Global Information Assurance Certification Paper

Social Engineering – "How secure are you?"

By J Hollinshead, MCP, CNS

GIAC Security Essentials Certification (GSEC)

Practical Assignment

Version 1.4

Social Engineering n. **Term used among crackers and samurai for cracking techniques that rely on weakness in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark whom has the required information and posing as a field service tech or a fellow employee with an urgent access problem.**[1]

Security is an ever growing problem in the IT industry; however one of the greatest if not the greatest threat is not the network hardware but the human factor. Social engineering is a reconnaissance tactic to gain any and all information which might help a hacker exploit vulnerabilities in a company's network. We will discuss the problems and solutions on how a company and customers can suppress a social engineer's advances. While looking at your hardware vulnerabilities, do not forget to evaluate your human vulnerabilities.

Many companies overlook social engineering when evaluating their network security. They do not evaluate how easy or hard it is to enter the company without an appointment, how deliveries are handled, how free their employees are with company information when talking with or around strangers, or how secure the server room itself is from intruders. Every security evaluation should involve a third impartial party. They can evaluate how difficult it is to gain access to vital information through social engineering techniques. Reconnaissance is a major part of breaching a network. Can the third party confuse the staff, impersonate someone, or just walk into the office building to gain access to the network? Are there company policies in place to educate company employees and gatekeepers on how to handle visitors and deliveries?

Data is only as good as the person inputting it, and security is only as good as the person writing the policies and implementing them. A computer just sits there until someone turns it on, and a company is only secure until someone breaches it. Through the following information, I hope to help you tighten your company's security and make your network anything but simple for an intruder to access.

Network security issues continue to rise. MSNBC.com reports, "The total number of reported computer security incidents doubled in 2001, compared with the previous year, with more than 52,000 Web Site attacks, viruses, network intrusions and other security breaches recorded by the Computer Emergency Response Team at Pittsburgh's Carnegie Mellon University. And analysts predict the number of computer security incidents may double again this year."[2] The Computer Security Institute (CSI)/FBI Computer Crime and Security Survey states, "Forty percent of respondents detected system penetration from the outside (only 25% reported system penetration in

2000). Thirty-six percent of respondents detected denial of service attacks (only 27% reported denial of service in 2000). Ninety-one percent detected employee abuse of Internet access privileges (for example, inappropriate use of e-mail systems). Only 79% detected net abuse in 2000. Ninety-four percent detected computer viruses (only 85% detected net abuse in 2000."[3]

Have you ever had one of those days when out of the blue someone you don't know says they know someone that knows you, and that that certain someone asked them to contact you? Confused? Hopefully you are. As a salesperson, confusion has always been an easy way to get to a key contact person. People are too trusting and therefore, security is not something they pay much attention too. I have used reconnaissance techniques to get in with the IT managers of companies from small/medium business to Fortune 500 companies. In doing so, I was able to retrieve vital information about their network security.

Kevin Mitnick Quote:

"(As) the media characterizes social engineering, hackers will call up and ask for a password. I have never asked anyone for their password."[4]

Another way social engineers gain access to vital information is to gain the trust of someone within the company. If someone's trust is gained, they will usually give enough information for someone else to gain unauthorized access to their network. Some use this information to commit illegal acts like fraud extortion, and or industrial espionage. However, someone may simply want to manipulate the network just to be malicious. Another approach to gain information is through manipulation. For example, it is easy to impersonate someone within a company. This is can be done simply by listening to a "mark", someone designated as a target for information, and practicing until it is possible to impersonate them.[13] Some go as far as using a voice changer to impersonate their mark. Be wary of female voices. Women are perceived to be more trusting and therefore easier to confide information or trust.[5]

Problems:

As mentioned above, my goal on a reconnaissance call is to confuse the gatekeeper (receptionist or security guard) enough for them to let me visit with a key contact person. This can be rather easy if you inform them you are there to visit a specific person. How did you get this person's name? Did you have to dig hard? No you just went to their company's website, did an internet search for publications including some of the company's information, or you just asked for the IT director's name.

