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.

Understanding and Auditing

Social engineering is an oft-underestimated threat that can be warranted against through education and policies and procedures. While most companies are utilizing training and introducing new policies and procedures to combat social engineering, the only way they can be sure these methods are effective is through auditing specifically for these types of attacks. However, before auditing can take place, it is important to understand the social engineers methods and strategies. It is also important to identify the most c...

Copyright SANS Institute
Author Retains Full Rights

AD

Social Engineering: Understanding and Auditing

By

Chris Jones

GSEC, v1.4b, Option #1
November 4, 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Social Engineering: Understanding and Auditing

Abstract

Social engineering is an oft-underestimated threat that can be warranted against through education and policies and procedures. While most companies are utilizing training and introducing new policies and procedures to combat social engineering, the only way they can be sure these methods are effective is through auditing specifically for these types of attacks. However, before auditing can take place, it is important to understand the social engineers methods and strategies. It is also important to identify the most common defenses against social engineering.

Once there is a clear understanding of the threat of social engineering and defenses against it, it is possible to begin planning an audit. Then we may explore some simple techniques security personnel may use in emulating these methods for their own audits. By utilizing these methods, it may be possible for security personnel to reduce the risk of a breach through social engineering. They may also develop these techniques into even more complex strategies to further enhance their internal audits.

Introduction

When most corporations prepare their defenses against hackers, they focus on detailing a firewall policy, hardening Internet-facing servers, or possibly securing internal network file transfers. Most companies are unaware that the arsenal of the successful hacker contains many simple tools, such as a telephone or an e-mail client. The hacker's efforts to manipulate the human side of security, through social engineering, are usually a sure sign of an eventual security breach. In fact, most corporations are unaware of such a breach until well after it has occurred.

Although policies and procedures can provide an adequate defense against many types of social engineering, how can we insure that they are as effective in practice as they may appear in theory? Conducting regular security audits can help to find inadequacies in security policy, but most security audits do not specifically cover those areas that are most vulnerable to social engineering attacks. This paper covers background information relating to social engineering, and outlines some suggestions for security personnel on developing an audit specifically for social engineering attacks. It also discusses various techniques that they may employ in their own audits to identify possible breaches in policy and procedures, specifically dealing with the human element of security.

What is Social Engineering?

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

A formal definition of social engineering from the High-Tech Dictionary is "breaking an organization's security by interactions with people; for example, tricking someone into giving out a password."[1] A more informal definition of social engineering from "The Complete Social Engineering FAQ" states: "…social engineering takes advantage of holes in people's common sense."[2] Both of these definitions capture the general idea of social engineering, but it is also important to understand how social engineering relates to hacking in general.

Hacking characteristically involves entry into forbidden systems through technical means. While the typical hacker "takes more advantage of holes in security,"[3] the social engineer manipulates personnel to gain information that would not normally be available, such as passwords, user IDs, or even corporate directories. In effect, social engineering is typically employed by hackers as a means to acquire information that would be extremely difficult to obtain through strictly technical means. Unlike hacking, social engineering taps into the psychology of what people expect from others and their natural tendency to be helpful. Many of the techniques that the social engineer will utilize are based on these simple premises.

Strategies of the Social Engineer

The social engineering attack is divided into two stages: (1) the physical location where the attack is carried out, and (2) the psychological methods used to extract the needed information.[4]
The three major physical settings where this may take place are:

- The Workplace – Impersonating a maintenance worker or a consultant, an attacker could just stroll through the front door. Once inside, the intruder can "shoulder-surf" passwords, gather passwords or sensitive documents left carelessly on employee workstations, or gain access to the corporate network through unguarded network ports. After gathering the necessary information, the attacker may return home to exploit the network at his leisure.[5]

- By Telephone - Social engineering attacks by telephone are the most common type. Help Desks are especially vulnerable to this method of attack. It is also common for the attacker to play tricks with the PBX or the company operator to appear that they are calling from within the company and not from an outside line.[6]

- Online - Online attacks are primarily carried out through e-mail or through online chat software such as Instant Messenger, ICQ or IRC. The goal of the attacker in an on-line attack could be to convince the victim to run malicious programs on their local machine or to fill out a form to obtain passwords or personal information.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

