Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Intrusion Prevention Systems- Security's Silver Bullet?

Presently available network security components like Firewalls, Anti-Virus programs and Intrusion Detection Systems (IDS) cannot cope with the wide range of malicious attacks and zero day exploits on computer networks and systems. Multi-exploit worms like Nimda, Trojan horses, and polymorphic viruses are penetrating defenses, causing downtime and huge financial loss to businesses. "Script kiddies" can create malicious code with tools like Fragrouter and ADMutate. This paper takes a look at Intrusion Prevention Systems ...

Copyright SANS Institute

Author Retains Full Rights

AD

INTRUSION PREVENTION SYSTEMS – SECURITY'S SILVER BULLET?

BY
DINESH SEQUEIRA

GSEC Version 1.4B
OPTION 1

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

TABLE OF CONTENTS

Introduction 3
Security Components 3
Anti-Virus Programs 3
Firewalls 4
Intrusion Detection Systems (IDS) 5
Types of IDS 5
IDS Evasion Techniques 6
Intrusion Prevention Systems 7
IPS Approaches 8
Types Of IPS 9
Host based Intrusion Prevention (HIP) 9
Network based Intrusion Prevention (NIP) 10
Summary 11
Works Cited 12

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Introduction

Presently available network security components like Firewalls, Anti-Virus programs and Intrusion Detection Systems (IDS) cannot cope with the wide range of malicious attacks and *zero day exploits* on computer networks and systems. Multi-exploit worms like Nimda, Trojan horses, and polymorphic viruses are penetrating defenses, causing downtime and huge financial loss to businesses. Predictions are that it will get worse (Skoudis). “Script kiddies” can create malicious code with tools like Fragrouter and ADMutate. CERT (Computer Emergency Response Team) Coordination Center at Carnegie Mellon University reports that the number of reported security incidents is doubling each year (CERT/CC).

This paper takes a look at Intrusion Prevention Systems (IPS), preceded by a history of network security components that fortify our networks. An understanding of Firewalls, Anti-Virus programs, and IDS is important, before moving onto IPS. Earlier systems have served us well, but with the proliferation of sophisticated attacks and the discovery of new vulnerabilities, new methods are needed to protect precious data and network resources.

IPS use a new proactive approach that stops the hackers (black hats) before they can do damage. Host and Network based IPS are now commercially available and more are to come in the next few months. Could IPS help secure our network and critical business assets? This paper probes into the technology behind these systems, why we need them, how they function, their pros and cons, and some highly rated products.

Security Components

Anti-Virus Programs

Two decades ago computer viruses were spread mainly by exchanging infected floppy disks. Viruses would infect files but needed human intervention to trigger them, like inserting a floppy disk or opening an email attachment. They spread slowly and this gave anti-virus vendors time to generate anti-virus signatures and distribute them. Anti-virus programs with updated signatures would then foil further attempts to break-in, containing the spread.

Today with networked systems and sophisticated polymorphic viruses, it is hard to keep up even though great progress has been made and vendors issue signatures for new exploits in a few hours rather than days. Currently, a typical encrypted virus can spread around the globe in a few hours while changing its size and characteristic byte code from computer to computer – thus circumventing pattern matching anti-virus software that must exactly match the attacking code to be effective. This approach has become reactive and in the ensuing period great damage has already been inflicted on thousands of target hosts globally. Anti-virus programs then basically become clean-up programs even though they have tens of thousands of signatures (Nachenburg). The white-hats are a step behind the hackers, not sure what the next exploit will do, similar to a cop watching out for a criminal, unsure about his modus operandi

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Worms spread automatically through networks without any user intervention or interaction. Worms like Nimda – a multi-exploit worm that compromised Windows PCs, and Code Red – a worm that spread via a buffer overflow exploit in Microsoft IIS Web Server (Skoudis). These have caused losses in the billions of dollars. Trojan horses replace key system files with malicious versions that perform pre-programmed destructive activities. SirCam is a worm that spreads through email. Once activated it acts as a Trojan horse and mails user files to email addresses in the user's address book.

Firewalls

A Firewall conjures up images of a safe and protected environment, but how safe is the firewall that guards the network as the first line of defense? It's anything but a wall! Firewalls can block traffic, but in order to share data and connect to networked resources, holes are punched through it. This then leaves the network vulnerable to exploits and open to malware. There are several types of firewalls, from static packet filters to the powerful application level proxy firewalls.