There was one instance I told a receptionist I needed to talk to Mr. Smith and she connected me to a Mr. Smith. I told him they must have transferred me to the wrong extension since I was looking for another department. Not only was I transferred but in transferring me I received important information, a key contact's name. Once I made contact, I would ask for an e-mail address so I could send him/her some information.

Can you tell me how many login names are the prefixes of an e-mail address? Many network administrators use the login name as the first part of the e-mail address because it easier to configure the network. Half of a hacker's job is now complete. They have the person's name and/or e-mail address. You can also use the person's name when trying to gain certain critical information about the company from other employees or administrators. Once you have an employee's user name figured out, you can use an assortment of password crackers to access the network from this account. Whether the intruder enters the network through an internal or external source, once access to a computer or the network has been achieved intruders can deploy malicious viruses, deploy a Trojan virus to open network ports or even deploy a sniffer program to capture password and network activity.

Other areas of security weakness are in the way deliveries and walk-ins are handled. It is amazing how far you can get into a company by just walking in or acting like you have a package to deliver. By telling the gatekeeper you know where the office is or even by asking for directions to the person's office, you would be amazed how many companies will let you go on your way. Other times you might say "HI" as you just walk right past the gatekeeper. Once you make it past the gatekeeper, it's not hard to find your way to the server room.

Here is a true story I found in Sarah Granger's "Social Engineering Fundamentals, Part 1: Hacker Tactics":

"One morning a few years back, a group of strangers walked into a large shipping firm and walked out with access to the firm's entire corporate network. How did they do it? By obtaining small amounts of access, bit by bit, from a number of different employees in that firm. First, they did research about the company for two days before even attempting to set foot on the premises. For example, they learned key employees' names by calling HR. Next, they pretended to lose their key to the front door, and a man let them in. Then they "lost" their identity badges when entering the third floor secured area, smiled, and a friendly employee opened the door for them.

The strangers knew the CFO was out of town, so they were able to enter his office and obtain financial data off his unlocked computer. They dug through the corporate trash, finding all kinds of useful documents. They asked a janitor for a garbage pail in which to place their contents and carried all of this data out of the building in their hands. The strangers had studied the CFO's voice, so they were able to phone, pretending to be the CFO, in a rush, desperately in need of his network password. From there, they used regular technical hacking tools to gain super-user access into the system.

In this case, the strangers were network consultants performing a security audit for the CFO without any other employees' knowledge. They were never given any privileged information from the CFO but were able to obtain all the access they wanted through social engineering. (This story was recounted by Kapil Raina, currently a security expert at Verisign and co-author of mCommerce Security: A Beginner's Guide, based on an actual workplace experience with a previous employer.)" [13]

One time I rang the delivery door bell to a local office. When I was greeted, I said I had a delivery for someone and that I knew where his office was located. The greeter let me right in without requesting any information from me. Here is the thing that really got me. When I arrived at the server room, I found it unlocked and the IT Director out to lunch. The server room was isolated and unlocked. The servers were locked down, but all I would have had to do was put in NTAccess, a software which identifies the administrator's user name and resets the administrator's password in less than ten minutes. I could have stolen the backup tapes and/or loaded a backdoor access Trojan or a virus in less than ten minutes from this uncontrolled server room.

Another vulnerability can be found at social gatherings. How many times have you attended a "networking" (card swapping) chamber gathering? It is not hard to follow or meet a person and get them to tell you all about their workplace. This is an easy way of gathering important information. People like to brag, discuss or gripe about their workplace. Have you heard the saying `any press is good press`? Well, any information you can retrieve is useful information. The more you know about a company or person, the easier it will be to gain access to their company's information.

Network administrators should consider limiting their staff's ability to use online chatting or Instant Messaging for communication purposes. Recently, CERT announced that thousands of victims have downloaded malicious Trojans, Denial of Services (DOS), or other files without knowing what they are downloading. "This is purely a social engineering attack since the user's decision to download and run the software is the deciding factor in whether or not the attack is successful, "said the report, by CERT Internet security analysis, Allen Householder.[6] The company associates should also be reminded that they need to know who is on the other end of the chat session or instant message so they do not divulge anything which might help a social engineer penetrate the network.

