Global Information Assurance Certification Paper

Social Engineering:
Testing the Boundaries of my Organization

By
Lisa Taylor

GIAC Security Essentials Certification (GSEC) – Practical Assignment

Version 1.4c.

October 28, 2004

Table of contents

Introduction

4 years ago, I was hired as a Network Administrator at my organization, (medium sized enterprise) and my duties fell within the description of what a Network Administrator was. Since that time, our company has become more reliant on technology in many facets of our business, primarily with web applications. Our company provides information solutions to a specific industry. In the last few years we have moved from providing this in print format only to offering it via the web. The evolving nature of our network environment and the added complexities of new technologies has propelled me into the roll of the Network/Security Administrator. Initially our network security consisted of a proxy gateway. Since then we have added many security layers to our network; firewalls at all locations connected via our VPN infrastructure, an IDS and an IPS solution and viral server protection. In a nut shell we are developing a "Defense in depth" network Infrastructure that has domino-ed down to our workstations. As much as I am proud of our achievements, after taking the GSEC course I now see some holes in our security practices that we have ignored, that now must be addressed.

This paper addresses one of those holes which plays with the very culture of my organization; for we take pride in our "warm and fuzzy family-oriented" work environment. Documented here is the process I applied when I orchestrated, *an authorized,* Social Engineering attack on my company.

What is Social Engineering?

When I asked some friends and IT colleagues what they thought Social Engineering was, they either stared at me blankly or started laughing nervously? Regardless of the initial response the answer came back a resounding "I don't know?" In search of a simple definition to satisfy the perplexity on their faces I found that it is:

> An attack based on deceiving users or administrators at the target sire. Social engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user to attempt to gain illicit access to systems. [1]

I ended up piecing together my own definition and now I simply tell them that it is:

> A technique used by hackers' to gain unauthorized access to information/resources by means of deceiving people.

Social Engineering is a form of Information Warfare, which is a tool that is used in political and business circles to manage and alter the perceptions of people towards products; companies; countries and even their very *own* opinions. Attackers armed with this knowledge patiently seek out for a door of opportunity to breach the innate trust that we as humans have with each other. Being helpful is a human core-building block that we are taught from Kindergarten. Trusting and respecting people of authority is another. Attackers basically abuse our response to people in a dilemma. People, are listed as one of the top risks for business continuation - stated

by ey.com's Information Security Risks and Solutions presentation[2]. This is an area of network security that senior management tends to overlook.

> The difficulty in securing your enterprise is no longer a technical problem. It is a social, political and cultural problem. Senior leadership wants objective measurement of an inherently subjective discipline… the threats are changing daily; and many organizations are forced to do more with fewer people. [3]

It is for these reasons senior management needs to champion the issue of security – to implement good security practices at all levels. Security-educated employees are vital to the success of securing the confidentiality and integrity of the corporation not just IT staff and management.

From studies of companies hacked or internally attacked, we see there is a procedure that an attacker follows: reconnaissance, enumeration and penetration. It is in the initial reconnaissance that an attacker will use social engineering to discover many, or better yet, uncover all of the security holes in an organization. Kevin Mitnik[4], used a method of social engineering to discover the trust relationships between Shimomura's computers before launching his famous IP spoofing attack [5][6].

Attackers can gain unauthorized access to information and resources, using social engineering in one of two methods - technology guises and psychological manipulation.

Technology Guises

You've just received an email from a financial institution or credit card company asking you to click on the link below to immediately update your records, most times claiming to have a problem. Now if you do not belong to this financial institution or carry one of their cards, it's at this point most people would know that someone is *phishing*[7] for information. When a hacker sends out these types of mass mailings, they are not looking for everyone to respond. All it takes is one user to respond to the questions being asked and an attacker will have access to your accounts. This type of attack is not limited to emails. Pop-up windows at websites requesting a user to re-enter their password mislead the user to believing that they are actually interacting with the original website.

Psychological Manipulation

> Security is all about trust. Trust in protection and authenticity. Generally agreed upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack. Many experienced security experts emphasize this fact. No matter how many articles are published about network holes, patches, and firewalls, we can only reduce the threat so much... and then it's up to Maggie in accounting or her friend, Will, dialing in from a remote site, to keep the corporate network secured. [8]

Psychological schemes are primarily successful due to the lack of security education for employees. Many people say that this type of Social Engineering exploits a

human weakness[9], but I don't see trust as being a human weakness. Trust as a 'whole value' plays an important role in security. It is this integrity or trustworthiness that we are protecting in our data and yes in the people *that* protect the data. When Social Engineering uses psychological manipulations, I believe it challenges our complacencies and fears.