While knowing where an attack may come from is useful, it is also important to understand how the attack will be carried out. Social engineers use a variety of psychological weapons against their victims including:

- Authority – Assertions of authority can be highly effective when attempting to manipulate others.[7]

- Natural Tendency to be Helpful - It is a natural tendency of humans to be inclined to help those who are in need. Unfortunately, the social engineer knows this and uses it to his advantage. By impersonating a deliveryman with many boxes to unload, the social engineer could gain physical access when friendly employees hold the door. A late night call to the Help Desk from a desperate individual attempting to access the corporate network from home could place sensitive information into an attackers hands.[8]

- Liking and Similarity – When conversing with a victim the social engineer may attempt to probe for a personal connection. Because it is a natural tendency for humans to like people who are like themselves, the social engineer may attempt to connect with the individual through hobbies, birthplace, favorite movies or other areas of personal interest. Once this connection has been made, the victim may feel more responsive towards the social engineer and therefore may be more likely to trust them with sensitive information.[9]

- Reciprocation - Typical social interaction dictates that if someone gives us something then it is only right for us to return the favor. When social engineers use this against a potential victim, it is called "reverse social engineering." For example, the social engineer may cause a small network outage, then contact the potential victim and claim that the network will be unavailable for quite some time. The typical response to this is one of dismay and the social engineer responds by "repairing" the outage as a favor to the victim. The social engineer will then proceed to request a favor from the victim, which will usually gain the information that was desired to begin with.[10]

- Commitment and Consistency - Untrustworthiness is an undesirable trait in our society and any actions that may bring about this trait are disagreeable.[11] The social engineer may ask "favors" of his victims and insinuate that if they are not quick to comply; they will be looked down upon or reprimanded. This technique is also commonly coupled with an assertion of authority to provide even more intimidation.

- Low Involvement - Low involvement refers to employees who may have very little interest in what the social engineer is trying to ask them to do. Security guards, members of the cleaning crew or receptionists may be considered low involvement targets. Due to their detachment from the

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

task they are being asked to accomplish, these targets may be easily overwhelmed by seemingly logical reasons for the request, the urgency of the request, or the assertion of authority.[12]

Defenses Against Social Engineering

One point that separates the typical technical hacker attack from the social engineering attack is the level of employees who are involved. In the usual technical attack, those involved may include any combination of employees from the IT department to the Information Security department. These are targets that may have a high level of technical knowledge, security awareness and the understanding that the systems under their care may come under attack. However, the typical social engineering attack may involve anyone, from the front desk receptionist to the late night cleaning crew. These employees may have little to no technical knowledge and they may be less aware of security, particularly when they feel that the information they are working with may not be highly classified or sensitive.

So what is the answer to the problem of defending against social engineering attacks? In "Social Engineering Fundamentals, Part II: Combat Strategies", Granger proposes:

> In order to be successful, organizations must make computer security part of all jobs, regardless of whether the employees use computers (qtd. in Harl). Everyone in the organization needs to understand exactly why it is so crucial for the confidential information to be designated as such; therefore, it benefits organizations to give them a sense of responsibility for the security of the network (qtd. in Stevens).[13]

In essence, this implies that training and education are key in defending against social engineering attacks. In fact, one of the most important defenses against social engineering is to know when you are being exploited. While there is no guaranteed way to completely avoid a social engineering breach, we can mitigate the risk and attempt to minimize the damage if such a breach should occur.[14]

Besides training and education, other useful deterrents include:

- Improved Physical Security - A good start to implementing social engineering defense is to insure that any valuable information stays in your company. Though not very effective against attackers working from the inside, improving physical access security can help thwart outside attackers from just walking in and taking what they want.[15]

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Strong Security Policy – Developing strong controls for sensitive information can go a long way in deterring the social engineer. This goes hand in hand with training and education. Employees must be well trained in order to follow the policy and make it.