Solutions:

In the very beginning, the IT Director needs to sit down with upper management and find out how secure they think their financial, policy, and competitive information is. Discuss the policies you think need to be in place in order to actually achieve security. Will their employees or they be disturbed in their everyday activities? New security policies should inconvenience employees as little as possible. Making employees learn several new in-depth policies could cause them to complain to upper management, which could cause political headaches.[7]

The first place to implement security policies is with the front desk attendants and security guards. Write some guidelines on how to repel an unwanted guest. An unwanted guest is someone without an appointment. Implement an appointment only policy. Let the gatekeeper know under no circumstance are they to allow anyone past their area. Write down some qualifying questions to determine the validity of the guests visit. Inform them not to reveal any company or employee information during their

conversation with the guest. Keep it on a need to know basis. They do not need to know anything if they do not know it already. The gatekeeper is going to get bombarded with questions about the company and themselves (with possibly a little charm thrown in), but make sure the gatekeeper knows to keep their gate closed.

Most gatekeepers answer the phones, take messages, and notify staff when their appointments arrive. It is hard to take security serious when you feel your role is not very important. Make sure the gatekeepers know they have the most important security job of anyone in the company. They are the first line of defense. The gatekeeper does not need to have a lengthy conversation with visitor. Remember the phone case involving an AOL customer service representative. Sarah Granger quotes the Vigilante report in her article. "In that case, the hacker called AOL's tech support and spoke with the support person for an hour. During the conversation, the hacker mentioned his car was for sale cheaply. The tech supporter was interested, so the hacker sent an e-mail attachment `with a picture of the car`. Instead of a car photo, the mail executed a backdoor exploit that opened a connection out from AOL through the firewall."[13] This is why you need to inform your gatekeepers to be hospitable but get to the point. Intruders will attempt to gain information through deception and trust. The longer the intruder can keep a gatekeeper on the phone, the more likely it is that they will be able to obtain valuable information.

With the evolvement of the Internet, social engineers can now research articles in newspapers, magazines, and company websites. Although you cannot limit the access of media information, you can limit the amount of company information your website reveals. Remove all specific staff information from your website. This includes e-mail addresses, names, positions, direct phone numbers, and extensions. A person can still retrieve staff names from surfing the web or just asking someone leaving the building but why make their job any easier by posting everything on your site.

Recently, CNN.com reported that Richard Clarke, head of the White House Office of Cyberdefenses said, "al Queda was using the internet to do at least reconnaissance of American utilities and American facilities". Clarke said, "If you put all the unclassified information together, sometimes it adds up to something that ought to be classified". Clarke also said the U.S. doesn't know whether there have been successful penetrations of critical infrastructure networks. But, "If I were a betting person, I would bet that many of our key networks have already been penetrated," he said."[8] It is very scary to think terrorists use the Internet for their reconnaissance missions. When implementing a company or client website, remember to limit information social engineers might be able to use to access your network. You want to use your website as an information medium, but you also want it to intrigue customers to actually contact you about your company. When they contact the company, then your gatekeeper has memorized the new policies and can qualify the caller as a real potential customer.

Implementing a honey pot phone system is another line of defense. If someone calls in an attempt to gain information, they can be directed to a fictitious voice mailbox. Set up a voice mail box with a female voice and another one with a male voice. You can

even go as far as putting a name with the voice mailbox. This will come in handy if you receive callbacks for this person. When they callback and ask for the bogus person, you know the call in not legitimate and to transfer them to the fictitious mailbox. This will help secure your employees from devious callers.

Just like a implementing the callback feature, for remote access server, you should do the same if you do not have a voicemail system or if the company's name is an owner's name. (Callback feature is when the computer calling into the remote access server is called back by the remote access server at the number specified for the user. This insures the correct person is gaining access to the network and database items.) For example, lawyers, CPAs, and doctors must have their names as the company, or as part of the company name in the state of Texas. Obviously, it makes it a lot easier to get in with an individual's name. If the owner accepts the call and then realizes they should not have, they can ask for a return number so they can call them back. If at all possible, limit your name from the company name. It is unfortunate that the above professions have to list their own names in Texas. Here you have three professional areas where client confidentiality is key, and their names are there for social engineers to use to help them manipulate their way into their networks and databases.

