Global Information Assurance Certification Paper

Jake Evenson
GSEC 1.4b

Abstract

This papers objective was to study the different methods of social engineering and how they can be recognized. The average user may not be paying attention to the guy standing behind him drinking coffee. He doesn't pay any attention to the expired memo reminder he just threw in the trash. When he goes to the bar with his buddies, and he's BSing about work, how much did he say? These things seem like no big deal but the fact is unless you know what to look for you could be pumped for information and not realize it. This study's conclusions indicates steps to defend yourself against social engineering

Social Engineering: A Way Around the Hardware

Introduction

It was a little after 5 o'clock pm on 4th of September 2000 I received a call from an Internet retailer and this is how the call went. "Hello sir, I just wanted to verify this order before we send it out. We are wondering why this orders billing address is in Washington and this order is going to Brownsville Texas." I replied "I haven't ordered anything from you guys!" "Well is your name Jake Evenson, account number xxxx-xx-xx-xxxx?" "That's correct but again; I never ordered anything from you!" The woman replied "well this is getting entirely too common." This order was for $4500.00 and consisted of miscellaneous computer hardware and software.

I couldn't figure out how someone obtained my credit card information and placed this order. After telling my wife what happened, her face turned pale white. "Yesterday someone from MSN popped onto the screen and needed to verify our account information." She said the dialogue box looked like an official MSN page and it said "due to a server glitch we just need to get your account information so your service will not be interrupted." She thought she was doing the right thing. How was she supposed to know, she really doesn't know much about how the internet works. Now if someone went through all the trouble to get a home users information, imagine what is happening in the corporate world.

What is Social Engineering?

Social Engineering: Term used among crackers and samurai for cracking techniques that rely on weaknesses 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 who has the required information and posing as a field service tech or a fellow employee with an urgent access problem.

Source: http://dictionary.reference.com/search?q=Social%20Engineering

The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information. The reasons for gaining access could be to commit fraud, gain access to corporate networks, government espionage, or to steal someone's identity. The hacker might not even want access to your sensitive data, but to wreak havoc on your system or network (Granger).

Typical targets include government installations, large corporations, and financial institutions. A good reason for using social engineering is that most of these networks are protected by state of the art firewall equipment or physical security such as locked doors that require access badges to gain entry. Instead of cracking passwords with Loftcrack or Jack the Ripper, the hacker uses his communication skills to gain access to unauthorized information. Even though a hacker can break their way in, sometimes it's just easier to go through people in the company (Gaudin). It can also be described as pitting your wits up against another human.

Social engineering is the human side of breaking into a corporate network. Companies with authentication processes, firewalls, VPNs and network monitoring software are still wide open to an attack if an employee unwittingly gives away key information in an email, by answering questions over the phone with someone they don't know or even by talking about a project with coworkers at a local pub after hours (Gaudin).

PC and Phone based Social Engineering Examples

Isn't this just a form of hacking? Hacking takes more advantage of holes in security while the social engineering takes advantage of holes in people's common sense (Bernz).

I think the statement above is a great way of distinguishing the difference between hacking and social engineering. There are many methods of PC and phone based social engineering:

- Phreaking
- Trojans
- Viruses
- Pop-ups

Phreaking

/freek'ing/ n. [from `phone phreak'] 1. The art and science of cracking the phone network (so as, for example, to make free long-distance calls). 2. **By extension, security-cracking in any other context (especially, but not exclusively, on communications networks) (see cracking).**

Source: http://dictionary.reference.com/search?q=phreaking

Phreaking is used to access companies in other ways besides computers. They use con games to draw info out of operators. Redboxing[1], and other phreaking techniques can be used to avoid the phone bills while you are on the phone trying to scam passwords. When you are telnetting to a different state it is free, using a phone costs money! Calling and impersonating someone from the IT helpdesk to get someone's password could work something like this:

---

[1] Red boxing, the art of getting free payphone calls by tricking the machine into thinking you inserted money (while you actually just played a tone).

A secretary answers the phone, “Kathy Smith, may I help you?”

“Yes this is Bob Robertson from the information center; we think someone has compromised one of the file servers. Can I talk to the person in charge?”

“Well it’s Friday afternoon and everyone has gone home for the weekend,” Kathy says.

“How’s your day going Kathy?”

“Pretty good, and you?”

A sigh. “Well not so good Kathy, I have a mountain of paperwork, our copier died this morning, and as I said before we think your file server was broken into.”

“How do you know our file server was broken into?”

“Well isn’t your login *ksmith*?”

“Yes”

“We’ve noticed some unusual traffic coming and going from your file server. Are you sure there isn’t anyone there who can help me? I’m afraid while we’re talking right now that someone could be downloading files off your file server. What you could do is log onto the file server and remove the server from the network until one of us can do a thorough investigation.”

“I wouldn’t have any idea how to do that!”