- Reprimands for Security Related Infractions - A security policy is worthless if the employees are not aware of its importance This means that upper management must be willing to punish employees who regularly break security policy controls. Coupled with heavy training and education, employees can be made aware of the importance in following policy.[16]

- Detailed Incident Handling Procedures - While knowing when a social engineering attack is taking place is extremely important, it is just as important to know what to do during an attack. Employees should be provided with detailed procedures on how to verify caller identity and on whom to contact if they feel an incident has occurred.[17]

Social Engineering and Auditing

Now that we have explored some of the ideas and tactics behind a typical social engineering attack, we can see that social engineering is an attack against the human factor of security. The actions of humans, unlike firewalls, servers, or Intrusion Detection Systems, are not controlled by a fixed set of policies or rules. Their acts are largely unpredictable and are principally guided by logic and past experiences. By training and teaching security policy, we can better dictate the actions of employees and provide guidelines on how they should act. However, what is the use of implementing strong information controls or in-depth training if they are not taken seriously or possibly even ignored? How can we know that the actions that have been taken to protect the company are adequate? It is because of these very questions that we have security audits.

"The Telecom Glossary 2K" defines a security audit as:

> Of data processing operations, an independent review and examination of system records and activities to (a) determine the adequacy of system controls, (b) ensure compliance with established security policy and operational procedures, (c) detect breaches in security, and (d) recommend any indicated changes in any of the foregoing.[18]

Because social engineering defense is largely based upon the strength of the security policy, it only makes sense that regular security audits be performed to identify weaknesses and to better improve the policy itself. Security auditing also plays a large part in a company wide security awareness program. If employees

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

are made aware that security is as much a part of their job as anyone else's, controls are made even more effective. Through security audits focused on social engineering, employees can be shown that they are as much a target as anyone else in the company.

Pre-Audit: Preparing for the Audit

Before conducting an audit, it is important to spend a considerable amount of time in preparation, especially if your company does not already have an audit program in place. While an in-depth discussion of the specifics of audit preparation is beyond this paper, there are a few points that should be mentioned.

- Define mission and objectives – It is important that your organization define a mission or a statement of purpose for the program. This allows the program to focus itself and to provide accountability for those involved. The purpose of the audit could be to improve on already established controls, test ideas for new policy, or to expose illegal activities, but whatever is chosen must be adhered to.[19]

- Obtain Permission – Before conducting any form of security test, it is important to obtain permission from upper management. As many of these auditing techniques work against company policy and could be construed as unauthorized activity, it is important to insure you have authorization before proceeding.[20] (textbook)

- Notify Employees – It is also important to insure that employees are properly notified before any security auditing takes place. While it may not be necessary to reveal whom you may be testing, it is imperative that the general employee body is aware that security testing will be taking place.[21] (textbook, art of deception)

- Review Current Policies and Procedures – Familiarization with current policies and procedures is necessary to assist in formulating an objective for the audit. It may also be helpful to create a checklist of which controls you will touch upon in the audit, and to divide outcomes into differing levels of severity.

Social Engineering Auditing Techniques

Intelligence Gathering Phase

The social engineer who begins his attack with little or no information is destined for failure. Because of this, it is likely that an extensive information gathering campaign will mark the beginning of the attack. Gathering information about the company, its practices, culture and employees, and identifying potential

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

weaknesses is the goal. Employee lists, internal phone numbers, corporate directories and sensitive security information are prized possessions to the social engineer. Thusly, all employees should treat these documents as sensitive information.[22]

The tools for researching a particular company can be as simple as a web browser.

- Corporate Website – The first place to begin is with the company's own Internet-facing website. Company directories and brochures can provide a wealth of information to the social engineer.[23] If there are any of these items present for anyone to access, this is definitely a potential problem.

- Search Engines – Search engines such as Google™ can reveal a plethora of information on a company. It can be used to find general information about a company, users at the company, and even possibly, who the company's clients are. A couple of useful searches at Google™ are: (mycompany should be replaced with the actual name of your company):

    - "mycompany"[24] – This search will produce a number of articles and information about a company. In fact, if your company is exceptionally large and well known, this search may produce too much information. This search is also useful at Google™ News (http://news.google.com) where news sources about your company can be verified. Browse the articles to insure that no sensitive information is being leaked. If any is found, the poster of the offending material should be contacted.
    - "@mycompany.com"[25] – A search for instances of your company's domain can reveal employee e-mail addresses that have been posted publicly. These will most likely be forum entries from employees and can provide information on what types of information your employees may be revealing on the Web.[26]
    - "*search-string* site:www.mycompany.com"[27] - This search command can help the auditor attempt to find specific information at the company's website. Replacing "search-string" with appropriate expressions can help in insuring the company's public website is free from internal information.