Now we have discussed how to handle an unwanted guest personally and on the phone, how can we keep someone from just walking in while the gatekeeper is on the phone or talking with another visitor?

If at all possible, the entrance area should be isolated from the rest of the building by using buzzer doors. Another security option is that employees be required to use an alternate entrance using ID cards for access. After September 11, 2001, IT and personal security have become a priority. INFORMATIONWEEK wrote an article a week after 9/11 about how the terrorist act has caused companies to think seriously about their security. The article stated that a metal company's security chief had been lobbying for months, without success, for an employee photo or ID system based on smart cards to gain access to buildings and the network. "We could be a highly targeted company," he said. "What's to stop a terrorist from walking into the building with a satchel [containing a] bomb?".[9] Employees coming in and out of the front door is just one more obstacle for the gatekeeper to monitor. What happens when there are multiple visitors and employees coming through the same entrance at the same time? The gatekeeper can become confused and an intruder can slip in with the employees. Once inside the building the intruder is like a mouse in a maze, all they have to do is find a vacant office and they have found their piece of cheese.

Now that we have all of the entrances contained, how should deliveries be handled? To insure an intruder does not take advantage of a relaxed delivery policy, consider implementing some of the following deterrents. A set time for daily deliveries should be posted. Have everything delivered to the same location every time. Implement a sign-in log and ID policy for all deliveries. Obviously, the ID policy may not work for UPS or FEDEX delivery personnel, but you can make it work for everyone else. Inform companies of your delivery policy before they arrive so there will be less resistance. The

sign-in sheet should require their name, company, time of appointment, copy of their ID, and who they are there to meet. Just as you want a warning message when a user logs in to the network, create a warning at the top of each sign in sheet page which informs the visitor they may have access to confidential information while passing through the building; and if any information they retain during their visit is used in a malicious or destructive way towards your company, they will be prosecuted. For example, this policy might help you prosecute someone who has used confidential company information that was obtained from an employee's monitor while passing through the building. The most important policy is not to allow guests past a certain point in the building. If you can implement these policies, you can reduce a social engineers chance of penetration.

If someone does make it into the building, how can you secure the server area? Even though the server may be locked when no one is in the area, an intruder can get around a locked server by using certain software tools. All dedicated IT managers should have a lock on the door leading into the server room or closet. The lock should not be a deadbolt or twist knob lock. Employees have to remember to physically lock the deadbolt. The door should automatically lock when it is closed. Types of authentication locks to consider include an electronic keypad, combination, card scanner, thumb scanner or retina scanner. Network administrators should also install cameras in the server room or closet pointing toward the server to view all actions (this may help reverse any damage inflicted). Another camera should view who enters the room, and another should view people as they leave. Make sure that the recording devices are set up with timestamp features and that the time is correct. That way, if someone enters the server room and performs an illegal or unauthorized operation on there server environment, they will be caught in the act. If the company has implemented a secure anti-social engineering policy, then it will be harder to gain access the servers. The cameras will help identify any employee or former employee who gains access to the servers. Other employees are the most likely candidates to over-hear the access code to the server room.[10]

Many administrators configure e-mail addresses to match the login name. If a person's e-mail address is mike@smithco.zoo, you can almost bet the user name is mike. Although it is more time consuming, administrators should consider implementing different usernames and e-mail prefaces. A hacker with a user name has won half of the battle. As mentioned before, then all you need is a good password cracking software to gain access to the network and its databases to steal information or execute any number of intrusion or malicious software.

You should also encourage your business associates to discuss as little as possible with strangers and limit the office information they give to clients or family members. People are listening, and although you might not think it is harmful to mention the president's name and title, someone might use that information in a malicious way. Not only do they now have the president's info, they have your name as a source to use when contacting the president. This exploit can be used to gain inside access. The employee use of Instant Messenger's and chat rooms should also be limited. If the IM ports cannot be closed, at least tell staff members not to reply, download or communicate company information through a chat or IM.

Now that you have read this, how many things have you inadvertently overlooked at your company? Sometimes it is the most obvious things which can cause the most harm. It is no longer necessary to dive into dumpsters to retrieve compromising information on a company. Someone just has to be a good listener to exploit a company's vulnerabilities. If a gatekeeper does not handle confusion well; then confuse them until you are inside. If a gatekeeper takes what you say as the truth; then tell them whatever they want to hear to gain inside access. A good social engineer will be very creative to gain access to vital company information. How secure is a company from a well dressed, well mannered, and creative social engineer?

