Interested in learning more about security?

SANS Institute
InfoSec Reading Room

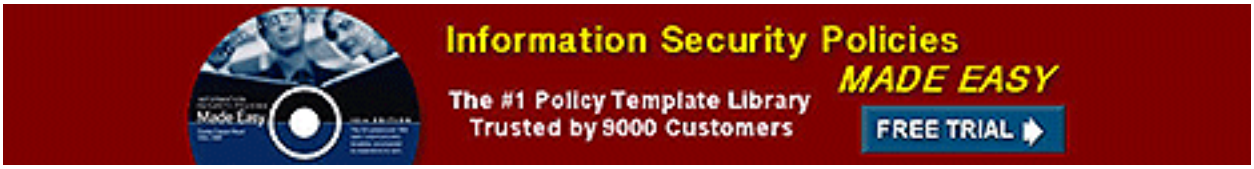
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Deception: A Healthy Part of Any Defense in-depth Strategy

Deception, which is one of the foundational offensive strategies employed by an attacker, can also be used by the defender. This paper will define and discuss the major components of a multi-layered defense with special emphasis on security policies and their framework, how it can be used by the defender, deception tools used in a defensive strategy, and it's role in a multi-layered defense.

Copyright SANS Institute
Author Retains Full Rights

AD



Deception: a healthy part of any Defense in-depth strategy

Paul Anderson

GSEC version 1.3

February 15, 2001

© SANS Institute 2002, Author retains full rights.

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

Deception: a healthy part of any Defense in-depth strategy

Introduction

With the increase of terrorist and cyber attacks, information assurance is on everyone's mind. New vulnerabilities , self-propagating viruses, and trojan programs, increasingly pose a threat to the functionality and productivity of our business community. If we look at current history, we see a multitude of attacks on the availability, confidentiality, and integrity of our corporate information systems. Viruses, worms, denial of service attacks, session hijacking, syn flooding, man in the middle attacks, all have contributed to countless hours of downtime and loss of productivity. With such a multi-layered arsenal arrayed against our poor system administrator, the need for a multi-layered defensive strategy becomes evident. In many instances, attackers use deception and stealth to accomplish their goals. Deception, which is one of the foundational offensive strategies employed by an attacker, can also be used by the defender.

Scope

This paper will:

- Define and discuss the major components of a multi-layered defense with special emphasis on security policies and their framework.
- Define deception and discuss how it is used by the attacker, how it can be used by the defender, deception tools used in a defensive strategy, and it's role in a multi-layered defense.

Discussion

A multi-layered defense should include the following components: security policies, defense against social engineering, technology, implementation/operation, auditing, and finally deception.

Security Policies: A security policy is the culmination of the security philosophy, strategy, policies, and practices of the company. It is a document that explains the organizations' approach to ensuring the availability, confidentiality, and integrity of its' information. It also defines the classification structure, what needs to be done, how it is to be done, and by whom. If we examine the security policy framework more closely, we see that it entails the following:

1. The organizations' approach to security
2. A classification system
3. Defined levels of responsibility and accountability
4. Identification of the areas that need to be addressed (identifying the threat)
5. The creation of issue-specific and system-specific documents to address these areas previously identified. (examples of issue-specific topics: physical security, internet usage, authentication, auditing/review, employee security

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

awareness, etc...). According to the article Introduction to Security Policies, Part 3: Structuring Security Policies by Charl van der Walt (http://online/securityfocus.com/infocus/1487), each of the issue-specific documents should include the following:

a. Scope
b. Validity
c. Ownership
d. Responsibilities
e. Supporting documentation
f. Position statement
g. Review
h. Compliance

By examining this framework, it becomes evident that security policies provide a standard by which all of the other components within a multi-layered defensive strategy, can be defined and measured.

Social Engineering: Social engineering and reverse social engineering refers to the use of psychological ploys or deception on legitimate users, to attain information that will aid in the compromise of the system or network. These types of attacks are effective for two reasons;

1. Most people want to be helpful and are trusting.
2. Most people have not been educated to recognize this type of attack.