- Newsgroups – Newsgroups can also divulge a wealth of information for the social engineer. Google™ Groups is an excellent resource for searching newsgroup articles from the past 20 years. Using the "Author" field of the "Advanced Groups Search", you can search for "@mycompany" to find all articles written by employees (both past and present) at your company. This is useful to insure an unsuspecting system administrator has not fallen prey to a "friendly" request to share firewall configurations.[28]

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Job Sites - Although searching job sites may not reveal any sensitive information, it can be a perfect indicator of where a company is going and where it may be lacking in personnel. As a potential job seeker could be a social engineer in disguise, searching job sites for openings can assist auditors in selecting targets for the more in-depth social engineering tests.

Physical Entry Phase

While the social engineer will generally attempt to accomplish his mission without ever physically stepping foot on company property, sometimes it is necessary to gain physical access to gather further information. Insuring that an attacker cannot just walk into your facility unchallenged could involve the use of badge readers, security guards, mandatory check-in of all guests, or various other means. There are many common tricks that the social engineer can use to gain physical access to a facility. The security auditor can also use these to test physical security procedures.

- Employee Impersonation – A typical trick of the social engineer is to attempt to blend in as an employee of the company. While this trick can be difficult to pull off for an auditor who may be well known to others at the company, it can be done by employing an employee from another site, an outside colleague (with management approval) or a hired contractor. A social engineer attempting to impersonate an employee will utilize two tricks to make themselves more believable:

    - Dress Code – It is important in order to blend in to adopt the typical dress of the corporate culture. A suit and tie will definitely attract attention in a more casual workplace. While a social engineer may hang around the workplace to gather this information, it should be no problem for the internal auditor to emulate.[29]

    - Fake ID Badge – A fake ID badge can go a long way in proving credibility. These can be easily made with a laminating machine and some digital imaging software. There are also high dollar alternatives that can produce very realistic replicas. It is highly recommended that if the auditor's company uses ID badges to verify identity, he/she should manufacture several fakes of various qualities. Badges with incorrect pictures, misspelled names, made up names, and substandard graphics and logos are all good examples of ways to formulate imperfect badges. This is an excellent way of gauging how closely security personnel and other employees are looking at ID badges.

- Tailgating – After impersonating an employee, the social engineer's next avenue of attack is to gain access to off-limits areas. This may only

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

include sensitive work areas or it may include the facility itself. A typical means of gaining access to these areas is tailgating or following other employees into secure areas without providing any verification of identity. The auditor can easily test this by hanging around secure entrances and attempting to step-in behind employees with legitimate access.

- Masquerade – Impersonating an employee is not the only means of disguise that the social engineer may utilize. Delivery personnel, utility workers or even visitors can be a potential cover for the social engineer.

    - Delivery Personnel – Delivery personnel can easily be impersonated by simply buying a pair of brown coveralls or by purchasing branded clothing from a major delivery service such as UPS or FEDEX. They can be easily be obtained from EBay or another online auction site.[30] One typical technique as a delivery person is to approach a door carrying many heavy boxes and see if anyone is "kind" enough to open the door.[31] Try this at other entrances to the facility such as back and side doors. If an employee makes a confrontation, then attempt to convince them you should be allowed through this door and use the name of an upper manager or someone with authority.

    - Utility Workers – Utility Workers follow the same pattern as the delivery personnel. Obtain a worker's uniform (usually coveralls or jeans with a company branded t-shirt), approach the front desk, and claim you are there to fix the telephone, toilet, etc. It is best to pick a time when the Building Manager is out. Expressing a sense of urgency can also usually help to gain entry.

    - Client or Visitor with Appointment – Knowing what types of businesses your company deals with and then attempting to gain access by masquerading as a representative of one of those businesses is another trick of the social engineer. A good way to test this is to claim that you have an appointment with someone who is on vacation or out for the day. When it is discovered that they are not available, then ask to meet with someone else who may then give you access to the office. Another trick is for the social engineer to ask to wait in a conference room while they are waiting for their supposed appointment. Once inside a conference room, the attacker can attempt to gain access to the corporate network through unprotected wall jacks. As with all social engineering tactics, the more believable and manipulative your story is, the greater the chances are of success.