- Static packet filtering firewalls filter packets according to allow/deny rules based on the header fields like source/destination IP addresses and ports, protocol type and TCP flags. These firewalls do not look into the payload for malicious intent and it treats each packet as an individual entity. Border routers are good as static packet filters and are the first line of defense. The advantage is that it is fast, but it's prone to spoofing and fragmentation attacks.

- Stateful packet filtering firewalls are an improvement over static packet filtering firewalls, as it has a notion of *state.* In client/server applications, the client contacts the server with a request and receives a response. Since the client initiated the request the response is allowed in, bypassing the firewall rules and optimizing the screening process, thereby improving firewall performance. However the firewall needs additional resources to maintain *state* tables. *State* tables can be maintained in hardware or software.

- Stateful Inspection firewalls are an improvement over stateful firewalls for applications that use two or more ports, like FTP. Instead of leaving ports above 1023 always open for a data connection, it examines the payload and selectively opens and closes ports *on the fly* as per the protocol. To do this it needs to peek into layer 4 to 7 information and configure the firewall rules in real-time. This allows normally troublesome protocols like FTP to be passed securely.

- Proxy firewalls break up a client/server connection to examine the protocol's syntax. If it meets the rules it forwards it's payload to the corresponding daemon process. Proxy firewalls require a lot of resources,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

but provide a strong isolation between the internal network and the Internet.

Intrusion Detection Systems (IDS)

IDS are the second layer of defense. It detects the presence of attacks within traffic that flows in through the holes punched into the firewall.

As defined by Rebecca Bace and Peter Mell, "Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of *intrusions,* defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network."

Richard Kemmerer and Giovanni Vigna explain, "… intrusion detection systems do not detect intrusions at all - they only identify evidence of intrusion, either while in progress or after the fact." IDS identify security threats by detecting scans, probes and attacks but does not block these patterns; instead it merely reports that they took place. IDS logged data however is invaluable as evidence for forensics and incident handling. It detects internal attacks, which are not seen by the firewall and also aids in firewall audits.

Some attacks are contained in a given session but attacks also do occur in traffic spanning multiple sessions like port scans and network scans. These types of attacks are identified by IDS.

Types of IDS

There are two main categories of IDS based on the IDS alarm triggering mechanism - action that causes the IDS to generate an alarm. They are - Anomaly detection based IDS and misuse detection based IDS.

- <u>Anomaly detection based IDS</u> report deviations from "normal" or expected behavior. Behavior other than "normal" is considered an attack and is flagged and recorded. Anomaly detection is also referred to as profile based detection. The profile defines a baseline for normal user tasks. The quality of user profiles directly affects the detection capability of the IDS. There are various techniques for constructing user profiles -

    - Rule-based approach – Normal user behavior is represented by rules. Creating rules by analyzing normal traffic is a complicated task. Protocol anomaly detection falls under this category and analyzes packet flows.

    - Neural Networks – These systems are trained by presenting them with a large amount of data, and rules about data relationships. They then determine if traffic is normal or not. Abnormal traffic raises an alarm.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Statistical approach – Activity profiles characterize the behavior of system or user traffic. Any deviation from normal triggers an alarm.

The advantage of anomaly detection is that it can detect previously unknown attacks and insider attacks, without the need for signatures. It's also impossible for the attacker to know what activity generates an alarm and so they cannot assume that any particular action will go undetected. The disadvantage of this approach is in the large number of false positives – alerts that are generated due to legitimate activity. Besides being complicated and hard to understand, building and updating profiles also requires a lot of work (Carter).

- Misuse detection based IDS trigger an alarm when a match is found to a "fingerprint" – a signature contained in a signature database. These "fingerprints" are based on a set of rules that match typical patterns of exploits used by attackers. Since there is a known database of attacks, there are few false positives. The disadvantage is that they can only detect previously known attacks. Besides, the "fingerprints" database needs to be continuously updated to keep up with new attacks. IDS products available in the market today, mostly use misuse detection.

The other way to classify IDS is by monitoring location -

- Network based IDS (NIDS) sit behind the firewall, on the demilitarized zone (DMZ) or the private network and sniff packets in *promiscuous* mode invisible to the attacker. It monitors and analyzes packets and can use anomaly or misuse detection techniques. While the firewall screens out unwanted traffic, the NIDS will alert to what is "leaking" through the firewall. NIDS need to keep up with the high volume of traffic or else it could miss attacks. High speed is also essential for low latency. Thus, it's usually available as dedicated hardware appliances.

- Host based IDS (HIDS) software is run on each host. The software monitors and detects user and operating system activity and logs. Attacks on a given host are detected using misuse detection. HIDS have a closer and deeper look at the activity of attack tools on the host and should be employed on Web, DNS servers and target hosts.