We experienced this while gathering network information from a company that we recently acquired. I asked one of my team members to connect our new branch office to the corporate vpn. In doing so, he needed to gather network information from them. In one or two phone calls, he had everything he needed, with the exception of the employee's credit card numbers and expiry dates. In the initial phone conversation, after stating his name, department, and company from which he was calling from, he inadvertently asked to speak with an employee that did not work there. There was no challenge of his credentials or questions raised; they simply responded, "Oh you must mean ....., we'll put you right through". This is no surprise. We are not naturally suspicious of people, this is learned behavior. How can we prevent or minimize the effects of a social engineering attack? Educate the user. Educating the user to recognize this kind of attack pattern must be included in any defensive strategy.

Technology: We rely on technology every day to keep us secure from malicious users, whether internal or external. In fact, we rely so heavily on technology that we sometimes forget about the other aspects such as employee education/training, mentioned earlier. Without doubt, technology is crucial to any defensive strategy. We would not, knowingly, connect our internal networks to the internet without some sort of perimeter defense, such as a firewall. However, even a firewall can not be relied upon as a sole means of protection. We need to layer technology in order to provide maximum coverage and security of our information. The three primary layers of technology are the perimeter, network, and hosts. This means, that along with a firewall, we will use a network based IDS, such as snort, to log and analyze the traffic being passed through the

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

network. We might also do a phone scan with Phone Sweep to verify if there are modems on auto answer that may circumvent our firewall. We will use host based IDS such as Tripwire or Aide to ensure host integrity. TCP wrappers and Port Sentry will also be employed on the host to deny unauthorized access. Technologies such as encryption, anti-virus, system auditing and logging, backups, honeypots, etc... will round out our layered defense and provide overlap if a compromise should occur in another layer.

Implementation/Operation: Once the security framework has been designed, it needs to be implemented, maintained, and operated. A strong security framework in theory, might not live up to expectations in practice. Two months ago, our network was audited by a security company, and although they were no able to find any exploitable vulnerabilities, they did find a potential for one. One of our web servers was potentially vulnerable to a buffer overflow attack that would give the attacker root access. We were warned that changes to the directory rights would have to be made with the greatest of care. One mistake would open us up to this vulnerability. Misconfiguration during implementation, or human errors made during the maintenance/operation, may open up holes that can be exploited. Written procedures and checklists can help reduce these types of errors from occurring, but what is required is properly trained and educated security staff. These are the people in the trenches who are doing the work on a daily basis. Time and money must be spent to ensure that they not only know what to do, but also, know how to do it.

Auditing: What is referred to here is not system auditing and logging, such as logging the date, time, and location of an invalid login attempt on a root account. This was addressed under the technology section. Rather, it refers to a security audit performed by a qualified external source. Even a seasoned security veteran can benefit from an outsider's perspective. Self-audits are important. As a security professional, you will be running hacker tools against your network [with permission, is implied], but this should be coupled with a quarterly or bi-yearly external security audit. As a principle, a security audit should not be performed by the one who designed the security architecture. If there was an oversight in the security design, the designer will, most likely, overlook it in the audit as well. External audits will provide a means of verifying that your multi-layered defense is, in fact, functioning as it is supposed to.

Deception: This section will attempt to define deception and discuss how it is used by the attacker, how it can be used by the defender, deception tools used in a defensive strategy, and it's role in a multi-layered defense According to the Meriam-Websters dictionary online [http://www.m-w.com/home.htm] the definition of deceive is: to ensnare, to cause to accept as true or valid what is false or invalid, to give false impression. The definition of snare is: something by which one is entangled, involved in difficulties, or impeded; something deceptively attractive. With this in mind, lets examine what the goal of deception is in an information warfare model. The goal of deception in this model is the concealment of activity, identity, or information. For instance, a port scan in stealth mode is meant to conceal the activity from being detected, ip spoofing the real ip address which could identify the attacker, or a honeypot which

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

diverts attention away from the production system information. Whatever the means, the goal is concealment; and this is accomplished through affecting what the target can observe. By affecting what the target sees (or doesn't see in the case of a port scan in stealth mode), you can attract attention to or divert attention from the activity, identity, or information you wish to conceal. If an attacker's reconnaissance probe goes undetected by the system administrator's methods of intrusion detection, then the chances of a successful compromise increase. By not arousing the defender suspicions to a possible attack, the perpetrator has more time and information to stage an effective attack tailored to your exploitable vulnerabilities. The old saying "What you don't see won't hurt you" doesn't apply here. Conversely, if you can convince a hacker that your honeypot is a valuable target, then you not only divert attention away from your critical systems and information, but you consume the resources that he has on a fruitless endeavor. The time and information advantage previously afforded the perpetrator, is now on the side of the system administrator. He now has the time and information to evaluate the attack and ensure that the production systems are not susceptible to the particular exploit, and thus remain concealed.