- After Hours Entry – Attempting to gain access to the site after hours is also a good way to test security involving over-night security personnel

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

who may not be familiar with all employees, and to catch low-involvement personnel such as cleaning crews, unawares. Attempt to gain access here by utilizing the social engineer's methods of coercion. It may also help to use a fake badge as described earlier.

Shoulder Surfing and Eavesdropping

After gaining physical access, there are several options open to the social engineer. He may attempt to find an open network port to gain unprotected access to the company network, he may target a specific individual's machine in order to steal sensitive documents, install Trojan horse software or even shoulder surf passwords from employees. When performing an internal audit, insure that offices of employees who deal with sensitive information have physically locked their doors and their cabinets to prevent unauthorized access. Also, if security policy has divided data into classifications, insure that employees are not leaving sensitive data in unsecured areas.

Attempting to catch employees entering passwords in order to attempt a "shoulder surf" attack can be difficult, so it may be necessary to resort to a bit of trickery. It will be necessary to attempt this on employees that may not be entirely familiar with the auditor. Impersonating a system administrator, attempt to find employees who have not logged into their machine in some time and request they log into their machines for you. Create a plausible reason for this, perhaps you are attempting to insure they will not lose work during a short network outage or that their machine has updated virus definitions. In addition, wearing a fake ID badge may also lend to the appearance of credibility. If they buy this argument, watch carefully as they enter the password and observe if they attempt to conceal their keystrokes. This test is a great way to gauge not only the effectiveness of "shoulder surfing" attacks, but also a measure of how trusting your employees may be toward suspicious people with semi-plausible stories, who are asking them to provide physical access to their machine.

Another common tactic of the social engineer with physical access to a facility is to attempt to gather more information about the company through eavesdropping. While most serious attempts at eavesdropping are carried out through technical means, possibly through bugged devices or hidden microphones, it is still possible for a low-tech attacker to overhear sensitive information just by hanging around company break rooms, smoking areas or even in the lobby. If you suspect that this has occurred at your company, it may be necessary to enlist the services of a Technical Surveillance Counter Measures firm to perform a "bug sweep."

When auditing for less technological means of eavesdropping, simply hang around points where employees gather, and listen. Make note of any extended conversations that involve sensitive material or information that might provide

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

further assistance to an attacker. It may be impossible to completely prevent employees from discussing sensitive information in open areas, but if the results of the audit show this to be a big problem, it may be necessary to change policy to discourage this activity.

Telephone Based Auditing

The telephone is a very important tool for the social engineer. It allows the attacker to remain relatively anonymous and opens up almost every employee to possible exploitation by the attacker. While it may not be possible to define definite guidelines for telephone-based social engineering auditing, a few guidelines can be identified in order to develop a plan.

The first task is to identify the type of information that you want to gain from employees. This information could be passwords, sensitive documents, additional telephone numbers, or any other information that may assist an attacker. It is important to remember that the resolute attacker will very rarely ask for information outright from there first victim, but may use a chain of trust among individuals to slowly extract the required intelligence.

Once the information you will be attempting to obtain has been identified, it is necessary to identify those individuals that will act as “gateways” to that information. The “gateway” personnel will be those who are authorized to provide the information you will be seeking. It may also be necessary to study the individual to gather information on co-workers, direct reports, and superiors. Develop a chain of trust for this particular individual in order to find out which areas to apply advantage. Discovering the victim’s habits, work ethic, and details of their particular position may also provide hints on how to approach them. It may be helpful to utilize a template such as that in Figure 1 to keep track of this information and the calls you make.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Social Engineering Telephone Attack Template

Attack Scenario	
Telephone #	
Person	
Description	
Results	

Figure 1 – An Example of a Social Engineering Telephone Attack Template[32]

After gathering all required intelligence, it is time to actually phone the individual and place the request. It is important to remember a couple of typical techniques when making the request: authority and urgency. Attempt to invoke the fear of authority in the potential victim by name dropping an immediate supervisor and adopting the attitude that this request needed to be fulfilled yesterday. Typical PBX trickery can be emulated simply by using another employee's telephone so that the number that appears on his or her phone does not appear immediately suspicious. If you are going to be masquerading as an outside client, use an outside line to make the ruse more believable.[33]

E-mail Based Auditing

With the prevalence of ever more powerful worms that utilize e-mail to exploit users, it has become more common for users to be faced with trickery in their mailbox. Like a virus or worm, social engineers also utilize e-mail in order to trick unsuspecting victims into running Trojan backdoor software or visiting malicious web sites.

