The psychology of Social Engineering

- Elicitation (teasing information out of somebody)
- Framing (politicians are very good at this: they are asked a question, but they respond to it by building a frame about something else, completely ignoring the question).
- Pretexting (pretext - password reset over the phone, in a hurry, because of a report that the boss needs)
- Cold Calling

We find SE in any aspect of our lives, and not just hackers or professionals.

Bypassing physical security:

- technology cannot solve the problem
- post exploitation
- binary evasion

Social Engineering Tools:

- CEWL , CUPP, CREEPY, DRADIS, GOOGLE
- KALI LINUX, MALTEGO, RECON-NG FRAMEWORK, SCYTHE FRAMEWORK, SHODAN, SOCIAL ENGINEERING TOOLKIT (SET)

What you will learn?

- Various social engineering techniques and tools
- Proven ways to communicate
- Experience will reinforce methodology
- Let's do some labs!

What is social engineering?

The art of getting information from people, having them carry out activities, disclosing sensitive information and more, all through manipulation!

A psychological means to a technical end...

- the fundamental problem is the human problem
- understanding assumed/presumed culture, heritage and upbringing is key

The Social Engineer

In this lesson, Subject Matter Expert Dean Pompilio defines the Social Engineer as someone who influences people to take actions that may not be in their best interest.

You will learn that intrusion by a Social Engineer relies on:

- psychological manipulation
- facial expression
- body language
- misdirection
- emotional highjacking

The SME discusses why SE is performed and describes SE attacks: how and where attacks are used, who does them, how people respond, and how they result in 100 percent success in physical breaches. You will learn about categories of Social Engineers, who the “natural” Social Engineers are, and what a Social Engineer’s goals are (detailed below).

Categories of Social Engineers

- average citizens
- governments
- recruiters
- posers and scam artists
- disgruntled employees
- identity thieves
- spies
- penetration testers
- hackers

“Natural” Social Engineers

- children
- job seekers
- bar patrons
- sales and marketing personnel
- interrogators
- polygraphists

Goals of a Social Engineer

- entertainment
- ego gratification
- entrance into or enhanced status within a social group
- knowledge
- power

- social cause
- money

Social Engineering Attacks:

- Used in a high percentage of attacks by hackers, hacktivist, and nation states
- most people that are asked will provide the spelling of their names and their email addresses without confirming the identity of the person asking the questions
- many people will give out social security numbers, birth dates or employee numbers
- 100% success ratio in physical breaches

Why is Social Engineering performed?

- software vulnerability discovery and exploitation is non-trivial
- defense is many-to-many
- offense is one-to-many
- a path of least resistance
- Why not?

Exploitation Life-Cycle

In this lesson, Subject Matter Expert Dean Pompilio discusses how the exploitation life-cycle is used to carry out the goals of hacking.

The SME presents the five phases of the exploitation lifecycle:

- reconnaissance (digital information gathering, network lookups, traceroutes, social engineering)
- scanning (port scanning, OS identification, social engineering?)
- gaining access (SE: phishing, spear-phishing, whaling), Watering hole (infecting sites well knows to victims), USB drop (bars &clubs, coffee shops, universities)
- maintaining access (stealthy, persistent software/hardware implant, rootkits & backdoors, adding a firewall exception, SE?)
- clearing tracks (deleting logs, disabling auditing, SE?)

You will learn the tools and methods used by hackers and Social Engineers to successfully carry out each of the five phases with the aim of gaining unauthorized access to sensitive and confidential data and information about a person, company, organization, or government entity.

Social Engineering Techniques

In this lesson, Subject Matter Expert Dean Pompilio discusses social engineering techniques that are used to manipulate people into giving out sensitive information or performing in certain ways that allow attackers to be more successful with less effort when hacking computers or stealing information.