It's easy for security to be in the fore-fronts of our minds after incidents like September 11th, but as soon as the smoke clears we all too quickly get comfortable again in our environment. We want to forget why we have to be on our guard, and this is just what an attacker wants you to do to.

Impersonation

Impersonation happens when an attacker plays out the role of an authority figure or valid employee, either over the phone or in person. This could be as simple as a call to the Helpdesk, requesting a password reset. The Helpdesk technician who does not know every voice will helpfully resets the password and provide it to the caller. With no controls or verifying procedures in place an attacker could walk away now having a valid username and password to the internal network. Professional hackers are even known to use special voice boxes to disguise their speech [10].

The Setup

Since reading the GSEC material and analyzing several attacks, I tried to adopt a hackers' frame of mind as I planned my experiment [11]. This was going to be a challenging, since I have great knowledge of the organization. I would have to try to erase the last six years of working here and start from the beginning.
I first gathered together 3 accomplices. I gave each of them different goals but there was a common element, to note the time of day and duration required for each successful attack.

Suzie

Suzie had two telephone calls to make at random times through the day. For the first phone call, she posed as a tax/accounting professional setting up a new business. She wanted to subscribe to various products in her field and wanted to speak to a sales person. Her first goal was to get the name, and title of this sales person.

In the second phone call, her goal was to get the name of the Network Administrator. She called in pretending to be a shipper from Cisco Systems. She explained that she was sending a box to the Network Administrator but the person who took the order did not take the Administrator's name.

Now obtaining this information on its own is pretty harmless since people call in all the time and we give them our contact info. But in order to assimilate an attack I had to start with the basics of just getting a feel of how friendly, open and receptive this company was. As an attacker, going to our website gives you a lot of information on our products and even how to find a field sales rep, but that could be all hype. So getting a real feel of the company would require some phone calls.

Justin

Justin is a Cabling Technician who works for the vendor that the organization uses for data cabling. He has been in and around the building on many occasions and knows the floor plans well. The Helpdesk staff thinks he's a funny guy who always does his work with a smile. Justin's goal is to get onto the 9th floor and then into the computer room. On a scheduled work day no one would even pay attention to this but on this occasion he is not being escorted by an IT staff member. He is however wearing a visitor's badge that he left with from a previous visit instead of a contractor's passcard. To get through the doors on each floor you require a passcard that would be used in the card reader. Since the visitor's badge is a simple MSWord generated label with a protective cover, it was easy to create one even if he failed to retain one. Once in the computer room he is to leave a box in the corner.

Lance

Lance has been briefed with the 9th floor, floor plan and has the visitors badge given to him by Justin. With the few names of individuals in the company (to throw around if necessary) given to him by Suzie, Lance arrives shortly after Justin has left. He is clumsily carrying a large Foundry box which seems heavy. During working hours, 8:30am to 5pm, the elevators do not require a passcard. His goal is to get up to the 9th floor, enter through the 9th floor doors that require a passcard, and into the computer room. If possible he should try to be left alone in the room. He is supposed to enter through the doors that are adjoining to the Helpdesk area and not Infrastructure support. There are fewer employees on that side plus the Second-line support-Infrastructure group would be more likely to be vigilant and stop him. Everything he needs to copy data is in the box and the additional hardware is in the box that has Justin left for him.

I must make note here that, Lance is 6ft 5in tall, 250lbs, and is of African-Canadian decent. He is an actor and in *all* circles his stature commands attention. It's for these reasons initially I didn't want to use him. But once I thought about it, I figured if he could get in unnoticed then anyone could.

Attack Results

Suzie

In the first phone call, Suzie explained her situation to the receptionist and was transferred to the Inside Sales Manager. She received his voicemail which told her his name and title.

In the second phone call Suzie did receive some opposition. The receptionist did not know who the Network Admin was so she transferred her to the Helpdesk. At the helpdesk the senior tech, who was answering calls was leery of why someone would be asking for the Network Administrator name. He put Suzie on hold and asked a System Admin person if they thought it was strange.
Regardless, the name was given.

Goal accomplished.
Time of first phone call – 2 minutes
Time of second phone call – 6 minutes
Total: 8 minutes

Justin

Justin was cool as a cucumber when he walked in with a user from the 9th floor. He walked directly to the computer room and said, "hi" to some IT staff that he knew. He casually asked one person to open the computer room, telling them that I had gone to get a passcard for him. He put the box down on the floor, took a peak at the patch panel and then left.

Goal accomplished.
Time to enter 9th floor doors – 2 minutes
Time to enter computer room – 1.5 minutes
Exit time – 1 minute
Total: 4.5 minutes

Lance

As I sat outside and watch Lance walk in the front doors my stomach was in knots. Out of all my accomplices, he knew least about technology. I was afraid that my briefing was not as informative and that he would fail to accomplish his goal.

As Lance approached the building a man opened the front doors for him. Lance got on the elevator with this gentleman and immediately pressed 9. He soon realized that the gentleman was going to the same floor which made him a little nervous but he continued to hold his position. When they both got off the elevator, the gentleman

asked him who he was looking for. Lance explained to the gentleman that he was looking for Lisa Taylor. The gentleman said, “oh sure!” and took him to my desk and then walked away.

The procedure is to have all visitors sign-in at reception. With Lance going directly to the 9th floor it was clear that he did not sign in.

Lance then continued to walk towards the computer room (walking through the Infrastructure support area that I told him to avoid) and passed a group of three techies. He proceeded to the bank of desks where I told him he should solicit help from. Since no one was there he walked back to the group of techies and stated that he needed to find me since he needed to rack the equipment in the box right away. Without hesitation he was taken to the computer room. Once inside, he persuaded the tech to go and look for me while he began racking the equipment. He spent a good 5 minutes in the computer room walking around and pretending to fiddle with the network equipment. Completely alone in the room he had access to every device. Lance left on his own without saying a word to anyone, came down the elevator and met me outside to give me the results.

Goal accomplished.
Time get in the 9th floor doors – 2 minutes (approx.)
Time to get into the computer room – 2 minutes (approx.)
Time to cause a possible problem – 5 minutes
Exit time – 2 minutes
Total: 11 minutes (approximately)

As I am typing in the results of my experiment, I am deeply troubled because I now realize that it was someone from my department that escorted Lance all the way into the computer room and left him there unattended. I am even more concerned that it is very late in the day and no one has mentioned to me that they allowed a delivery person in to rack equipment. No one has noticed the box on the floor of the computer room in the middle of isle. This box could have contained anything, even a bomb. Below is a picture of the box. It’s not small or inconspicuous. This has been a great learning experience for me, my manager and the CIO of my company.

> O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible; and hence we can hold the enemy's fate in our hands.
>
> Sun Tzu on the Art of War

The Internal Attacker

Defense in Depth is not only a technical term. If this methodology is not applied to our physical and social layers then not even the world's greatest Firewall or IDS can save us. As I proved in this report we are only as strong as our weakest link. Experts say that nearly 80% of information security breaches and resulting loses originate from inside an organization[12]. With more information about the organization and greater accessibility to resources than a hacker, the internal attacker can cause damages of enormous proportions. Nsi.org reports on one company losing 10 million dollars when an internal attacker planted a time-bomb[14] that deleted all of the company's software[13]. An internal attacker using social engineering as a tool can succeed easily by using simple tricks to gain information or access. A common trick, known a shoulder surfing, happens when an attacker watches while someone is typing in their password. Another approach is to wait for a co-worker to be incapable of fulfilling a task and then offering their assistance. The attacker is more than happy to help and nonchalantly accepts the password to make changes or obtain access to additional resources.

Attackers are also known to use a method called Reverse Social Engineering. This technique happens when an attacker creates the impression that they are a figure of authority. This could be senior management or better yet a system or network administrator. In this type of situation, users tend to give information that is not even being solicited. With additional pieces of the puzzle being handed to them, attackers are able to plan a stronger more effective attack.

For most people, throwing out the trash is a duty they'd rather delegate to someone else. For an internal user seeking to acquire information to exploit or gain access this is a great place to start. It is not uncommon for an employee to organize and pay bills from their desks. They may even sort through all their personal mail on a lunch break. Dumpster-divers[15] look for such opportunities to obtain addresses, credit card information or requests, and confidential material.

For the majority of people, we judge others based on our value system. Since we have various levels of integrity, we assume that others share the same values. It's because of these assumptions that an attacker can work along side of us for years and never have their actions questioned even when their actions are questionable. This is precisely why an attacker is able to walk in and about users' desks looking for passwords written down on sticky notes.

Mitigation Strategies

Defense in depth mythology emphasizes that no *one* product can address securing the network infrastructure, hosts, applications, and data. Security must be applied to all layers of the infrastructure but also to all levels of an organization.

Here are a few guidelines to mitigating the risks of Social Engineering.

- **Appoint a member of upper management to champion Information Security.**
  Senior management controls the company's governance and budgets. Without management backing, security gets pushed to the back burner. Executives are focused on growth and getting the product out the door. As security professionals we need to learn to translate security risks into dollars. Showing the 'Return on Investment' (ROI) is a vital factor in obtaining their buy in.
  Security breaches = lost customers = lost revenue

- **Conduct a risk analysis from a technology and social view.**
  A risk analysis must point out areas of penetration, from network to physical to psychological levels and will show the probability of those risks becoming a reality.
  Areas to consider as risk factors: Access to phones; Dumpsters; computer room; meeting rooms; mailroom; building entrances; intranet and internet; employees; and disasters.
  Any element that would hinder the continuation of the business must be considered a risk.