Utilizing the same auditing techniques as those described in "Telephone Based Auditing," we must first identify users who have access to information that we may desire. Then we must attempt to trick them into revealing it via e-mail. It is also useful to employ a template here for the purpose of tracking what e-mails have been sent and to whom. Various methods may be utilized when performing this type of audit, ranging from simply asking for the information, attempting to trick the user into running malicious software, or visiting a malicious website.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Social Engineering E-mail Attack Template

Attack Scenario	
Email	
Pretext	
Description	
Results	

Figure 2 – Example of a Social Engineering E-mail Attack Template[34]

Gathering the requested information is simply a matter of using the same techniques as in the telephone-based attack. Attempt to craft an e-mail message that expresses authority and urgency, and remember that the victim will be more wary of this type of attack due to the less demanding nature of e-mail in general. If you are going to attempt to trick the user into running malicious software or visiting a malicious website, a useful technique is to impersonate the IT department of your organization and request that the user click a link due to some maintenance request (such as a virus update or a new OS patch). Setting up a simple website to record IP addresses and linking that in the e-mail address can pinpoint those employees who may have fallen for the trick. This e-mail may also be sent out as a follow-up to a previous telephone attack. In fact, this was how AOL was hacked in 2000, when malicious hackers targeted help-desk personnel with virus infected e-mail attachments.[35]

Conclusion

The fact that AOL was the victim of a successful social engineering attack drives home the fact that social engineering is a legitimate risk to corporate security. Understanding the tools and methods of the social engineer can give security personnel a better understanding of what they face and can provide new insights on how to combat this threat. Since the largest portion of defense against social engineering lies in a company's policies and procedures, it is important to include audits of these procedures and to direct them towards the human element of security which social engineering targets. The lack of material regarding auditing against social engineering is less than adequate. It is hopeful that others may continue to expand on this material to better assist security personnel responsible for their own audits. In utilizing these techniques, it may someday be possible to mitigate the risk of attacks via social engineering methods.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Endnotes

[1] John Silltow and Michael Hines, "Social Engineering, Part 3," ITAudit, 15 Dec. 2001, 26 Aug. 2003 <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=347>.

[2] Bernz, "The Complete Social Engineering FAQ!" 14 Jan. 1997, 19 Aug. 2003 <http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt>.

[3] Ibid.

[4] Sarah Granger, "Social Engineering Fundamentals, Part I: Hacker Tactics," SecurityFocus, 18 Dec. 2001, 19 Aug. 2003 <http://www.securityfocus.com/infocus/1527>.

[5] Ibid.

[6] Ibid.

[7] Jonathan J. Rusch, "The "Social Engineering" of Internet Fraud," 19 Aug. 2003 <http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm>.

[8] Sharon Gaudin, "Social Engineering: The Human Side of Hacking," Datamation, 10 May 2002, 19 Aug. 2003 <http://itmanagement.earthweb.com/secu/article.php/1040881>.

[9] Jonathan J. Rusch, "The "Social Engineering" of Internet Fraud," 19 Aug. 2003 <http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm>.

[10] Kevin D. Mitnick and William L. Smith, The Art of Deception (Indianapolis, IN: Wiley Publishing Inc., 2002) 247-248.

[11] Jonathan J. Rusch, "The "Social Engineering" of Internet Fraud," 19 Aug. 2003 <http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm>.

[12] Harl, "The Psychology of Social Engineering," 07 May 1997, 19 Aug. 2003 <http://cybercrimes.net/Property/Hacking/Social Engineering/PsychSocEng/PsySocEng.html>.