IDS Evasion Techniques

Although there are various categories of IDS, IDS evasion techniques have also become sophisticated. The basic idea behind evasion is to fool the IDS into seeing different data than the target host thus allowing the attacker to slip through. IDS systems work fine for signature-based attacks but the new breed of stealthy attacks go unnoticed. Ed Skoudis, a distinguished SANS faculty member

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

points out, “The IDS vendors will have to graft on anomaly and behavior-based detection or they will die”.

Some of the IDS evasion techniques are -

- Polymorphic buffer overflow attacks - Polymorphic buffer overflow attacks, alter the attack’s shell code. ADMutate - an on line tool can take an attack’s shell code and transform it in such a way that the code looks different from the known signature but is functionally equivalent. Once it gets to the target, it reassembles, having eluded the IDS (SANS). Marty Roesch, the inventor of Snort says, “It’s a hard problem. The idea is that signature-based IDS like Snort look for traffic in a payload called Shell Code, but you can evade this with polymorphic shell code generation” (Messmer).

- Path obfuscation – The path statement looks different but does the same thing. For example /winnt/. /. /. / is the same as /winnt, but the signatures don’t match and so IDS will miss this attack (Frederick).

- Hex encoding – Hex characters can be used to represent characters in URLs. %20 means hex 20, is the equivalent of a space in ASCII. HTTP protocol uses hex encoding, but not all IDS understand it and so could miss an attack (Frederick).

- Unicode directory traversal – Directory traversal exploits use strings like “.. /.. /.. / ”. Most IDS have signatures to detect it, but attackers replace the slash with the Unicode equivalent, “%co%af ”, and evade the IDS (Frederick).

- Protocol anomalies – Host applications could vary in protocol implementation, as RFC’s may not be accurately specified. Network IDS may have a different interpretation of the protocol from that on the host (Handley).

- Fragmentation – Fragmented packets are typically reassembled only at the destination. Fragmented pieces of attack code could slip through, unleashing their evil intent at the end host (Handley).

Intrusion Prevention Systems

Traditionally, firewalls and anti-virus programs try to block attacks and IDS tries to identify attacks as it occurs. Such techniques are critical to a defense in depth approach to security, but have limitations. A firewall can stop services by blocking certain port numbers but it does little to evaluate traffic that uses allowed port numbers. IDS can evaluate traffic that passes through these open ports but cannot stop it. IPS can proactively block attacks.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Signature based approaches focus on how an attack works, trying to detect certain strings. If the attacker makes minor changes by using the IDS evasion techniques discussed above, the previously written signatures no longer detect the attack. IPS focuses instead on what an attack does, which does not change.

IPS Approaches

Some of the approaches being used are

1.Software based heuristic approach - This approach is similar to IDS anomaly detection using neural networks with the added ability to act against intrusions and block them.

2.*Sandbox* approach - Mobile code like ActiveX, Java applets and various scripting languages are quarantined in a *sandbox* - an area with restricted access to the rest of the system resources. The system then runs the code in this *sandbox* and monitors it's behavior. If the code violates a predefined policy it's stopped and prevented from executing, thwarting the attack (Conry-Murray).

3.Hybrid approach –On network-based IPS (NIPS), various detection methods, some proprietary including protocol anomaly, traffic anomaly, and signature detection work together to determine an imminent attack and block traffic coming from an inline router.

4.Kernel based protection approach – Used on host-based IPS (HIPS). Most operating systems restrict access to the kernel by a user application. The kernel controls access to system resources like memory, I/O devices, and CPU, preventing direct user access. In order to use resources user applications send requests or system calls to the kernel, which then carry out the operation. Any exploit code will execute at least one system call to gain access to privileged resources or services. Kernel based IPS prevents execution of malicious system calls.

Programming errors enable exploits like buffer-overflow attacks to over-write kernel memory space and crash or takeover computer systems. To prevent these types of attacks a software agent is loaded between the user application and the kernel. The software agent intercepts system calls to the kernel, inspects them against an access control list defined by a policy, and then either allows or denies access to resources. On some IPS systems the agent checks against a database of specific attack signatures or behaviors. It could also check against a database of known good behaviors or a set of rules for a particular service. Either way if a system call attempts to run outside its allowed *zone*, the agent will stop the process.