This lesson covers the following techniques:

- Dumpster diving
- Impersonation
- Shoulder surfing
- Making malicious copies of legitimate Web sites
- Phishing
- Making a malicious copy of an Interactive Voice Response (IVR) system
- Baiting
- Quid pro quo
- Tailgating (also known as Piggybacking)

You will learn where you can legally dumpster dive, how effective impersonation can be, where shoulder surfing can be done, and how malicious copies of Web sites or IVRs can be used to obtain sensitive information. SME Pompilio discusses the differences between phishing, spearfishing, and whaling and how baiting is done with iUSB flash drives infected with malware that runs with the autorun or autoplay function when the flash drive is inserted into a victim's computer.

This lesson covers the techniques of quid prop quo – where the attacker convinces the victim that they are each doing a favor for the other person – and tailgating, which is also known as piggybacking. An attacker uses tailgating to enter a building by surreptitiously joining a group that has legitimate entry to the building. This technique also can be carried out by dressing as a technician or delivery person to gain entrance or by impersonating someone who genuinely works in the building.

Phishing:

- obtaining private information via email
- email appears to come from legitimate business/person
- email contains malicious attachment
- email contains link to fraudulent web page that appears legitimate (spear phishing, whaling)

Interactive Voice Response (IVR):

- recreate a legitimate-sound copy of an institutions IVR system
- prompt victim with phishing email to verify information using fraudulent IVR

Baiting:

- drop USB flash drive with intriguing label in highly trafficked area
- victim inserts drive and is infected with malware via autorun or autoplay

Quid Pro Quo:

- cold call as technical support in hopes of reaching a person with significant problem
- victim discloses private information and or installs malware

Tailgating:

- attacker looks legitimate and this is allowed to walk behind the person with legitimate access to enter restricted area
- attacker may fake the action of presenting or once knowing or owning an identity token

Demos

In this lesson, Subject Matter Expert Dean Pompilio discusses the demonstrations that he will carry out in this course of the tools used by Social Engineers. The demonstrations will be done within the Kali Linux environment and will use the built-in Dradis tool. SME Pompilio goes through the menu system, how to download, and how to build your own virtual machine.

The tools used are generally used for report generating and for gathering and organizing documents. Dradis lets you use a self-contained Web site to organize your information as you gather it. It is a very useful tool for creating folders, adding notes, and adding attachments. You will be replicating the demonstrations in your own Kali environment.

- Kali Linux
- Dradis

Kali Lab

In this demonstration, Subject Matter Expert Dean Pompilio presents a basic, high-level overview of Kali Linux. He discusses what is involved in the different aspects of data gathering, digital information gathering, and electronic methods used to socially engineer someone. This first lab* explores Kali Linux, which will be used for most of the demos in this course.

During this lab, you will learn to use the private StartPage search engine that does not track your email address, being mindful of the digital breadcrumbs you leave behind. You also will learn:

- How to access the Kali Web site (kali.org)
- How to use Kali as your penetration testing platform

- How to download depending on your needs
- How to easily boot Kali
- The links for VMWare and VirtualBOX images
- About using a VM Ware player or workstation to create a new virtual machine
- How to boot up a virtual machine
- How to configure your virtual machine
- About command shell basics
- About using CTRL-SHIFT-T
- About the IceWeasel browser

SME Pompilio discusses a useful Web site for people new to Kali: tools.kali.org. You can use this Web site to

- Learn about and how to use the Kali tools
- Learn about and how to use the menu system (especially the Kali Linux menu)
- Learn about the top ten security tools

In this lab, SME Pompilio shows you how and how often to keep your instance of Kali on your virtual machine always updated, and he discusses updating the tools separately.

Dradis Lab

In this lab, Subject Matter Expert Dean Pompilio discusses **Dradis**, a useful tool for **gathering information and generating reports on that information**. Dradis is a self- contained Web application that is a repository for gathering and organizing all your information. It is very simple to use and to configure to organize output from scans and word lists for password cracking and to attach files to a folder for a particular project. SME Pompilio stresses that life is a lot easier when you are organized, and good organization leads to fewer mistakes.