How is deception used by the enemy? Deception is the main staple of the intruder. Most tools and techniques rely heavily upon it as a means to an end, which in this case, is the successful exploitation of a vulnerability. By examining a few examples of the deceptive techniques employed by the enemy, we may gain some useful insight that can be leverage by our system administrator.

Social engineering attacks count on the fact that people are trusting and want to be helpful, and therefore can be deceived. If properly staged, the perpetrator can glean all kinds of useful information to further his intelligence efforts. Legitimate users are more than willing to give out critical information if they believe it will benefit the company in someway or another. Usernames and passwords, system information such as ip addresses, remote access points, etc... , all can be retrieved by the attacker under the proper guise. Some common ploys are to call the IT helpdesk, posing as an executive, claiming to have forgotten a password, and requesting that it be reset; or appearing as an IT worker who needs a user's login name and password in an effort to solve some system anomaly. Whatever the ploy, it is usually cloaked in urgency, and steeped in deception. Reverse social engineering is even more subtle, it has the legitimate user asking the attacker for help (to read more on this type of attack see Rick Nelson's Methods of Hacking: Social Engineering at http://www.isr.umd.edu/gemstone/infsec/vers2/papers/socaileng.html).

Trojan programs and viruses, historically, have depended on the user to execute them. So the creators use deceptive tactics and packaging to help facilitate their propagation. Electronic mail attachments entitled "I Love You" or "Anna Kornikova" entice the user into executing them. His curiosity is played upon. The receiver would think twice about opening these attachments if they were appropriately named "Nasty virus" or "I Hate You". Now, once executed, these types of viruses often go through a user's e-mail address book and e-mail themselves out. This enhances the deception; the user now sees a friend or trusted colleague's name on the e-mail. Immediately, the reflex

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

to believe what the computer is telling them (that this attachment is, in fact, sent from a friend/colleague) kicks in. Due to the proliferation of these types of viruses and the exposure to this type of deception, individuals are beginning to recognize some of the patterns. This simply means that the perpetrator must become more creative in their disguises.

Port scanning in stealth mode attempts to fly under the radar of detection, while gathering intelligence on possible exploitable vulnerabilities. The packets that the scanning tools generate are crafted in such a way as to go unnoticed by firewall logging. For example, Nmap uses TCP FIN , Xmas tree, and NULL scan modes to surreptitiously scan for listening ports. Other options within Nmap allow the attacker to send decoy packets so that it appears to the target that he is being scanned by multiple hosts. This is an attempt to overwhelm the target with bogus information so that discovery of the source is not obvious. Hping takes a more clandestine approach in that it uses idle machines on the internet as the source of the scan. It then monitors these idle machines to see what type of responses they receive. In so doing, the intruder can do a port scan against the target's systems or network while remaining anonymous to the target. If the target happens to be monitoring for port scans, then, only the host/ip addresses of the idle machines that hping used, will show up in the logs. The real source of the scan will remain concealed. Although I have not scratched the surface of tools and techniques used by the hacker, it will suffice for the purposes of this paper to expose some basic principles of deception that may be explored in a defensive strategy.

How can the system administrator employ such deceptive tactics in the defense of his network? At first glance, all of the aforementioned deceptive tactics were directed towards offense, but under closer inspection, we will find that many of these forms of deception are universally applicable. Although the tactics may be similar, the tools and techniques are not. Enemy tools are meant to be intrusive, they are designed to be clandestine, to reveal and exploit the target's vulnerabilities. “Search and destroy” (among others) is characteristic of the attackers strategy, but should not be so of the defenders. The moral and legal issues with adopting such a policy would be overwhelming. A defensive strategy that uses deceptive tactics is listed below:
(This is by no means an exhaustive list)

Use of deception to:

1. Deter
2. Learn
3. Conceal
    - Impede/Confuse/Overload
    - Misinform
4. Ensnare

Deception as a deterrent: If the enemy thinks that you are too difficult a target he will look elsewhere. For instance running the deceptive defense notifier on port 365 may be enough to discourage someone from attempting to compromise your environment, even though the Deception Toolkit is not installed. You may not deter all of the attempts but you will deter some.

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

Deception to Learn: This is really reverse reconnaissance because you are luring the hacker into an environment that is quarantined and monitored. The purpose of this is to understand the nature of of the intrusion, how it was staged, why it was successful, what tools were used, whether it is was a known exploit or a new one, what the compromised system will be used for, etc... . Unlike the reconnaissance efforts of the enemy, this type of intelligence gathering is a much more passive method but yields greater results. What is interesting to note, is that it is based on the same principal that is used in a reverse social engineering attack. In a reverse social engineering attack, the perpetrator plants a bug or anomaly into the system software. The error message, that was planted, refers the user to the perpetrator as a resource. The target will tend to trust what the computer tells him, in this case the system error message. In the same way, the hacker, who becomes the target once he is lured into this environment designed for counter intelligence, is also susceptible. As long as the environment looks and feels normal, he will tend to trust what the computer tells him. He has no reason to doubt it. The hacker may be a little savvier, but as long as the interaction is within the reasonable limits of expectation and experience, he will fall prey to the same type of deception that he employs to deceive others. This should be no surprise; we as humans, base our judgements on experience.

Deception to Conceal: Deception to conceal is broken down into two parts: to impede/confuse/overload and to conceal through misinformation.

Impede/Confuse/Overload: This is a common tactic exploited by the enemy. In the previous discussion, we examined Nmap's ability to use decoy addresses when doing a port scan. By flooding the target system with bogus packets, it is hoped that the identity of the source will go unnoticed. In fact, if enough decoy packets are sent, the real source address may not be logged by the target's firewall or intrusion detection system. In any case, it definitely impedes the process of finding the true source if it was logged. In another form, a system or process is overloaded by syn packets from bogus addresses; the result is a of denial of service. These methods of deception are meant to consume resources (whether that be time, money, processing power, ability to respond, manpower, etc...) and can therefore be exploited by the system administrator as well. Decoy systems can be setup in a network to look and respond like their production counterparts. One physical machine can be made to look like hundreds of production systems and can be designed to engage the perpetrator so as to waste his resources. The added benefit is that it not only impedes the attackers progress towards your critical systems, which gives the defender time to better protect them, but also allows you to monitor and gather intelligence about the attack. A network loaded with decoys can become confusing to the enemy. Are they tampering with a production system or a decoy? This is a form of information overload, and is a good defensive strategy.

Conceal through misinformation: Sometimes the best place to hide something is in plain view. If you can convince your enemy that the system/information that is valuable has no value whatsoever, then there is no need to hide it. Planting incorrect information which will lead the attacker to incorrect conclusions can be effective. The danger is if the perpetrator is not fooled. Steganography, for example, may be passing critical information which is not viewed as such by a hacker. The value of the data is

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

diminished in the eyes of the enemy by concealing it in a picture. If by chance the ruse is discovered, he will decode it. All the information is in his hands and has been all along; he just didn't know it.

Deception to Ensnare: From the intelligence gathering process, you try to trace the attacker back to the source with the intention to prosecute him. This is not only difficult but requires an understanding of forensics, so as not to damage evidence that could be later used in court.

What are some of the deception tools available to the defender? Honeypots and honeynets are the tools for the system administrator. Honeypots are systems that are designed to be probed, attacked, and compromised. They are decoy systems used to gather information on the attacker. Some examples found at Lance Spitzner's site are BackOfficer Friendly, Specter, and Deception toolkit. These honeypots range from low to medium interaction, which means they have limited functionality for the hacker to interact with. Honeynets are simply high interaction honeypots, they are real systems that have been setup to capture information on the attacker (Mantrap is a commercial honeynet product). The question, which to deploy in the network, depends on what the goal is. If the goal is deception to learn, then the honeynet or mantrap solutions might be more appropriate. If the goal is deception to deter or conceal, then the other solutions might be a wiser choice. They offer less interaction, which generally means, less opportunity for the enemy to compromise the honeypot itself. This, and more information can be found at Lance Spitzners' site http://www.enteract.com/~lspitz/honeypots.html.