Securing your hardware, using security tools, and which tools to use for searching network vulnerabilities are discussed much more than social engineering. Not focusing on the human factor as a main vulnerability is a mistake. Educate customers and/or staff members about the vulnerabilities that are involved in social engineering. Once they are aware of security vulnerabilities which are not IT related, they can help secure their network by being more aware of the social engineering tactics being used to gain network access.

It is easy to test firewall and server vulnerabilities. It is easy to run disaster recovery drills. It is not so easy to test social engineering vulnerabilities. A security specialist must know more than how to secure your hardware. Sometimes a hacker is not on the computer but walking through the halls, chatting online with an employee, or reading articles. They may be using the K.I.S.S. (Keep It Simple Stupid) method, but it is up to us to make sure social hacking is anything but simple.

I leave you with three quotes to help you consider how secure you are against a social engineer:

"Also, the human part of the security set-up is the most essential. There is not a computer system on earth that doesn't rely on the humans. This means that this security weakness is universal, independent of the platform, software, network or age of equipment.

Anyone with access to any part of the system, physically or electronically is a potential security risk."[11]

Kevin Mitnick Quote:

"there was something missing from the conference. No sessions were offered covering physical attacks or social engineering. You could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain vulnerable to old-fashioned manipulation."[12] [13]

Patricia Rapalus, CSI Director Quote:

"Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions."[3]

---

[1] "Social Engineering Definition" The Jargon Dictionary
URL: http://info.astrian.net/jargon/terms/s/social_engineering.html
[2] Barnett, Jennifer. "Hacking Grows With Internet Use" 3/26/02 MSNBC.com
URL: http://ww.msnbc.com/news/724952.asp?cpl=1
[3] Power, Richard. "Computer Security Issues & Trends: 2001 CSI/FBI Computer Crime and Security Survey Volume 7 No. 1" Computer Security Institute Spring 2001
[4] Lemos, Robert. "Mitnick teaches 'social engineering" 7/16/00 ZDNET.com
URL: http://zdnet.com.com/2100-11-522261.html
[5] Bernz. "The Complete Social Engineering FAQ!" 1996
URL: http://users.rcn.com/bobrob.nai/socialen.txt
[6] "CERT: Instant Messaging is threat to your corporate security" 3/22/02 www.cw360.com
URL: http://www.360.com/bin/bladerunner?REQUNIQ=1016824399&REQSESS=0Z91864L
[7] Austin, Doug; Bryce, Alexander; Dinehart, Rob; Estep, Brian M.; Joyce, Stephen; Kramer, Carol; Marchany, Randy; Northcutt, Stephen; Ritter, John; Scarborough, Matt; Triulzi, Arrigo; Cole, Eric. "Basic Seurity Policy" Track 1 – SANS Security Essentials 1.2 SANS Security Essentials II: Network Security.
[8] Thibodeau, Patrick. "Clarke: Terrorists used Net for info on targets" 2/15/02 CNN.com
URL: http://www.cnn.com/2002/TECH/internet/02/15/terrorists.internet.idg/index.html
[9] Hulme, George v. with Martin J. Garvey. "Terror Attack Brings Renewed Emphasis on Security" 9/17/02 CMP Media LLC.
[10] Weber, Richard. "Security Essentials: Conducting a Security Audit" 1/2002 Technical Support Magazine. Technical Enterprises, Inc.
[11] Text of Harl's Talk at Access All Areas III. "People Hacking: The Psychology of Social Engineering" 5/07/97
URL: http://cybercrimes.net/Property/Hacking/Social%20Engineering/PsychSocEng/PsySocEng.html
[12] Mitnick, Kevin. "My first RSA Conference" 4/30/01. URL: http://online.securityfocus.com/news/199
[13] Granger, Sarah. "Social Engineering Fundamentals, Part 1: Hacker Tactics" 12/18/01
URL: http://online.securityfocus.com/infocus/1527

Last Updated: September 22nd, 2017

Upcoming Training

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