This demonstration shows you how to:

- access the Kali Web site
- choose the reporting tools you will use, including Dradis
- explore other options besides Dradis

Google Hacking

In this lesson, Subject Matter Expert Dean Pompilio introduces Social Engineering tools such as Google hacking. Google hacking techniques allow you to narrow search results considerably to give answers more quickly and to reduce noise and narrow results when performing a search. Can also use these tools on other search engines.

You will learn about:

- using special syntax to narrow your search results
- using the link command to return pages that link to a specified URL
- cache searching for deleted pages
- using archive.org (the “wayback machine”)
- finding related links using operators
- using search texts to find what you are looking for

SME Pompilio also discusses valuable resources to use: 1) the dorks section of www.exploitdb.com and 2) hackersforcharity.org, the Google hacking database.

The next three lessons will present overview demonstrations of using Google hacking to save time; Maltego, which allows you to gather information about an organization and then make connections between those pieces of information; and the Recon-NG framework.

Syntax: link: , cache: , related: , http://www.exploit-db.com/google-dorks/

Information Gathering Labs: Google hacking, Maltego, Recon-NG.

Google Hacking Lab

In this lab, Subject Matter Expert Dean Pompilio discusses Google hacking techniques and presents an introduction to some of the things you can do when gathering information for a Social Engineering audit.

SME Pompilio discusses how to use Google specifically to do targeted searches. (Although this demonstration refers to the search engine Google, the search engine StartPage may be a better choice for a search engine for privacy purposes).

A review of the various search operators and their uses covers the following:

- main search operators such as sites and links
- related search operators
- special search operators such as info and cached
- use of the advanced search function page

SME Pompilio presents several examples of how to obtain confidential information about a target when you want to find some vulnerability information about a Web site, or you want to reveal a site’s debugging information. A Social Engineer can search for vulnerabilities of information that should not be available on the public Internet.

There is a considerable amount of confidential information that is available deep in the public Internet that a target probably does not know is available and that will allow you to dig deeper into the environment in which the target company operates; you will learn more info about the company’s systems, applications, and people.

It is suggested that Social Engineers should spend time on exploitdb.com to have access to a large database of exploits organized by category. There also are more than one thousand security papers on this site that can be accessed to further your knowledge and increase your skill set. (This is the site that Dean Pompilio used to present the examples in this demonstration).

SME Pompilio also presents other aspects of Google hacking that will allow you to get the code of a page through Google without going directly to the Web page, and he discusses Google Dork, which is a preformatted search string that identifies systems that have too much information available on the public internet.

https://support.google.com/websearch/answer/2466433?hl=en

Look for the car, not the animal:

ex: jaguar speed - car

Add an asterisk as a placeholder for any unknown or wildcard terms:

"a * saved is a * earned"

Search Operators:

`site:`	Get results from certain sites or domains. Example: `olympics site:nbc.com` To get results from multiple sites or domains, combine with `OR`. Example: `Olympics site:nbc.com OR site:.gov`
`related:`	Find sites that are similar to a web address you already know. Example: `related:time.com`
`OR`	Find pages that might use one of several words. Example: `marathon OR race`
`info:`	Get information about a web address, including the cached version of the page, similar pages, and pages that link to the site. Example: `info:google.com`
`cache:`	See what a page looks like the last time Google visited the site. Example: `cache:washington.edu`

http://www.googleguide.com/advanced_operators_reference.html

Examples:

inurl:citrix/metaframeXP

site: edu|org + inurl:"faculty_login.asp| .php"

site: .edu|org + inurl:"faculty_login.asp | .php"

intitle:"Index of" intext:"iCloud Photos" OR intext:"My Photo Stream" OR intext:"Camera Roll"

intitle:"Index of" "DCIM"

inurl:CrazyWWWBoard.cgi intext:"detailed debugging information"

intitle:"Retina Report" "CONFIDENTIAL INFORMATION"

Maltego Lab

In this lab, Subject Matter Expert Dean Pompilio demonstrates **Maltego** for Kali Linux. (Maltego also can be installed on Windows systems). This tool allows you to visualize the relationships between and among various bits of information, which Maltego calls entities, that you discover about the target of a Social Engineering Audit.

