States. I think that once this effort is completed, it will help Cyberspace overall and create/ partner with many other national initiatives that will be brought forward and improved upon.

Next Generation Secure Computing Base (NGSCB) – Microsoft is trying to build a Trusted Computing Base by using NGSCB to increase system integrity, security and privacy within a Windows environment. This initiative will require new hardware and software to be rewritten in order to comply with the standards. Some of the planned improvements to Windows involve secured memory usage, secured files via encryption and hardware combination, protection on layer 7 of the OSI model, and the requirement of proven identity before communication can take place. Another important objective is that a secured channel is created between input and output devices. This would make it difficult for Spyware or Trojans to be successful.

The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) – OCIPEP is a Canadian initiative created for the same reasons as the US strategy towards securing cyberspace. Similarly, the partners involved are Public and Private Sector, as well as key international partners, primarily the U.S.A.. The primary objective is to create national emergency preparedness and centralize alerts of threats and vulnerabilities to departments and agencies. OCIPEP plans to expand their services to providing advice and assistance relating to malicious incidents. A future OCIPEP initiative may be to setup information sharing relating to policies and collection/analysis of malicious data.

Security Intelligence – Because Firewalls primarily protect against layer 3 and 4 attacks, many new exploits take advantage of Layer 5-7 vulnerabilities. A more preventative approach with less false positives must be added as another layer of security. This will probably be in the form of a gateway appliance with multiple security objectives and more AI features that increase the "learning" capabilities which in turn will reduce false positives and provide better overall security against protocol anomalies, vulnerabilities and exploits.

[4] The National Strategy to Secure Cyberspace – p. x

Conclusion – The use of the internet and speed at which we connect provides anyone the opportunity to perform malicious activity. There are many threats, vulnerabilities and exploits that appear publicly on a daily basis. Unfortunately, there is no more time in the day. However, security professionals still face the challenge of securing their environment. In order to do this, we must continually share information and keep our systems, networks, and ourselves up to date with the latest tools, information and resources. As attacks increase, so to does awareness, communication, sharing of information, and initiatives. This problem is realized world wide and many major initiatives are underway and need time to mature. We never wait and see what may happen, but instead continue to evolve.

References –

Myasnyankin, Vladislav V. and Chuvakin, Anton. "Complete Snort-based IDS Architecture, Part One." November 6, 2002.
URL: http://www.securityfocus.com/infocus/1640

Cuff, Andy. "Intrusion Detection Terminology (Part One)." September 3, 2003.
URL: http://www.securityfocus.com/infocus/1728

Cuff, Andy. "Intrusion Detection Terminology (Part Two)." September 24, 2003.
URL: http://www.securityfocus.com/infocus/1733

Spitzner, Lance. "Honeypots: Simple, Cost-Effective Detection." April 30, 2003.
URL: http://www.securityfocus.com/infocus/1690

Skoudis, Edward. "Malware – The Worm Turns." July 2002.
URL: http://infosecuritymag.techtarget.com/2002/jul/wormturns.shtml

Trilling, Steve. "The Changing Face of Cyber Attacks." July 1, 2003.
URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=2305&EID=0

McAlearney, Shawna. "Zero-Day IE exploit just the beginning." Oct 1, 2003.
URL:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci930187,00.html

Briney, Andrew. "Security Gets Smart." June 2003.
URL: http://infosecuritymag.techtarget.com/2003/jun/note.shtml

"The National Strategy to Secure Cyberspace." February 2003.
URL: http://www.whitehouse.gov/pcipb/

"Next Generation Computing Base." June 2003.
URL: http://www.microsoft.com/resources/ngscb/four_features.mspx

"Microsoft Next – Generation Secure Computing Base – Technical FAQ." July 2003.
URL: http://www.microsoft.com/technet/security/news/NGSCB.asp?frame=true

"Sans/FBI Top 20 List – The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus." May 29, 2003.
URL: http://www.sans.org/top20/

McClure, Stewart, Scambray, Joel and Kurtz, George. Hacking Exposed: Network Security Secrets and Solutions, Fourth Edition. McGraw-Hill/Osbourne, 2003.

Brenton, Chris and Hunt, Cameron. Active Defense: A Comprehensive Guide to Network Security. Sybex Inc., 2001.

Beale Jay, Foster, James C., and Posluns, Jeffrey. Snort 2.0 Intrusion Detection. Syngress Publishing, Inc., 2003.

Barber, Katherine. The Canadian Oxford Dictionary. Oxford University Press Canada, 1998.

Hoglund, Greg. "A *REAL* NT Rootkit, patching the NT Kernel."
URL: http://www.megasecurity.org/Info/p55-5.txt

"Certified Firewall Products."
URL: http://www.icsalabs.com/html/communities/firewalls/newsite/cert.shtml

"HoneyPots: Frequently Asked Questions."
URL: http://www.tracking-hackers.com/misc/faq.html

"Top 75 Security Tools."
URL: http://www.insecure.org/tools.html

Last Updated: September 24th, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive