Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

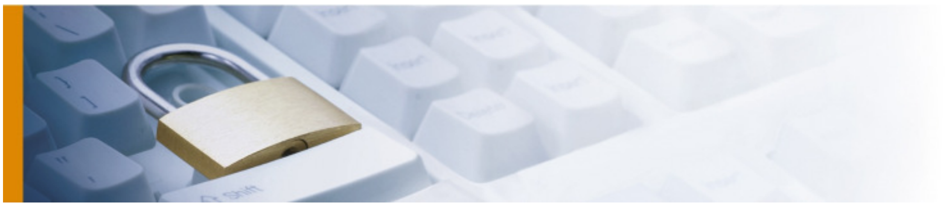
T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

# Social Engineering

# Test Cases

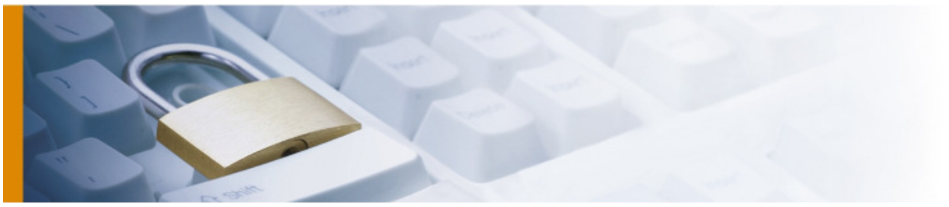
# June 9th, 2009

| | |
|---|---|
| Document Name: | Social_Engineering_V2.0.docx |
| Version: | v2.0 |
| Project Number: | 80XXX |
| Author(s): | Ivan Buetler, Compass Security AG |
| Date of Delivery: | June 9th, 2009 |
| Classification: | PUBLIC |



# Social Engineering – Test Cases – v2.0

## Table of Content



# 1 Social Engineering

"The best way to obtain information in a social engineering attack is just to be friendly"

## 1.1 Abstract

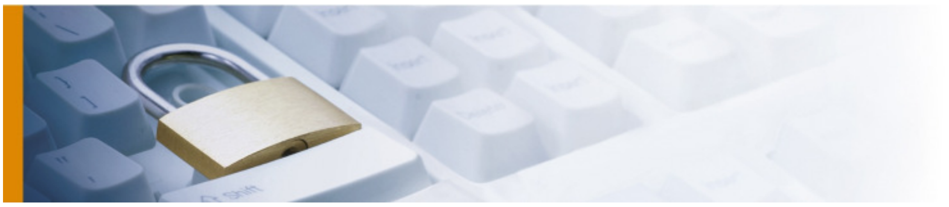
One morning a few months back, a stranger walked into a Swiss Bank and walked out later having access to the entire corporate network. How was it done? By obtaining small amounts of information, bit by bit, from a number of different employees. First, he did research about the company for two days before even attempting to set foot on the premises. For example, he learned key employees' names by calling HR. Next, at the front-door he pretended to service the companies Lexmark printers, and the front-desk allowed him to access the building. When entering the third floor secured area, he had "lost" his identity badge, smiled, and a friendly employee opened the door. Once at the Lexmark printer, a wireless access point was placed on the local network. Thus, leaving the internal network to be accessed from the street, where some more criminals were waiting gain access to the internal network. From there, they used common network hacking tools to elevate privileges and to gain super-user access on critical system.

Most people consider "Social Engineering" as a criminal minds use of psychological tricks on legitimate users of the target computer system. In order to obtain information, an attacker needs to gain access to the system. The one thing that everyone seems to agree upon is that social engineering is generally an attacker's clever manipulation of the natural human trust. The goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.