SME Pompilio gives an example that demonstrates the various ways you can run “transforms” of the known entities about your target. The entities are connected and displayed on a graph.

There is a discussion of the various available layouts, the various modes, how things are color-coded, changing size from the default, and other options for viewing your data that are useful for organizing your data.

SME Pompilio demonstrates how to transform email address from the specific domains discovered for the Social Engineering Audit target. Then he does a search for various categories of information to filter his data. He then runs a transform of the various email addresses to uncover other emails and other profiles on other social networking sites. He then can run other transforms to correlate all the data in various ways.

Various free and paid plug-ins are available for Maltego that enhance its basic features.

Run **Maltego**. Services@coronacomputers.com email used to register.

Recon – NG Lab

In this lab, Subject Matter Expert Dean Pompilio provides an introduction to **Recon-NG**, which is an interesting framework similar to Metasploit. Recon-NG is used for gathering information that is accessed through the Kali Tools Web site. It is already built into Kali, so there is no need to worry about launching it.

SME Pompilio demonstrates how to launch a command shell to use the tool. He shows how to create a workspace to keep data organized, and he demonstrates an Interesting feature of Recon-NG: the "no check" feature that turns off version checking to avoid flagging errors because of lack of updating.

There are lots of options inside the tool. SME Pompilio discusses and demonstrates the following:

- creating and using a workspace — you can create workspaces to organize your activities on a case-by-case basis, which increases the tool's functionality
- how to show modules by running the Show Command (he recommends that you try all of the modules separately to learn a great deal about your target)
- using the netcraft command
- using the run command
- using the load command
- using the resolve command
- using the add and delete commands to configure lists

Examples are given of using different modules to get information and to narrow it to reflect what you are looking for. You can look for sites that have interesting types of files — such as a robots.txt file — to narrow your list of targets for a Social Engineering audit. There is a discussion of the importance of having permission to use a tool like this and of knowing that some services are paid services.

SME Pompilio looks at possible types of reports generated by using the available options and shows the various exporting options.

Example:

```
cd /usr/share/recon-ng/
./recon-ng  --help
./recon-ng --no-check
workspaces select target-company.com
show modules
use netcraft
set source coronacomputers.com
run
set SOURCE cnn.com
run
```

```
use ip
use resolve
use recon/hosts-hosts/resolve
run
use discovery/info_disclosure/interesting_files
run
use ipin
run
set source cnn.com
run
use pgp
show contacts
show hosts
del contacts 1-12
use pwn
use recon/contacts-credentials/pwnedlist
run
show credentials
run
use html
show options
set CREATOR AKset CUSTOMER coronacomputers.com
run
```

#####

Targeting

In this lab, Subject Matter Expert Dean Pompilio discusses targeting techniques. Targeting techniques allow you to gather information about a target in an active way (that may be noticed by the target) or in a passive way using public sources (that may not be noticed by the target). He explains that targeting efforts need to be personal and custom crafted so that your efforts are not given away by sounding scripted when you attempt to elicit information from your target. SME Pompilio also discusses using a quid pro quo approach in which you determine what will motivate the target to help you and then you create an incentive for the target to help you.

The following targeting labs will be presented in the remaining Parts of this Module:

- Spearfishing with the Social Engineering Toolkit – this is built into Kali
- Cupp – which is the Common User Password Profiler
- Cewl – which allows you to crawl a Web site and look for clues

- Shodan – which is a search engine that lets you explore the Internet of things and the IP address space of your target
- Scythe – which is a user name enumeration tool
- Creepy – which lets you look at sites such as Twitter, Google Plus, and Flickr to find out what your target is using these web sites for and to get time stamps of your target's activities

Information Gathering is Key!