Deception's role in a defense in-depth strategy: As previously stated, security policies are the foundation on which any defense in-depth strategy is based. Other components should include, personnel, technology, implementation/operation, auditing, and deception. We have defined deception, discussed it's goal within an information warfare model, how it is used by the attacker, how it can be used by the defender, and tools available. Now we will examine its role in a multi-layered defensive strategy. The theory behind multi-layered defense is straightforward. If the tools or techniques fail at one layer, the safeguards implemented at the other layers will compensate to prevent system compromise. Deception, like the other components, can be utilized to enhance or supplement any network/system security. For example, a target system running NT, can appear to a remote OS identification probe as a Unix machine. This means that even though it may have an exploitable vulnerability that has not been patched, the hacker trying to exploit it, will, most likely, fail; of course this depends on how well the deception is done. In this case, an exploitable hole in the NT service is covered by the layer of deception (hopefully, long enough for the system administrator to properly patch it). You may be able to stave off unwanted attention by appearing to the enemy as a difficult target. If the perpetrator decides to look elsewhere for an easier target, then you have avoided an attack altogether. This is worth its weight in gold. A considerable benefit that deception adds to your layered defense is in it's use to conceal. Populating your network with devices, such as honeypots, has a multifaceted effect which will aid in the concealment of production systems. If the enemy is in the reconnaissance phase and

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

is scanning for vulnerabilities, then his efforts may be impeded by information overload (responses from the bogus machines all showing potential exploitable vulnerabilities). He may expose some of the honeypots, and abort, or be forced to move with caution. Either way, time and resources begin to sway in favor of the defender. If he decides to proceed, he must take extra care to ensure he is not occupying himself with a decoy. If he is unaware of the honeypots, then odds are, assuming the ratio of decoys to productions systems is in favor of the decoys, he will be fooled. By engaging it, he will consume his resources and most likely set off an alarm that will notify the administrator that an attempted intrusion is occurring. The use of deceptive tactics can, potentially, add a whole new dimension to your network security and should be considered a necessary component to any defense in-depth strategy.

Now that we have discussed the potential benefits of using deception for defense, what are the downfalls? Using deception as a deterrent, is a win-win situation. If you appear to be a difficult target then you will eliminate the hackers who are looking for easier targets. Some forms of misinformation are also safe and effective, for example our firewall makes our NT boxes appear to be machines running AIX Unix, when probed with Nmaps remote OS identification tool. This is good, any way you look at it. Where we begin to see a potential hazard is when we start discussing honeypots and honeynets. Honeypots are meant to be targets; they are designed to be high profile, which means that the honeypot software itself has the potential of being broken. Although this is more likely on a honeynet, because it is a high interaction unit, the danger is still there. If a honeynet is compromised then:

1. The intruder knows you are operating honeynets on your network and will be cautious to avoid them.
2. The compromised system can be utilized to stage attacks on internal(if the honeynet is mixed in with other production machines) or external targets (which could end up in liability case against you or your company)

Albeit, there are some negatives when using deception within a defensive strategy, the overall benefits gained, should, more than compensate. (You should consult with legal counsel before monitoring and logging the activity of your honeypots)

Conclusion

The foundation of any defense in-depth planning must begin with security policies. Security policies provide the framework by answering questions like; What is the organization's approach to security? What classification system will be used? Who is responsible/accountable for what? What areas need to be addressed by security measures? etc... . From this framework, a defense in-depth strategy can be designed. It is clear that networks will continue to evolve, and that the complexities involved in securing them will increase as well. It is also clear that a linear approach to security will not offer the protection that is required in such a layered network. A multi-dimensional or layered approach is required. This paper has attempted to provide a defensive architecture that includes deception as a component. The potential benefits of using

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

deceptive tactics are undeniable, but it remains up to the company policy makers to determine the extent to which these tactics can or will be employed.

Resources

Walt, Charl van der. "Introduction to Security Policies, Part One: An Overview of Policies." 27 August 2001.
URL: http://online.securtiyfocus.com/infocus/1193 (20 March 2002)

Walt, Charl van der. "Introduction to Security Policies, Part Two: Creating a Supportive Environment." 24 September 2001.
URL: http://online.securtiyfocus.com/infocus/1473 (20 March 2002)

Walt, Charl van der. "Introduction to Security Policies, Part Three: Structuring Security Policies." 9 October 2001.
URL: http://online.securtiyfocus.com/infocus/1487 (20 March 2002)

Walt, Charl van der. "Introduction to Security Policies, Part Four: A Sample Policy." 22 October 2001.
URL: http://online.securtiyfocus.com/infocus/1497 (20 March 2002)

Palumbo, John. "Social Engineering: What is it, why is so little said about it and what can be done?" 26 July 2000.
URL: http://rr.sans.org/social/social.php (20 March 2002)

Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics." 18 December 2001.
URL: http://online.securityfocus.com/infocus/1527 (20 March 2002)

Nelson, Rick. "Methods of Hacking: Social Engineering."
URL: http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html (20 March 2002)

VanMeter, Charlene. "Defense In Depth: A primer." 19 February 2001.
URL: http://rr.sans.org/start/primer.php (20 March 2002)

Cohen, Fred. Lambert, Dave. Preston, Charles. Berry, Nina. Stewart, Corbin. Thomas, Eric. "2001: A Framework for Deception." 13 July 2001.
URL: http://all.net/journal/deception/Framework/Framework.html (20 March 2002)

Cohen, Fred. "A Mathematical Structure of Simple Defensive Network Deceptions." Copyright © 1999.
URL: http://all.net/journal/deception/mathdeception/mathdeception.html (20 March 2002)

Wilson, Michael. "Defense-In-Depth: Design Notes." Copyright © 1997.
URL: http://www.7pillars.com/papers/didfinal.htm (20 March 2002)

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

Spitzner, Lance. Roesch, Marty. Dittrich, David. “Honeypots – Definitions and Value of Honeypots.” 8 March 2002.
URL: http://www.enteract.com/~lspitz/honeypots.html (20 March 2002)

Fraser, B. “Site Security Handbook .” RFC 2196. September 1997.
URL: http://www.ietf.org/rfc/rfc2196.txt?number=2196 (20 March 2002)

© SANS Institute 2002, Author retains full rights.

Last Updated: February 9th, 2016

Upcoming SANS Training

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

SANS Northern Virginia - McLean 2016	**McLean, VAUS**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS Munich Winter 2016	**Munich, DE**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
ICS Security Summit & Training - Orlando	**Orlando, FLUS**	**Feb 16, 2016 - Feb 23, 2016**	**Live Event**
SANS Secure India 2016	**Bangalore, IN**	**Feb 22, 2016 - Mar 05, 2016**	**Live Event**
SANS Southern California - Anaheim 2016	**Anaheim, CAUS**	**Feb 22, 2016 - Feb 27, 2016**	**Live Event**
RSA Conference 2016	**San Francisco, CAUS**	**Feb 28, 2016 - Feb 29, 2016**	**Live Event**
SANS Philadelphia 2016	**Philadelphia, PAUS**	**Feb 29, 2016 - Mar 05, 2016**	**Live Event**
SANS London Spring 2016	**London, GB**	**Feb 29, 2016 - Mar 05, 2016**	**Live Event**
SANS Abu Dhabi 2016	**Abu Dhabi, AE**	**Mar 05, 2016 - Mar 10, 2016**	**Live Event**
SANS 2016	**Orlando, FLUS**	**Mar 12, 2016 - Mar 21, 2016**	**Live Event**
ICS410 Dubai 2016	**Dubai, AE**	**Mar 13, 2016 - Mar 17, 2016**	**Live Event**
SANS Secure Singapore 2016	**Singapore, SG**	**Mar 28, 2016 - Apr 09, 2016**	**Live Event**
SANS Atlanta 2016	**Atlanta, GAUS**	**Apr 04, 2016 - Apr 09, 2016**	**Live Event**
SANS Northern Virginia - Reston 2016	**Reston, VAUS**	**Apr 04, 2016 - Apr 09, 2016**	**Live Event**
SANS Secure Europe 2016	**Amsterdam, NL**	**Apr 04, 2016 - Apr 16, 2016**	**Live Event**
Threat Hunting and Incident Response Summit	**New Orleans, LAUS**	**Apr 12, 2016 - Apr 19, 2016**	**Live Event**
SANS Pen Test Austin	**Austin, TXUS**	**Apr 18, 2016 - Apr 23, 2016**	**Live Event**
SANS Secure Canberra 2016	**Canberra, AU**	**Apr 18, 2016 - Apr 23, 2016**	**Live Event**
ICS Amsterdam 2016	**Amsterdam, NL**	**Apr 18, 2016 - Apr 23, 2016**	**Live Event**
SANS Copenhagen 2016	**Copenhagen, DK**	**Apr 25, 2016 - Apr 30, 2016**	**Live Event**
SANS Security West 2016	**San Diego, CAUS**	**Apr 29, 2016 - May 06, 2016**	**Live Event**
SANS Secure Japan 2016	**OnlineJP**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**