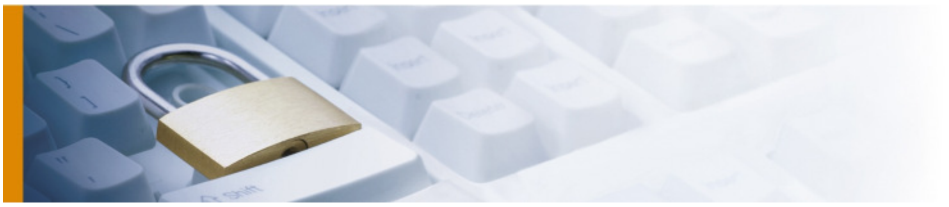
Security is all about trust. Trust in protection and authenticity. Generally agreed upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to social engineering attacks. Many experienced security experts emphasize this fact. No matter how many articles have been published about network holes, patches and firewalls, we can only reduce the threat. After that, it is up to the employees to keep the corporate network secured.

## 1.2 Types of Social Engineering

| Type | Description |
|---|---|
| Phone | The most prevalent type of social engineering attack is conducted by phone. An attacker will call up and imitate someone in a position of authority or relevance and gradually pull information out of the user. Help desks are particularly prone to this type of attack. |
| Dumpster Diving | Dumpster diving, also known as trashing, is another popular method of social engineering. A huge amount of information can be collected through company dumpsters. The LAN Times listed the following trash items as potential security leaks sh: "company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware." |



| Type | Description |
|---|---|
| Phishing | The Internet is fertile ground for social engineers looking to harvest passwords. The primary weakness is that many users often repeat the use of a single simple password on multiple accounts: Yahoo, eBay, Google, Linkedin, MySpace, whatever. Once the attacker has a password, then he or she can probably get into multiple accounts. Phishing is a technique to fraudulently obtain private information.<br>One way in which attackers have been known to obtain this kind of password is through faked on-line forms. They can send out some sort of sweepstakes information and ask the user to put in a username and password or requesting "urgent verification" of information and warn of some dire consequence if it is not provided. The message to hook up victims usually contains a link to a fraudulent web page that seems legitimate — designed in the corporate identity — and has a form requesting everything needed by the attackers. |
| Drive-by Infection | Web downloads of manipulated and executable files pose a high risks Victims are visiting malware pages because they sound so promising. Once they hit such a malware page, a Trojan horse will be downloaded and executed<br>a) Unintentionally (by exploiting a 0-day exploit of the browser)<br>b) Intentionally (by letting the user to confirm the security dialog)<br>Example of downloadable files:<br>“ Fake anti-virus product<br>“ Fake malware cleaner |
| E-Mail Infection | E-mail can also be used for more direct means of gaining access to a system. For instance, mail attachments sent from someone of authenticity can carry viruses, worms and Trojan horses. A good example of this is the AOL hack. In that case, the attacker called AOL's tech support and spoke with the support person for an hour. During the conversation, the attacker mentioned that his car was for sale cheaply. The tech supporter was interested, so the attacker sent an e-mail attachment with a picture of the car. Instead of a car photo, the mail executed an exploit that created a backdoor connection out from AOL through the firewall. This allowed the attacker to remote control its victim. |
| Baiting | In this attack, the attacker leaves a malware infected floppy disc, CD ROM, or USB flash drive in a location sure to be found (bathroom, elevator, sidewalk, parking lot, company canteen), gives it a legitimate looking label, and simply waits for the victim to insert the device into its computer.<br>For example, an attacker might create a disk featuring a corporate logo, readily available off the target's web site, and write "Executive Salary Summary Q2" on the front. The attacker would then leave the disk on the floor of an elevator or somewhere in the lobby of the targeted company. Unknowing employees might find it and subsequently insert the disk into a computer to satisfy their curiosity. |