Vendors are using a combination of the above-mentioned approaches to ward off combined attack types seen on today's networks. Even though the above approaches are different the goal is the same – to stop attacks in real-time before they cause harm. Harm could be prevented by (Bobbitt) -

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Protecting System Resources – Trojan horses, root kits, and backdoors alter system resources like libraries, files/directories, registry settings, and user accounts. By preventing alteration of system resources, hacking tools cannot be installed.

- Stopping Privilege Escalation Exploits – Privilege escalation attacks try to give ordinary users root or administrator privileges. Disallowing access to resources, which alter privilege levels, can prevent this and block exploits like Trojan horses, rootkits, and backdoors.

- Preventing Buffer Overflow Exploits – By checking whether the code about to be executed by the operating system came from a normal application or an overflowed buffer, these attacks can be stopped.

- Prohibit Access To E-mail Contact List – Many worms spread by mailing a copy to those in the Outlook 's contact list. This could be halted by prohibiting e-mail attachments from accessing Outlook's contact list.

- Prevent directory traversal – The directory traversal vulnerability in different web servers allows the hacker to access files outside the web servers range. A mechanism that would prevent the hacker access to the web server files outside its normal range could prevent such malicious activities. Unix's has a chroot command that does this.

Types Of IPS

Host based Intrusion Prevention (HIP)

STORMWATCH

OKENA's StormWatch uses a kernel-based approach and works on servers and workstations. Policies - collections of access control rules based on acceptable behavior, is available out-of-the-box for common applications such as Microsoft SQL Server, Instant Messenger, and IIS Server. Policies control what resource is being used, what operation is being invoked, and which application is invoking it. StormWatch hooks into the kernel and intercepts system calls (Okena).

It has four interceptors:

- File System interceptor– intercepts all file read and write requests.

- Network interceptor – intercepts packet events at the driver (NDIS) or transport (TDI) level.

- Configuration interceptor – intercepts read/write requests to the registry on Windows or to rc files on UNIX.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Execution space (Run-time environment) interceptor - requests to write to memory not owned by the requesting application will be blocked by this interceptor. For example, buffer overflow attacks would be blocked here. Thus it maintains the integrity of each applications dynamic run-time.

Since StormWatch intercepts File, Network, Configuration, and Run-time operations and compares them to application-specific access control rules or policies; it can track the state of an application. For example, Network interceptor provides address and port blocking like a firewall; File system and Configuration interceptors monitor and prevent changes to critical files or registry keys. Network and File system interceptors provide worm prevention.

By correlating events from multiple systems at the management station, StormWatch not only blocks the threat but also pushes out a new policy to all agents and blocks future attacks. This reduces the number of false positives and false negatives.

Storm Watch has a utility program called StormFront. It serves as a data analysis and policy creation tool, which analyzes applications as they operate in a normal environment and generates policies. Any other application behavior would be considered suspicious. Resources accessed by the application are separated into file, network, registry, and COM categories.

ENTERCEPT's Standard Edition

Entercept, a pioneer in kernel-based protection, proactively protects the host by intercepting system calls (Entercept). Unlike Okena's StormWatch it uses both, signatures and behavior rules to stop and detect attacks.

In an article by Ed Skoudis on "infosec's WORST NIGHTMARES", some nightmares that he mentions are stealthier attacks and "super" worms – "Fast spreading, multiplatform, multi-exploit, *zero-day*, metamorphic worms". He goes on to say that one way of preparing for these coming "super" worms is to, "Utilize host-based intrusion detection and prevention tools such as Entercept Security Technologies and OKENA's StormWatch on critical systems to block or rapidly discover attacks."

Network based Intrusion Prevention (NIP)

NIPS are generally appliance-based systems that sit inline, and block suspicious traffic after detecting an attack. They utilize different detection methods, signature detection, anomaly detection, and some proprietary methods, to block specific attacks.

Some of the methods adopted by vendors are –

- <u>Stateful Signature detection</u> – It looks at relevant portions of traffic, where the attack can be perpetrated. It does this by tracking *state* and based on the context specified by the user detects an attack. It is not completely automatic, as the user needs to have some prior knowledge about the attack. For example, the Love letter worm can be detected by a rule that

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

would read as follows - “Look for “ILOVEYOU” in the subject field only, ignore this string anywhere else in the email.” Basically it does pattern matching using regular expressions, which allow wildcard and complex pattern matching (NetScreen).

- Protocol anomaly detection - All vendors do detailed packet analysis with protocol decode engines to ensure packets meet protocol requirements.

Traffic normalization is also done to remove protocol ambiguities and ensures that traffic interpreted by the NIPS is the same as that seen by the end host, so that we do not miss attacks.

