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.

Social Engineering: A Means To Violate A Computer System

The purpose of this paper is to act as a guide on the subject of Social Engineering and to explain how it might be used as a means to violate a computer system(s) and/or compromise data and the counter-measures that can be implemented to protect against such an attacks.

Copyright SANS Institute
Author Retains Full Rights

AD

SOCIAL ENGINEERING

A MEANS TO VIOLATE A COMPUTER SYSTEM

By Malcolm Allen (updated June 2006)

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Contents

SOCIAL ENGINEERING *1*

CONTENTS **2**

FIGURES **2**

INTRODUCTION **3**

DEFINITION(S) OF SOCIAL ENGINEERING **4**

THE CYCLE **5**

HUMAN BEHAVIOR **6**

WHAT MOTIVATES AN INDIVIDUAL TO PERFORM A SOCIAL ENGINEERING ATTACK? WHAT TECHNIQUES MIGHT THEY EMPLOY? ARE THERE ANY COMMON TRAITS TO WATCH OUT FOR? THESE QUESTIONS ARE ANSWERED IN THE FOLLOWING SECTIONS. **6**

- MOTIVATION 6
- TECHNIQUES 6
- COMMON TRAITS 8

COUNTER-MEASURES **9**

- CONTROLS 9
- MAINTAINING PREPAREDNESS 10

..... **10**

********** **10**

SUMMARY **10**

GLOSSARY **11**

REFERENCES **12**

Figures

FIGURE 1: THE CYCLE **5**

Preface

This paper covers the security aspects of social engineering. If you'd like to learn more about social engineering and other hacker techniques, we recommend taking the SANS SEC504 Hacker Techniques, Exploits and Incident Handling course, available both online and via live training events.

Introduction

'Social Engineering' is a threat, often overlooked but regularly exploited; to take advantage of what has long been considered the 'weakest link' in the security chain of an organization -- the 'human factor'. The following real-life story is a classic illustration of this:

> "In 1994, a French hacker named Anthony Zboralski called the FBI office in Washington, pretending to be an FBI representative working at the U.S. embassy in Paris. He persuaded the person at the other end of the phone to explain how to

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

connect to the FBI's phone conferencing system. Then he ran up a $250,000 phone bill in seven months."

Bruce Schneier. "Secret and Lies".

As a security professional in today's ever-changing world, it is important to be familiar with Social Engineering techniques and the counter-measures available to reduce the likelihood of success. By having this knowledge, one can ensure appropriate (preventative, detective and corrective) measures are implemented to protect the staff and assets of an organization.

The purpose of this paper is to act as a guide on the subject of Social Engineering and to explain how it might be used as a means to violate a computer system(s) and/or compromise data. Topics touched on include:

- Definition(s) of social engineering
- The cycle of a social engineering attack
- Human behavior (from both sides of the fence)
- Counter-measures

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Definition(s) of Social Engineering

What is 'Social Engineering'? Social Engineering is probably most succinctly described by Harl in 'People Hacking':

> *"…the art and science of getting people to comply with your wishes."*

Other authors have provided the following definitions:

> *"Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick a person into revealing sensitive information or getting them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. It is generally agreed upon that "users are the weak link" in security and this principle is what makes social engineering possible."*
>
> Unknown Author, "Social Engineering", Wikipedia

> *"Social Engineering - A euphemism for non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems."*
>
> Unknown Author, http://www.sans.org/resources/glossary.php#s

> *"A social engineer is a hacker who uses brains instead of computer brawn. Hackers call data centers and pretend to be customers who have lost their password or show up at a site and simply wait for someone to hold a door open for them. Other forms of social engineering are not so obvious. Hackers have been known to create phoney web sites, sweepstakes or questionnaires that ask users to enter a password."*
>
> Karen J Bannan, Internet World, Jan 1, 2001

> *"In a system, there is hardware, software and wetware, wetware being the human element of the system. With million pound security systems and state of the art security technology, the first two systems may be impenetrable, but with enough patience and knowledge, a social engineer can use weaknesses in the wetware to trick an unsuspecting target into revealing sensitive information. Social engineering is a use of psychological knowledge to trick a target into trusting the engineer, and ultimately revealing information."*
>
> SirRoss, "A guide to Social Engineering", Volume 1

> *"Term used among crackers and samurai for cracking techniques that rely on weaknesses in the wetware rather than software. The aim is to trick people into revealing passwords or other information that compromises a target systems security. Classic scams include phoning up a mark that has the required information and posing as a field service tech or an employee with an urgent access problem"*
>
> Unknown Author, "Social Engineering", *The Jargon Dictionary*

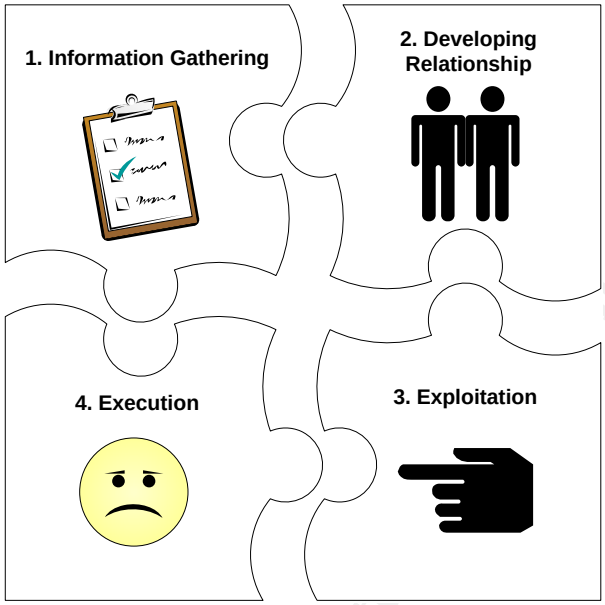
© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

The Cycle

Is there a common pattern associated with a Social Engineering attack? The answer is 'Yes'. As reported by Gartner in a paper titled '*Management Update: How Businesses Can Defend against Social Engineering Attacks*' published on March 16, 2005, any criminal act has a common pattern. Such a pattern is evident with Social Engineering, and it is both recognizable and preventable. For the purpose of this paper, this pattern will be known as 'The Cycle'.

Figure 1 illustrates 'The Cycle', which consists of four phases (Information Gathering, Relationship Development, Exploitation and Execution). Each Social Engineering attack is unique, with the possibility that it might involve multiple phases/cycles and/or may even incorporate the use of other more traditional attack techniques to achieve the desired end result.

Figure 1: The Cycle



1. **Information Gathering:** a variety of techniques can be used by an aggressor to gather information about the target(s). Once gathered, this information can then be used to build a relationship with either the target or someone important to the success of the attack. Information that might be gathered includes, but is not limited to:
    - a phone list;
    - birth dates;
    - an organization's organizational chart.

2. **Developing Relationship:** an aggressor may freely exploit the willingness of a target to be trusting in order to develop rapport with them. While developing this relationship, the aggressor will position himself into a position of trust which he will then exploit.
3. **Exploitation:** the target may then be manipulated by the 'trusted' aggressor to reveal information (e.g. passwords) or perform an action (e.g. creating an account or reversing telephone charges) that would not normally occur. This action could be the end of the attack or the beginning of the next stage.
4. **Execution:** once the target has completed the task requested by the aggressor, the cycle is complete.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Human Behavior

What motivates an individual to perform a Social Engineering attack? What techniques might they employ? Are there any common traits to watch out for? These questions are answered in the following sections.

Motivation

What motivates an individual to carry out a Social Engineering attack? A variety of motivations exist which include, but are not limited to:

- **Financial gain:** for a variety of reasons, an individual might become transfixed on monetary gains. For example, he may believe he deserves more money than he earns or maybe there is a need to satisfy an out–of-control gambling habit.
- **Self-interest:** an individual might, for example, want to access and/or modify information that is associated with a family member, friend or even a neighbor.
- **Revenge:** for reasons only truly known by an individual, he might look to target a friend, colleague, organization or even a total stranger to satisfy the emotional desire for vengeance.
- **External pressure:** an individual may be receiving pressure from friends, family or organized crime syndicates for reasons such as financial gain, self-interest and/or revenge.

Techniques

What techniques might be employed? The techniques that could be employed largely rely on the strength, skill and ability of the individual employing them.

As illustrated in Figure 1, the first phase of an attack will probably involve gathering information about the target. Examples of information-gathering techniques that could be used include:

- **Shoulder surfing:** looking over the shoulder of an individual as he types in his access code and password/PIN on a keypad for the purpose of committing this to memory so it can be reproduced.
- **Checking the rubbish (commonly referred to as 'Dumpster Diving'):** searching through rubbish thrown away to obtain potentially useful information that should have been disposed of more securely (e.g. shredding).
- **Mail-outs:** information is gathered about an individual/organization by enticing him/its staff to participate in a survey that offers enticements, such as prizes for completing the survey.
- **Forensic analysis:** obtaining old computer equipment such as hard-drives, memory sticks, DVD/CDs, floppy disks and attempting to extract information that might be of use about an individual/organization.

Upon the completion of this phase -- which is most likely to be the longest of the attack from the aggressor's perspective –- an aggressor may use one of a number of techniques to achieve his end objective. Each technique used can be grouped into one of two categories. The first category is 'human-based' and relies on interpersonal relationships, while the second is 'computer-based' and relies on technology.

No matter which technique is used, an individual is likely to favor simplicity to ensure success. Common techniques that might be used include the following:

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

- **Direct approach:** an aggressor may directly ask a target individual to complete a task (e.g. a phone call to a receptionist asking them for their username and password). While this is the easiest and the most straightforward approach, it will most likely be unsuccessful, since any security-conscious individual will be mindful of providing such information.
- **Important user:** by pretending to be a senior manager of an organization with an important deadline, the aggressor could pressure the Helpdesk operator into disclosing useful information, such as:
    - the type of remote access software used;
    - how to configure it;
    - the telephone numbers to the remote access server to dial;
    - the appropriate credentials to log in to the server.

  Upon obtaining this information, the aggressor could then set up remote access to the organization's network. The aggressor could then call back hours later to explain that he had forgotten his account password and request that it be reset.
- **Helpless user:** an aggressor may pretend to be a user who requires assistance to gain access to the organization's systems. This is a simple process for an aggressor to carry out, particularly if he has been unable to obtain/research enough information about the organization. For example, the aggressor would call a secretary within the organization pretending to be a new temp who is having trouble accessing the organization's system. By not wishing to offend the person or appear incompetent, the secretary may be inclined to help out by supplying the username and password of an active account.
- **Technical support personnel:** by pretending to belong to an organization's technical support team, an aggressor could extract useful information from an unsuspecting user. For example, the aggressor may pretend to be a system administrator who is trying to help with a system problem and requires the user's username and password to resolve the problem.
- **Reverse Social Engineering (RSE):** a legitimate user is enticed to ask the aggressor questions to obtain information. With this approach, the aggressor is perceived as being of higher seniority than the legitimate user who is actually the target.

  A typical RSE attack involves three parts:
    - ***Sabotage:*** after gaining simple access, the aggressor either corrupts the workstation or gives it an appearance of being corrupted. The user of the system discovers the problem and tries to seek help.
    - ***Marketing:*** in order to ensure the user calls the aggressor, the aggressor must advertise. The aggressor can do this by either leaving his business cards around the target's office and/or by placing his contact number on the error message itself.
    - ***Support:*** finally, the aggressor would assist with the problem, ensuring that the user remains unsuspicious while the aggressor obtains the required information.
- **E-mail:** the use of a topical subject to trigger an emotion that leads to unwitting participation from the target. There are two common forms. The first involves malicious code, such as that used to create a virus. This code is usually hidden within a file attached to an email. The intention is that an unsuspecting user will click/open the file; for example, 'ILoveYou' virus, 'Anna Kournikova' worm. The second equally effective approach involves scam, chain mail and virus hoaxes. These have been designed to clog mail systems by reporting a non existent

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

virus or competition and requesting the recipient to forward a copy on to all his/her friends and co-workers. As history has shown, this can create a significant snowball effect once started.

- **Website:** a ruse used to get an unwitting user to disclose potentially sensitive data, such as the password he/she uses at work. For example, a website may promote a fictitious competition or promotion, which requires a user to enter in a contact email address and password. The password entered may very well be similar to the password used by the individual at work.
- **Phishing:** uses specially crafted emails to entice recipients to visit a counterfeit website. This website is likely to have been designed, using well-known and trusted brands, to convince the individual to provide financial and/or personal information. The information harvested is then used for fraudulent purposes. In some instances, while visiting a website, malicious code such as Trojan key logging software is installed on the unsuspecting user's computer in an attempt to gain further sensitive information about/from the individual.

Common traits

Are there any common traits to watch out for? Whatever the motivation or technique used, there are certain traits that usually entice the target to comply with the request(s). These traits include:

- The movement of responsibility away from the target, so that the target is not considered solely responsible for his/her actions.
- The perception by the target that, by conforming with the request, the target will get on the 'right side' of somebody who could award them future benefits, more commonly known as "getting in with the boss".
- The target's instinct to act morally in helping someone out, thus avoiding the feeling of guilt.
- Communication on a personal level, resulting in the target voluntarily complying with the request without realizing the pressure being applied.
- The target believes he/she is making a reasoned decision in exchange for a small loss of time and energy.

The likelihood of the target's compliance is further increased if:

- The aggressor is able to avoid conflict by using a consultative approach rather than an aggressive one.
- The aggressor is able to develop and build a relationship through previous dealings. The target will probably comply with a large request having previously complied with smaller one.
- The aggressor is able to appeal to the target's senses, such as sight and sound. By appealing to such senses, the aggressor will be able build a better relationship with the target by appearing 'human' rather than just a voice or email message.
- The aggressor has a quick mind and is able to compromise.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Counter-measures

Is there an effective way to fully protect against Social Engineering an attack? The answer is 'No'. For the simple reason that no matter what controls are implemented, there will always be the possibility of the 'human factor' being influenced by a social, political and/or cultural event.

Nevertheless, as with any threat, there are ways in which to reduce the likelihood of success. This can be achieved by having an appreciation of the threat, and knowledge of both the techniques that could be used and the counter-measures that can be implemented.

Controls

Below is a list of core controls that can be implemented to protect against such an attack. However, when considering which of these controls to implement, it is important to ensure that they --

- do not disrupt normal day to day operations;
- are robust enough to block a variety of malicious actions occurring concurrently;
- can establish the difference between an attack and normal day-to-day activity.

Core controls that can be implemented:

- **Management buy-in:** managers require an understanding of their role to be able to define what requires protection, and why. This understanding should ensure that appropriate protective measures are taken to protect against associated risks.
- **Security policy:** a sound security policy will ensure a clear direction on what is expected of staff within an organization. For example, support teams should only offer assistance for a defined range of activities.
- **Physical security:** a key control that involves restricting physical access to computer facilities and systems for staff, contractors and visitors. For example, in order to remove the possibility of people overstating their authority, the use of access badges indicating an individual's status (e.g. employee, contractor, and visitor) is recommended. In addition, employees should be encouraged to look at the badges.
- **Education/Awareness:** a simple solution that can be used to prevent these types of attacks. For example, a knowledgeable user can be advised that he/she should never give out any information without the appropriate authorization and that he/she should report any suspicious behavior. A good training and awareness program focusing on the type of behavior required will undoubtedly pay for itself. This program might even provide users with a checklist on how to recognize a possible 'Social Engineering' attack.
- **Good security architecture:** smart infrastructure architecture will allow personnel to concentrate on more important duties. For example, by ensuring outbound firewall access controls are configured just as carefully as inbound controls, an administrator will know exactly how the networked environment will respond under certain events. This understanding will ensure that the administrator is able to avoid spending time following up on 'false positives'.
- **Limit data leakage:** reducing the amount of specific data available will ensure that the attack is not an effortless exercise. For example, websites, public databases, Internet registries, and other publicly accessible data sources should only list generic information, such as main

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

organization phone number and job titles instead of employee name(s) [for example, 'site administrator' instead of 'Joe Bloggs'].

- **Incident response strategy:** a documented response strategy will ensure that, if under pressure, a user will know exactly what procedures to follow. For example, if a user receives a request, he/she should verify its authenticity before acting on the instructions he/she has received. If, however, he/she has already acted on the request, then he should alert the administrator. It will then be the responsibility of the administrator to check with the users to ensure no other user has followed the instructions of the request.
- **Security culture:** building an information security culture within an organization starts with making people aware of security issues, providing them with tools to react, and encouraging two-way communication between security personnel, managers and employees. The creation of a security culture should be considered a long-term investment, which requires a constant effort to maintain and grow.

Maintaining Preparedness

Once the controls have been implemented, there are two ways for an organization to maintain a state of ongoing preparedness for such an attack.

The first is to perform regular reviews of the controls that have been implemented. These reviews will ensure that an acceptable standard is maintained on an ongoing basis.

The second and the least common approach used, is to simulate an attack. This type of review depends on the information that can be obtained from the public domain about the organization, as well as the value it could offer, versus the resource-intensive overhead. It should also be noted that many organizations are not comfortable with this type of review.

****

Summary

The skilled application of Social Engineering can be a threat to the security of any organization. As a security professional, it is important to understand the significance of this threat and the ways in which it can be manifested. Only then can appropriate counter-measures be employed and maintained in order to protect an organization on an ongoing basis.

This paper covered the security aspects of social engineering. If you'd like to learn more about social engineering and other hacker techniques, we recommend taking the SANS SEC504 Hacker Techniques, Exploits and Incident Handling course, available both online and via live training events.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Glossary

Access code: a sequence of characters and numbers used by a user when he is attempting to access a computer.

Aggressor: a self-confident individual who attacks a particular target(s).

Architecture: the arrangement of a computer's hardware or system software.

Attack: an offensive move made with the intention to bypass one or more security controls.

Data: raw material of information.

Forensic analysis: use of science and/or technology to investigate and establish facts.

Helpdesk: a service that gives assistance and information to users.

Incident: an event that has an adverse impact on a network or service.

Information: the output of processing and organizing data in a way that adds to the knowledge of the individual receiving it.

Key logging: a piece of software that captures the keystrokes the user enters on a keypad.

Malicious code: software that appears to carry out a useful task, but really provides unauthorized access to system resources.

Password: a sequence of characters and numbers used by a user to access a file, computer or program. Ideally, the password is a secret and is something that nobody could guess.

PIN (Personal Identification Number): a number used to gain access to, for example, a bank account(s).

Target: a person who is the aim of an attack by an aggressor.

Techniques: approach used to reach a specific goal.

Threat: the potential for a security breach due to the existence of a particular set of circumstances.

Trojan: a computer program that appears useful, but has a concealed and potentially malicious function.

Virus: a computer program that cannot run and/or propagate without user intervention. The result of this intervention may result in the consumption of computer resources.

Worm: a computer program that can run and propagate without user intervention. For example, it can copy a complete working version of itself onto other hosts on a network, and may consume computer resources.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

References

Allan, Ant, Noakes-Fry, Kristen, Mogull, Rich. “Business Update: How Businesses Can Defend Against Social Engineering Attacks”. Gartner, March 16, 2005.

Arthurs, Wendy. "A Proactive Defence to Social Engineering", August 2, 2001.
URL: http://www.sans.org/rr/whitepapers/engineering/511.php

Bernz. "The Complete Social Engineering FAQ".
URL: http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt

CERT Advisory CA-1991-04. "Social Engineering", Revised September 18, 1997.
URL: http://www.cert.org/advisories/CA-1991-04.html

Frank, John. “Locking Down Data Security”, Collections and Credit Risk. March 2006, pg 18.

Granger, Sarah. “Social Engineering Fundamentals, Part I : Hacker Tactics”, December 8, 2001
URL: http://www.securityfocus.com/infocus/1527

Goodwin, Bill. “Firms warned they are failing to block Social Engineering attacks”. Computer Weekly, April 4, 2006, pg 16.

Granger, Sarah. “Social Engineering Fundamentals, Part II : Combat Strategies”. January 9, 2002
URL: http://www.securityfocus.com/infocus/1533

Harl. "People Hacking". The Psychology of Social Engineering.

Horowitz, Alan S. "Top 10 security mistakes". Computerworld, July 9, 2001.

Hurley, Hanna. "Fear thyself". Telephony, June 21, 1999.

Lemos, Robert. "Mitnick teaches 'social engineering'", July 12, 2000.
URL:
http://netsecurity.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.zdnet.com%2Fzdnn%2Fstories%2Fnews%2F0%2C4586%2C2604480%2C00.html

Lewkovitz, Daniel. “Social Engineering”. Ruxcon Sydney, 2004.
URL: http://www.ruxcon.org.au/files/2004/14-daniel_lewkovitz.pdf

McDowell, Mindi. “Avoiding Social Engineering and Phishing Attacks”, US-CERT Cyber Security TipST04-014.
URL: http://www.us-cert.gov/cas/tips/ST04-014.html

McKay, Dave. “Social Engineering Fundamentals”, 2005
URL: www.bellua.com/bcs/asia05.archive/ BCSASIA2005-B12-McKay-Social_Engineering.ppt

Palumbo, John. "Social Engineering: What is it, why is so little said about it and what can be done?". July 26, 2000

Scambray, Joel and McClure, Stuart and Kurt, George. "Hacking Exposed - Second Edition".

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Schneier, Bruce. “Basketball Prank”, March 14, 2006
URL: http://www.schneier.com/blog/archives/2006/03/basketball_pran.html

Schneier, Bruce. “Social Engineering a Police Officer”, April 13, 2006
URL: http://www.schneier.com/blog/archives/2006/04/social_engineer_1.html

SirRoss. “A guide to Social Engineering, Volume 1”.
URL: http://www.astalavista.com/index.php?section=directory&cmd=detail&id=3487

SirRoss. “A guide to Social Engineering, Volume 2”.
URL: http://www.astalavista.com/index.php?section=directory&cmd=detail&id=3488

Stevens, George. "Enhancing Defences against Social Engineering". March 26, 2001

Thompson, David. "The social engineering of security". June 11, 2001.
URL: http://www.zdnet.com/enterprise/stories/main/0,10228,2771372,00.html

Tims, Rick. "Social Engineering: Policies and Education a Must". February 16, 2001

Unknown Author. "Crime, Security, and Privacy". University of Memphis.

Unknown Author. " Social Engineering". The Jargon Dictionary

Unknown Author. "Social Engineering". Wikipedia

Unknown Author. http://www.sans.org/resources/glossary.php#s

Wetzel, Rebecca. “Tackling Phishing”, Business Communications Review. February 2005,32, 2; pg46.

Winkler, Ira S. “Case Study of Industrial Espionage through Social Engineering”. National Computer Association.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 22nd, 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**