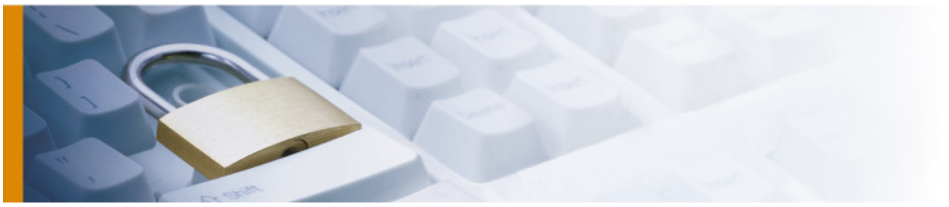


| Type | Description |
|---|---|
| | The consequence of inserting a malicious disk into a computer to see the contents will result in malware installation. It is very likely giving an attacker full access to the victim's PC and perhaps, the targeted company's internal network infrastructure.<br>Unless computer controls block the infection, PCs set to "auto-run" inserted media may be compromised as soon as a rogue disk is inserted. Due to anti-virus products are based on the detection of known malicious patterns . Thus, anti-vrus software cannot detect malicious software as long it is written for a specific attack. |
| Impersonation | Impersonation generally means creating some sort of character and playing out the role. Some common roles that may be played in impersonation attacks include: a repairman, IT support, a manager, a trusted third party or a fellow employee. In a huge company, this is not that hard to do. There is no way to know everyone - IDs can be faked. |
| Reverse Social Engineering | A final, more advanced method of gaining illicit information is known as "reverse social engineering". This is when the attacker creates a persona that appears to be in a position of authority so that employees will ask him for information, rather than the other way around. If researched, planned and executed well, reverse social engineering attacks may offer the attacker an even better chance of obtaining valuable data from employees. However, this requires a great deal of preparation, research, and pre-hacking to pull off. |

## 1.3 Compass Security Social Engineering Test Cases

### 1.3.1 Phishing

| Item | Description |
|---|---|
| Preparation | Create a web page that looks promising to the target. The web page has some sort of form-based authentication. |
| Social Engineering Type | “ Phishing |
| Webpage Types | The fake webpage is<br>“ A clone/copy of the victim's web page (SSLVPN, Login forms)<br>“ Reverse proxy to the real victim's real web page<br>“ Independent web page (not related to any victim web page) |
| Attraction | The victim shall be attracted by<br>“ E-Mail<br>“ Letter<br>“ Blogs/Boards on the victim web page |
| Bad Behavior | The victim visits the malicious web page and enters his/her credentials |
| Good Behavior | The victim will not enter any data and will inform the local security team |
| Measurement | Log files containing phished credentials |
| Alternatives | The web page could be a<br>“ E-Banking system (login)<br>“ Portal application (login)<br>“ SSL VPN solution (login)<br>“ Remote Mail (login)<br>“ Fake Windows lock screen (login)<br><br>Anything that starts with a web page |



### 1.3.2 Malicious Web Download

| Item | Description |
|---|---|
| Preparation | Create a web page that looks promising to the target and contains some sort of useful downloadable files. |
| Social Engineering Type | “ Phishing |
| Malware Type | “ Windows Executable<br>“ Windows Batch File<br>“ Windows Office Macro Files<br>“ Plattform independent Java Programms |
| Malware Functionality | The malware may contain the following functionality<br>“ Send recent docs via e-mail smtp host<br>“ Send recent docs via Outlook API<br>“ Write local log entry<br>“ Open inside-out tunnel to Compass (IE post, DNS, direct) |
| Attraction | The victim shall be attracted by<br>“ E-Mail<br>“ Letter<br>“ Blogs/Boards on the victim web page |
| Bad Behavior | The victim will download and execute the file |
| Good Behavior | The victim shall not download and execute the executables |
| Measurement | How to measure?<br>“ Collect log files<br>“ List e-mails received by the sendmail Trojan horse functionality<br>“ List covert-channels (dns, ie) |
| Alternatives | Java Scripts popup message alerts the user of known viruses found on his/her computer and the opportunity to download a free cleaner (virus). |