- **Create a clear, concise security policy that is easily accessible by all employees.**
  A security policy takes the guess work out of "how to handle security issues". Without clear directives, employees will make judgement calls that may not be in the best interest of the company.

- **Educate and train employees on the psychological and technical risks that surround them daily.**
  The importance of security needs to be constantly sent to existing and new employees. The message should not be one to put fear in a person's spirit but a message to preserve and protect the way the organization does business.

- **Implement regular audits of security policies and standards.**
  A security policy is a living-document. The only way to prove that it is meeting the needs of the organization at all times is to test it.

- **Setup an Incident Response team.**
  It is important to have more than one person who knows how to respond to a security breach, fire or other disasters.

Conclusion

Organizations can spend millions on security initiatives and still not be secure. All Employees must be educated about security risks and be active participants in enforcing security policies and standards. Securing an organization is a collective effort and is not only for the IT professional.

After attending one of the largest data security conferences in the world, Kevin Mitnik stated:

> "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..."[16]

As Computer Technology grows up and matures we can no longer sit back and clutch it immaturely. One of my favorites passages from the Bible says, "When I was a child, I talked like a child, I thought like a child, I reasoned like a child. When I became a man, I put childish ways behind me"[17]. Adopting industry-standard security practices allows us to put away our childish thinking that everyone is to be trusted.

References

[1] Mississippi Department of Technology Services
www.its.state.ms.us/et/security/glossary.htm

[2][3] Gabriel Apostu – Information Security Risks and Solutions – November 14th, 2002
http://www.ey.com/global/download.nsf/EYSEE/Information_Security_Risks_and_Solutions_-_14_Nov_2002/$file/Workshop%203%20v1%20Apostu.ppt

[4] Kevin Mitnick is one of the world's most well-known computer intruders. He was arrested in 1995 and spent four and a half years in prison as a pretrial detainee, before pleading guilty in 1999 to computer fraud. He was released from Federal prison in January 2000, and is currently under federal supervised release, barred from using computers and the Internet. His writing has appeared in Time Magazine and the U.K. Guardian. He now hosts a weekly radio talk show on KFI, Los Angeles

[5] Webopedia Online dictionary -http://www.webopedia.com/TERM/I/IP_spoofing.html
Ip Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

[6] SANS Institute – Internet Security Technologies 1.3 (ISBN 0-9724273-6-8)
Book 3, chapter13.

[7] Mindi McDowell - Cyber Security Tip ST04-014 - Avoiding Social Engineering and Phishing Attacks.
http://www.us-cert.gov/cas/tips/ST04-014.html
Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

[8] Sarah Granger - Social Engineering Fundamentals, Part I: Hacker Tactics.
http://www.securityfocus.com/infocus/1527

[9] Radha Gulati - The Threat of Social Engineering and Your Defense Against it - October 31, 2003
http://www.sans.org/rr/papers/index.php?id=1232

[10]Sarah Granger - Social Engineering Fundamentals, Part I: Hacker Tactics.
http://www.securityfocus.com/infocus/1527

[11] Jeremy Quittner – Hacker Psych: Who are Hackers and what makes them tick
http://tlc.discovery.com/convergence/hackers/articles/psych.html

[12][13] National Security Institute
http://nsi.org/SSWebSite/TheService.html

[14] Virus Information definitions - http://www.netguide.com.au/useful_stuff/virus/article2/
This is a program which sits on your computer and waits for a specific date - then "explodes' and usually deletes files or tries to create some sort of havoc. How many viruses spread? Not all the 200 or so new viruses every month get very far. Email is now an easy way for them to spread. For companies receiving large volumes of email, regular updating of anti-virus software and thorough scanning of incoming email are essential steps but still viruses slip through.

[15] WordIQ.com definitions - http://www.wordiq.com/definition/Dumpster_diving
Dumpster diving is the practice of rummaging through trash to find items of use that have been discarded

[16] Kevin Mitnik – My first RSA Conference – April 30th, 2001
http://www.securityfocus.com/news/199

[17] The Bible - 1Corinthians 13:11

Additional Reading material

- Sarah Granger - Social Engineering Fundamentals, Part II: Combat Strategies
  http://online.securityfocus.com/infocus/1533

- David Thompson – The Social Engineering of Security – June 11th, 2001
  http://www.eweek.com/article2/0,4149,118176,00.asp