[13] Sarah Granger, "Social Engineering Fundamentals, Part I: Hacker Tactics," SecurityFocus, 18 Dec. 2001, 19 Aug. 2003 <http://www.securityfocus.com/infocus/1527>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[14] Kevin D. Mitnick and William L. Smith, The Art of Deception (Indianapolis, IN: Wiley Publishing Inc., 2002) 245-246.

[15] Sarah Granger, "Social Engineering Fundamentals, Part II: Combat Strategies," SecurityFocus, 9 Jan. 2002, 19 Aug. 2003 <http://www.securityfocus.com/infocus/1533>.

[16] Kevin D. Mitnick and William L. Smith, The Art of Deception (Indianapolis, IN: Wiley Publishing Inc., 2002) 261-262.

[17] Malcolm Allen, "The Use of 'Social Engineering' as a means of Violating Computer Systems," Sans Institute, 26 Aug. 2003 <http://www.sans.org/rr/paper.php?id=529>.

[18] "Security Audit," T1 Glossary 2000, 28 Feb. 2001, T1A1 Technical Subcommittee on Performance and Signal Processing, 26 Aug. 2003 <http://www.atis.org/tg2/security_audit.html>.

[19] United States, National State Auditors Association and United States General Accounting Office, Management Planning Guide for Information Systems Security Auditing, 10 Dec. 2001, 28 Aug. 2003 <http://www.gao.gov/special.pubs/mgmtpln.pdf>.

[20] Eric Cole, et al, SANS Security Essentials with CISSP CBK, Vol. 1 (SANS Press, 2003) 2 Vols. 725.

[21] Ibid.

[22] John Silltow and Michael Hines, "Social Engineering, Part 3," ITAudit, 15 Dec. 2001, 26 Aug. 2003 <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=347>.

[23] Ibid.

[24] Google Help. 2003, Google Inc., 26 Aug. 2003 <http://www.google.com/help/refinesearch.html>.

[25] Ibid.

[26] John Silltow and Michael Hines, "Social Engineering, Part 3," ITAudit, 15 Dec. 2001, 26 Aug. 2003 <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=347>.

[27] Google Help. 2003, Google Inc., 26 Aug. 2003 <http://www.google.com/help/refinesearch.html>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[28] John Silltow and Michael Hines, "Social Engineering, Part 2," ITAudit, 1 Nov. 2001, 26 Aug. 2003 <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=379>.

[29] John Silltow and Michael Hines, "Social Engineering, Part 3," ITAudit, 15 Dec. 2001, 26 Aug. 2003 <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=347>.

[30] Leslie Knopp, "It's Amazing What You Can Find Online," 27 Feb. 2003 02 Sep. 2003 <http://www.komotv.com/stories/23351.htm>.

[31] Sharon Gaudin, "Social Engineering: The Human Side of Hacking," Datamation, 10 May 2002, 19 Aug. 2003 <http://itmanagement.earthweb.com/secu/article.php/1040881>.

[32] Pete Herzog, "OSSTMM 2.1. Open-Source Security Testing Methodology Manual," Security Testing, 23 Aug. 2003, Institute for Security and Open Methodologies, 28 Aug. 2003 <http://www.isecom.ca/mirror/osstmm.en.2.1.pdf>.

[33] Ibid.

[34] Ibid.

[35] Jim Hu, "AOL Boosts Email Security After Attack," CNET News.com, 21 Sep. 2000 19 Aug. 2003 <http://news.com.com/2100-1023-242092.html?legacy=cnet&tag=st.ne.1002.thed.ni>.

References

Allen, Malcolm. "The Use of 'Social Engineering' as a means of Violating Computer Systems." Sans Institute. 26 Aug. 2003 <http://www.sans.org/rr/paper.php?id=529>.

Bass, Alison. "Defense Against the Dark Arts." Darwin Magazine Jun. 2001. 26 Aug. 2003 <http://www.darwinmag.com/read/060101/defense.html>.

Bernz. "The Complete Social Engineering FAQ!" 14 Jan. 1997. 19 Aug. 2003 <http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt>.

Christopher, Abby. "The Human Firewall" Network World Fusion 26 May 2003. 26 Aug. 2003 <http://www.nwfusion.com/research/2003/0526human.html>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Cole, Eric, et al. SANS Security Essentials with CISSP CBK. 2 Vols. SANS Press, 2003.