Sigh….’Well I really need to get this server off the network so our sensitive company data isn’t compromised any more than it is right now.” Sigh. “Why didn’t I think of this before! You could just give me your password and I could do it, then after I am done you could change your password.”

Clock says 4:06pm. “Well…I guess.”

“Thanks Kathy, you did the right thing, now please remember to change your password Monday morning.”

Bob Robertson gets access to the network and steals sensitive data as he’s hanging up with Kathy.

Trojans

n 1: a subversive group that supports the enemy and engages in espionage or sabotage; an enemy in your midst [syn: fifth column, Trojan horse]

Source: http://dictionary.reference.com/search?q=trojan%20horse

The Trojan horse was a giant wood horse that was given to their foes as a piece offering. When the Trojans brought the large wooden horse inside their city walls, Greek soldiers snuck out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture the city of Troy[2]. This perfectly describes a Trojan horse you receive via email. You open the gift (email) and you think you are just receiving a file. What you are really receiving is a program that opens a port to hacker to control the infected system. There are three main types of Trojans: Backdoor Trojans, Password Steal Trojans, and just Trojan Horse. Here is a short description of the three.

Backdoor Trojans - These types of Trojans opens a port to allow a hacker control of a system.

Password Steal Trojans - A Trojan horse that gathers and sends some types of passwords.

Trojan Horse - Any other Trojan horse program that does not have backdoor or password-stealing capabilities. These programs can perform various malicious activities, such as deleting files, changing system settings, and running malicious programs (Symantec).

Viruses

n. [from the obvious analogy with biological viruses,
via SF] A cracker program that searches out other programs and
`infects' them by embedding a copy of itself in them, so that they
become Trojan horses. When these programs are executed, the
embedded virus is executed too, thus propagating the `infection'.

Source: http://dictionary.reference.com/search?q=virus

A virus is a program (a piece of executable code) that has the ability to replicate itself (Kolde). Computer viruses are like biological viruses as in they spread very quickly and are sometimes tough to eradicate. They are usually executed by the user by clicking on an email attachment. One example that you may remember is the ILOVEYOU virus that was first discovered on May 4, 2000.

The ILOVEYOU virus was written in relatively simple VBScript and spread via your Outlook address list. One part of the ILOVEYOU virus was the installation of

---

[2] http://www.webopedia.com/TERM/T/Trojan_horse.html

a password grabber. The password grabber was installed by changing the startup page of your web browser to a web page that will attempt to execute a program named WIN-BUGSFIX.exe (Kolde). This was cleverly named to dupe a user into running the program. If you clicked "yes" the password grabber is installed and set to run every time you boot. I was lucky enough not to have opened this email but many of my friends we not so fortunate. The part that's hard to believe is that everyone that was infected with this virus had to install it themselves. This is a form of social engineering by enticing the user to open the email by putting a subject line that is deceiving. Also by asking you if you would like to execute a program named "WIN-BUGSFIX" makes you think that "yes, you are running Windows" and "If it fixes problems in Windows, it is probably ok."

Pop-ups

Just like my story at the start of this paper, someone can come to you acting as an employee to an ISP and get your account information and possibly even your social security number. There are many people that have their son or daughter set them up with a computer so they can have access to the wealth of information on the internet. They have absolutely no idea how it works and they really don't care to know, they just want to chug around and get email. These people are unsuspecting and are an easy target for hackers. When a pop-up box can be made to look very official the average user probably won't realize that it's a scam. When you see the ISPs logo on the pop-up you think it must be official.

Human Based Social Engineering Examples

There are many different methods of human based social engineering. They range from as simple as asking someone straight out for their password to taking the time to befriend someone to gain their trust. Below I will give a little insight to some of the more common human based methods:

- The Direct approach
- Dumpster Diving
- Spying
- Person of Authority
- The New Friend

The Direct Approach

A hacker could directly ask a person for their login and password. Most likely this won't succeed if the person being asked has a little common sense.

Dumpster Diving

Do you ever wonder what happens to all your pay stubs or credit card receipts after you throw them away? Do you think about that memo you received at work yesterday after you tossed it? All these items are considered valuable to a hacker. Most of the time the building you work in or the house you live in has locks on the doors to keep unwanted people out, but what about your garbage can or dumpster at work? There are many valuable items that you can find in the dumpster such as:

- Company phone books;
- Organizational charts;
- Memos;
- Company policy manuals
- Calendars of meetings, events, and vacations;
- System manuals
- Printouts of source code;
- Disks and tapes;
- Company letterhead and memo forms;
- Outdated hardware (especially hard disks)

(Berg)

All of these items could be very dangerous in the wrong hands. Even the garbage can beside your desk could potentially hold login and password information that could be used to access sensitive data. The ability to know and learn names from a corporate phone book can make you sound very convincing to a secretary or IT helpdesk.