### 1.3.3 Fileserver Trojan Horses

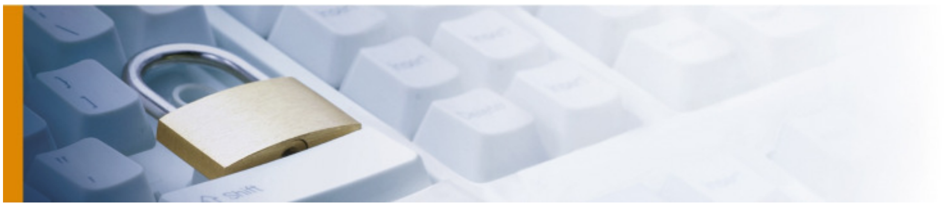
| Item | Description |
|---|---|
| Preparation | Save a test Trojan horse on a common network share within the corporate network where most of the users have access. Make sure the Trojan is not removable by the majority of the victims. Send a promising e-mail to a list of victims including the path to the file. |
| Social Engineering Type | “ Baiting |
| Malware Type | “ Windows Executable |
| Malware Functionality | The malware has the following functionality<br>“ Write local log entry |
| Attraction | The victim shall be attracted by<br>“ E-Mail |
| Bad Behavior | The victim executes the Trojan horse application |
| Good Behavior | The victim will not belief the e-mail and notify the local security group |
| Measurement | “ Collect log files |

### 1.3.4 Malicious Post Mail

| Item | Description |
|---|---|
| Preparation | Create an out-of-band Trojan/Malware and send it to a list of recipients (HR department, marketing)<br>“ USB stick<br>“ CD/DVD |
| Social Engineering Type | “ Baiting |
| Malware Type | “ Windows Executeable |
| Malware Functionality | The malware has the following foreground functionality<br>“ Trojan starts a Power Point slide<br>“ Trojan prints a file corrupt error messages<br>“ Trojan installs a useful open-source tool (e.g. disk-cleaner; admin privs required)<br>“ Trojan is just silent (nothing happens the use could see)<br><br>The malware has the following background functionality<br>“ Send recent docs via e-mail smtp host<br>“ Send recent docs via Outlook API<br>“ Write local log entry<br>“ Open inside-out tunnel to Compass (IE post, DNS, direct) |
| Attraction | The victim shall be attracted by<br>“ Letter |
| Bad Behavior | The victim is inserting the malicious device |
| Good Behavior | The victim shall not use the malicious device |
| Measurement | How to measure?<br>“ Collect log files after the exercise by the client<br>“ List e-mails received by the sendmail Trojan<br>“ List covert-channels (dns, ie) |

### 1.3.5 Impersonation

| Item | Description |
|---|---|
| Preparation | Find out the printer vendor of the victim. Impersonate the printer service center that wants to do the annual service. Call prior arrival to have an appointment. This social engineering case requires physical access on-site. |
| Social Engineering Type | “ Impersonation |
| Malware Type | “ WLAN access point installation |
| Malware Functionality | The WLAN access point does not implement malware functionality itself. Furthermore, it will give other penetration testers access to the victim's corporate network. |
| Attraction | The victim shall be attracted by<br>“ Phone call<br>“ E-Mail<br>“ Letter<br>“ Blogs/Boards on the victim web page |
| Bad Behavior | The victim is willing to let the service staff member into the building |
| Good Behavior | The victim is asking for a valid identification card and invitation. The attacker is concurrently supervised from an employee from the victim staff. |
| Measurement | How to measure?<br>“ Photos from within the company building<br>“ Proof stickers<br>“ Network scan results |
| Alternatives | Walk to the entry lobby of the victim's building by carrying a large flower / pizza box. Go without an appointment. |



# 2 Appendix

## 2.1 References

| Link | Details |
|---|---|
| http://www.securityfocus.com/infocus/1527 | Social Engineering Fundamentals, Part I: Hacker Tactics<br>by Sarah Granger<br>last updated December 18, 2001 |
| http://en.wikipedia.org/wiki/Social_engineering_(security) | Wikipedia |
| http://news.cnet.com/8301-1009_3-9995253-83.html | YouTube Live Social Engineering Videos |