Ecott, Tim. "Bug Watch: The Threat of Social Engineering." Vnunet.com 25 Apr. 2002 21 Sep. 2003 <http://www.vnunet.com/News/1131256>.

Google Help. 2003. Google Inc. 26 Aug. 2003 <http://www.google.com/help/refinesearch.html>.

Granger, Sarah. "Social Engineering Fundamentals, Part II: Combat Strategies." SecurityFocus 9 Jan. 2002. 19 Aug. 2003 <http://www.securityfocus.com/infocus/1533>.

Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics." SecurityFocus 18 Dec. 2001. 19 Aug. 2003 <http://www.securityfocus.com/infocus/1527>.

Gaudin, Sharon. "Social Engineering: The Human Side of Hacking." Datamation 10 May 2002. 19 Aug. 2003 <http://itmanagement.earthweb.com/secu/article.php/1040881>.

Harl. "The Psychology of Social Engineering." 07 May 1997. 19 Aug. 2003 <http://cybercrimes.net/Property/Hacking/Social%20Engineering/PsychSocEng/PsySocEng.html>.

Herzog, Pete. "OSSTMM 2.1. Open-Source Security Testing Methodology Manual". Security Testing. 23 Aug. 2003. Institute for Security and Open Methodologies. 28 Aug. 2003 <http://www.isecom.ca/mirror/osstmm.en.2.1.pdf>.

Hu, Jim. "AOL Boosts Email Security After Attack." CNET News.com 21 Sep. 2000 19 Aug. 2003 <http://news.com.com/2100-1023-242092.html?legacy=cnet&tag=st.ne.1002.thed.ni>.

Knopp, Leslie. "It's Amazing What You Can Find Online." 27 Feb. 2003 02 Sep. 2003 <http://www.komotv.com/stories/23351.htm>.

Mitnick, Kevin D., and William L. Simon. The Art of Deception. Indianapolis, IN: Wiley Publishing Inc., 2002.

Ollmann, Gunter. "The Fine Art of Deception." SC Magazine Aug. 2003. 26 Aug. 2003 <http://www.scmagazine.com/scmagazine/2003_08/feature_3/>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Robinson, Shane W. “Corporate Espionage 101.” Sans Institute. 21 Sep. 2003 <http://www.sans.org/rr/paper.php?id=512>.

Rusch, Jonathan J. “The “Social Engineering” of Internet Fraud.” 19 Aug. 2003 <http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm>.

Silltow, John and Hines, Michael. “Social Engineering, Part 2.” ITAudit 1 Nov. 2001. 26 Aug. 2003 <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=379>.

Silltow, John and Hines, Michael. “Social Engineering, Part 3.” ITAudit 15 Dec. 2001. 26 Aug. 2003 <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=347

“Security Audit.” T1 Glossary 2000. 28 Feb. 2001. T1A1 Technical Subcommittee on Performance and Signal Processing. 26 Aug. 2003 <http://www.atis.org/tg2k/_security_audit.html>.

“Social Engineering” The Jargon File, version 4.4.5. Raymond, Eric S. 14 Aug. 2003. 26 Aug. 2003 <http://catb.org/~esr/jargon/html/S/social-engineering.html>.

Social Engineering. Vigilante. 26 Aug. 2003 <http://www.vigilante.com/inetsecurity/socialengineering.htm>

Thomson, Iain. “You are the Weakest Link.” Vnunet.com 21 Oct. 2002. 21 Sep. 2003 <http://www.vnunet.com/News/1136127>.

United States. General Accounting Office. Federal Information System Controls Audit Manual. Vol. 1. Jan. 1999. 28 Aug. 2003 <http://www.gao.gov/special.pubs/ai12.19.6.pdf>.

United States. National State Auditors Association and United States. General Accounting Office. Management Planning Guide for Information Systems Security Auditing. 10 Dec. 2001. 28 Aug. 2003 <http://www.gao.gov/special.pubs/mgmtpln.pdf>.

Warning Signs of Covert Eavesdropping. 2002. Granite Island Group. 21 Sep. 2003 <http://www.tscm.com/warningsigns.html>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 23rd, 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