Spying

Do you ever feel like someone is looking over your shoulder? That is another method for getting your login and password. When you leave your desk do you lock your PC? Most of the time your login name is always displayed. Now that a potential hacker has your login all he/she needs to do is watch you enter your password and they have a way into the network. The same goes for doors locked with a combination. All it would take is you not paying attention and someone watching over your shoulder and the bad guy is looking through sensitive company data.

Person of Authority

Someone could use intimidation to get you to talk. Someone claiming to be your Commanding Officer calls the IT helpdesk and needs a password for the machine in the conference room because they're giving a presentation to visiting personnel you are most likely going to give that information pretty quickly because it could mean your job!

The New Friend

It could be the guy on your softball team or a co-worker that works in the mailroom. They will befriend you and gain your trust. Most everyone talks about work around your good friends. This method could take a long time unless you can't keep your mouth shut! When that friend starts to nonchalantly probe you for information you probably won't think anything of it. Maybe he's just making conversation? You would like to trust your friends, wouldn't you?

How to Defend Against Social Engineering

Now we can look at some methods to combat social engineering:

- A Security Policy
- Employee Education
- Educate Helpdesk Staff
- Anonymous Hotline
- Limit Access
- Watch What You Say
- Shred Documents
- Strong Password Policy
- Antivirus Software

A Security Policy

Having a security policy that is thorough but also easy to understand is paramount. A security policy that gets too technical is a security policy that never gets read. It should be easy to access and every employee should know how and where to access it. At my place of employment it is posted on the company Intranet. That way when it is updated which is often, a person will know because the link will be highlighted when updated.

This policy should include guidelines for password length and the frequency you need to change your password. At the end of this paper I have included a sample policy outline. It was taken from an article written by William Farnsworth of SANS Institute[i]. This is a great format to modify to fit your needs (SANS).

Employee Education

It doesn't do you any good to have a security policy if you don't educate the employees. Employees should be trained right away when they are hired. They should be quizzed periodically to where the policy is located and who to contact if you suspect someone is digging for information. Employees should also tested by bringing in random people to test security so the employer knows when to freshen their employees awareness.

Educate Your Helpdesk Staff

The helpdesk is there to solve users' problems. Usually this consists of connectivity issues or helping people that get locked out their account by forgetting their password. Most helpdesk staff is not trained on security issues. They are trained to be helpful to their customers and make things as convenient as possible. As a method for confirming who a person is really who they say they are the helpdesk should ask to call the person back at their desk to verify it is a corporate number the customer is calling from.

The helpdesk staff should also feel that if the call sounds shady that they can request a supervisor call for verification. They should not fear the loss of their job because they didn't give a password to a person that makes them uneasy. The helpdesk staff should feel that they are protected.

A Secure Anonymous Hotline

No one likes to be a tattle tale. "What if I'm wrong? I don't want to get the guy in trouble over nothing." If you have an anonymous hotline you can report the suspicious activity discretely. Make sure your employees know that there is no harm in reporting things that may be false alarms.

Limit Access

People should only have access to what is essential to do their job. A person in the engineering department doesn't need access to finance documents. Working for the government you are issued a badge that has your picture on the front with an employee number. The back has a magnetic strip that is coded with different door access points. You only have access to the spaces you need to do your job. This type of badge system is used in other corporations other than the government and should be implemented anywhere sensitive data resides. If people see someone they don't recognize they should stop the person discretely and ask for identification.

Watch What You Say

Have some common sense. Don't bring your work home with you. If you tell your wife or husband about work they may tell a friend not thinking it's a big deal. A potential hacker may befriend your wife or husband to seek information.

Shred Documents

Any documents you throw out make sure they go through a cross cut shredder. Using a straight-cut shredder, you still run the risk of someone putting that document back together. Sounds far fetched but with the right patients anything can be done. There are also DOD approved and NSA approved shredders that really cut up the paper making it almost impossible to reconstruct the paper.

A Strong Password Policy

It's good to enforce a strong password policy. They are harder for someone looking over your shoulder to memorize. People usually set their password to a pet's name or something else that's easy for a person to guess. Also making the user change their password every three months and no re-using of old passwords so the user doesn't just re-enter the old password when it is time to change it. Also don't use the same password for everything you do. Once someone figures out one of your passwords they will try that password everywhere. This is especially bad where you can RAS in to your corporate servers from a remote location, because this totally bypasses your firewall.

Antivirus Software

Running virus scanning software such as McAfee or Norton Anti-virus will help catch those Trojans that are so cleverly hidden in your downloads. Anti-virus software is only effective if the user keeps it updated religiously. The virus definitions change on a daily basis so maintenance is imperative.

Conclusion

Social Engineering will always be a very powerful tool. Businesses will always be trying to get a leg up on one another; foreign countries will use Social Engineering to gain intelligence against its neighbors. With the proper training you should know the signs to look for and steps to take if you suspect espionage. If something seems fishy, it probably is.

As a home user, you can use the same methods to protect yourself. And for some of us, we end up learning the hard way. Just use common sense and be aware that just because your computer is not hooked up to the net doesn't mean that your information is safe.

---

[i]

Sample Security Policy Outline

1. Introduction

1.1.1General Information
1.1.2 Objectives

1.2 Responsible Organizational Structure

1.2.1.1.1 Corporate Information Services
1.2.1.1.2 Business Unit Information Services
1.2.1.1.3 International Organizations
1.2.1.1.4 Tenants

1.2.2 Security Standards

1.2.2.1.1 Confidentiality
1.2.2.1.2 Integrity
1.2.2.1.3 Authorization
1.2.2.1.4 Access
1.2.2.1.5 Appropriate Use
1.2.2.1.6 Employee Privacy

2. Domain Services

2.1.1 Authentication
2.1.2 Password Standards
2.1.3 Resident Personnel Departure

2.1.3.1.1 Friendly Terms
2.1.3.1.2 Unfriendly Terms

3. Email Systems

3.1.1 Authentication
3.1.2 Intrusion Protection
3.1.3 Physical Access
3.1.4 Backups
3.1.5 Retention Policy
3.1.6 Auditing

4. WEB Servers

4.1.1 Internal
4.1.2 External

5. Data Center

5.1.1 Authentication
5.1.2 Intrusion Protection
5.1.3 Physical Access
5.1.4 Backups
5.1.5 Retention Policy
5.1.6 Auditing
5.1.7 Disaster Recovery

6. LAN/WAN

6.1.1 Authentication
6.1.2 Intrusion Protection
6.1.3 Physical Access

6.1.3.1.1 Modems
6.1.3.1.2 Dial-in Access
6.1.3.1.3 Dial-out

6.1.4 Backups
6.1.5 Retention Policy
6.1.6 Content Filtering
6.1.7 Auditing
6.1.8 Disaster Recovery

6.1.8.1.1 Network Operations Center
6.1.8.1.2 Physical Network Layer

7. Desktop Systems

7.1.1 Authentication
7.1.2 Intrusion Protection
7.1.3 Physical Access
7.1.4 Backups
7.1.5 Auditing
7.1.6 Disaster Recovery

8. Telecommunication Systems

8.1.1 Authentication
8.1.2 Intrusion Protection
8.1.3 Physical Access
8.1.4 Auditing
8.1.5 Backups
8.1.6 Retention Policy
8.1.7 Disaster Recovery

9. Strategic Servers

9.1.1 Authentication
9.1.2 Intrusion Protection
9.1.3 Physical Access
9.1.4 Backups
9.1.5 Retention Policy
9.1.6 Auditing
9.1.7 Disaster Recovery

10. Legacy Systems

10.1.1 Authentication

10.1.1.1.1 Password Standards

10.1.2 Intrusion Protection
10.1.3 Physical Access
10.1.4 Backups
10.1.5 Retention Policy
10.1.6 Auditing
10.1.7 Disaster Recovery

11. Security Services and Procedures

11.1 Auditing
11.2 Monitoring

List of References

Author Unknown. “ILOVEYOU.” March 9, 2003
URL:http://www.webkorner.com/support/warnings/iloveyou.htm

Author Unknown. “Social Engineering”
URL:http://onlinesecurity.virtualave.net/hacking/social.htm

Author Unknown. “Social engineering: examples and countermeasures from the real-world.” November 1999 URL:http://www.gocsi.com/soceng.htm

Berg, Al. “Cracking a Social Engineer”
URL:http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html

Bernz. “Bernz’s Social Engineering Intro and Stuff”
URL:http://packetstorm.decepticons.org/docs/social-engineering/socintro.html

Bernz. ”THE COMPLETE SOCIAL ENGINEERING FAQ!”
URL:http://packetstorm.decepticons.org/docs/social-engineering/socialen.txt

Cave, Richard. “Trojan Horse.” March 4, 2003.
URL:http://securityresponse.symantec.com/avcenter/venc/data/trojan.horse.html

Gaudin, Sharon. “Social Engineering: The Human Side Of Hacking.” May 10, 2002 URL:http://cin.earthweb.com/reports/article.php/11050_1040881

Kolde, Jennifer. (2002). “Security Essentials day III.” SANS Institute

SANS Institute. “What Do I Put in a Security Policy?”
URL:http://secinf.net/info/policy/policy.htm

Stevens, George. “Enhancing Defenses Against Social Engineering.” March 26, 2001 URL:http://www.sans.org/rr/social/defense_social.php
Tims, Rick. “Social Engineering: Policies and Education a Must.” SANS Institute

---

URL: http://www.sans.org/infosecFAQ/social/policies.htm