All this resource intensive processing is done with the aid of dedicated hardware boxes for speed and latency issues. Devices are already available that work at gigabit speeds. If it cannot cope with traffic load then it would drop packets and miss attacks. NIPS are reported to have a high rate of false positives but have blocked thousands of known attacks. Products are just being released and their performance needs to be evaluated especially with new attack methods. The disadvantage of being in-line is that if the device fails the entire network it serves is down. This can be overcome by having, failover or parallel systems. Initial reports have been encouraging but false positives are high (Cummings).
Many of the vendors provide or intend to provide Firewall/IDS/Anti-virus and vulnerability assessment capabilities. Some vendors integrate with other firewall, IDS, and vulnerability assessment tools.

Summary

Firewalls, anti-virus, and IDS have their place in the security landscape, each with its unique features. Depending on business needs, budget constraints, and organizational requirements we need to draw up a security policy and that policy will determine the mix of components that need to be installed, to meet security goals.

IPS adds to the defense in depth approach to security and is an evolution of IDS technology. Its proactive capabilities will help to keep our networks safer from more sophisticated attacks. Today the use of tunneling and encryption means putting more content out of the reach of perimeter controls. Even though NIPS will prevent attacks, some could slip through and HIPS would prevent them. HIPS – the last line of defense provides “operating system hardening” with greater granularity and application specific control. *Intrusion prevention* is a generic term. Before purchasing a product, study the detection and prevention mechanisms vendors have implemented vis-à-vis current attack methods.

Security is hard, some attacks could still slip through and no amount of automation can replace trained and vigilant security personnel. But tools like IPS can reduce the tedium and provide a silver lining if not a silver bullet!

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Works Cited

Bace, Rebecca, and Peter Mell. " Intrusion Detection Systems." URL: http://csrc.ncsl.nist.gov/publications/nistpubs/800-31/sp800-31.pdf (15 October 2002)

Bobbitt, Mike. "Inhospitable Hosts." Information Security. Volume 5, No.10 (2002): 35-47.

Carter, Earl, and Rick Stiffler. Cisco Secure Intrusion Detection System. Pearson Education, 2001.

CERT/CC Statistics, 1988 - 2002.URL:http://www.cert.org/stats/cert_stats.html (20 October 2002).

Conry-Murray, Andrew. "Behavior – Blocking Stops Unknown Malicious code." Network Magazine. Volume 17, No.6 (2002): 50-55.

Cummings, Joanne. "Intrusion detection to Intrusion prevention." NetworkWorld. Volume 19, No.38 (2002): 72-82.

[Entercept]. "Attackers and Their Tools: How Entercept Protects Servers." URL: http://www.entercept.com/whitepaper/attackertools/AttackerTools.pdf (15 August 2002).

Frederick, Karen. "Understanding Network Intrusion Detection Signatures." URL: http://www.nfr.com/publications/white-papers/Understanding_NID_Signatures.pdf (20 October 2002).

Hollander Yona, and Romain Agostini. "Stop Hacker Attacks at the OS Level." URL: http://www.entercept.com/products/entercept/news/intsecadvmag.pdf (25 August 2002).

Kemmerer, Richard, and Giovanni Vigna. "Intrusion Detection: A Brief History and Overview." IEEE Security and Privacy, 2002 (2002): 27-30.

Handley, Mark, Vern Paxson, and Christian Kreibich. "Network Intrusion detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics." URL:http://www.icir.org/vern/papers/norm-usenix-sec-01.pdf (6 November 2002).

Messmer, Allen. "Put to the Test." NetworkWorld. April 15, 2002: 1 and 76.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Nachenburg, Carey. "Behavior Blocking: The Next Step in Anti-Virus Protection." URL: http://online.securityfocus.com/infocus/1557/ (6 November 2002).

[Netscreen]. "Intrusion Detection and Prevention - Protecting your Network from Attacks." URL:http://www.netscreen.com/solutions/idp_wp.asp (8 November 2002).

Northcutt, Stephen et al. Inside Network Perimeter Security. Indiana: New Riders, July 2002.

[OKENA]. "A New Approach To Intrusion Detection: Intrusion Prevention." URL: http://www.okena.com/pdf/IDS White Paper.pdf? (20 Nov 2002).

Paulson, Linda. "Stopping intruders outside the gates." IEEE Computer. November 2002,Vol 35, No.11 (2002): 20-22.

[SANS] "ADMutate" SANS News Bites, Vol 4, No. 16.

Skoudis, Ed. "Infosec's Worst Nightmares." Information Security. November 2002, Vol 5, No.11 (2002): 38 – 49.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**