Make it personal:

- show depth
- be authentic
- provide incentive for revealing information

Toolkit Lab

In this lab, Subject Matter Expert Dean Pompilio demonstrates the **Social Engineering Toolkit (SE Toolkit)** that is built into Kali Linux and can be found by going to the Kali Linux Application Menu or by launching a command shell and going to User Share.

In this Part of Module 4 you will learn how to

- run the SE Toolkit
- trick your target into signing into a malicious Web site so that you can obtain their credentials
- use Web site attack factors
- perform SE attacks such as spearfishing
- trick your target into providing credentials by using the credential harvester
- use the tab nabbing tool
- use CTRL-SHIFT-T to open a new tab in your browser
- use the various templates
- choose the proper Web server for your activity
- clone a Web site to use to trick your target
- use the tiny URL Web site to streamline your process
- understand the security risks of using the tiny URL Web site
- communicate with your target to trigger them to go to the cloned Web site
- authenticate to the target's true Web site using their own credentials

Steps in SET:

two, three, one, your IP, two
-use tinyurl site to obscure your site/link before you send to user!!-then check in the html folder, with:

more harvester*
-to see harvested credentials for google.com or whatever site account!!!

Cupp Lab

In this lab, Subject Matter Expert Dean Pompilio demonstrates Cupp (Common User Password Profiler), which is an information gathering tool that you can get from GitHub.com. Enter CUPP into the site's search feature and choose MEBUS/Cupp from the choices returned. This tool allows you to generate a list of possible passwords to use in the Dictionary file. The Dictionary file(s) can be expanded as more information is gathered.

In this Part of Module 4, SME Pompilio demonstrates using Cupp to generate password word lists for a Cupp Dictionary. You will learn to:

- open the command shell USER SHARE
- work in interactive mode
- improve an existing Dictionary
- download a Dictionary
- generate a password word list for a Dictionary by answering questions about the target
- understand the various modes in Cupp
- evaluate the password word list generated by Cupp
- use another tool to save your output as a Rainbow Table

SME Pompilio reviews the config file and discusses the various modes, parameters, repositories, and default settings you can use.

```
Usage: cupp.py [OPTIONS]

    -h      this menu

    -i      Interactive questions for user password profiling

    -w      Use this option to profile existing dictionary,
            or WyD.pl output to make some pwnsauce :)

    -l      Download huge wordlists from repository

    -a      Parse default usernames and passwords directly from Alecto DB.
            Project Alecto uses purified databases of Phenoelit and CIRT which where merged and
enhanced.

    -v      Version of the program
```

#########

```
apt-get install cupp

root@kali:/usr/share/cupp# ./cupp.py -l

> Enter number: 3
> Enter number: 32
> Enter number: 29
```

- this is the rule based attack, which means you answer questions about the target and create a dictionary.

```
root@kali:/usr/share/cupp# ./cupp.py -i

[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: jim
> Surname: smith
> Nickname: jimmy
> Birthdate (DDMMYYYY): 07041980


> Partners) name: sue
> Partners) nickname: susie
> Partners) birthdate (DDMMYYYY): 12251980


> Child's name: bill
> Child's nickname: billy
> Child's birthdate (DDMMYYYY): 01012000


> Pet's name: boomer
> Company name: walmart


> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed:
cheapskate,religious, hunter, poker
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]:y
> Leet mode? (i.e. leet = 1337) Y/[N]: y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to jim.txt, counting 68372 words.
[+] Now load your pistolero with jim.txt and shoot! Good luck!
```

Cewl Lab:

In this lab, Subject Matter Expert Dean Pompilio demonstrates Cewl, a simple and useful tool for generating word lists for use with a password cracking tool. Cewl is built into Kali, or it can be downloaded and run from other UNIX systems. SME Pompilio gives an example of how a Social Engineer would use Cewl's spidering process to generate a word list for password cracking and how the output is evaluated.

You will learn to

- run the program
- examine the Help function
- understand the various options in Cewl
- specify the spidering depth
- specify word length
- specify an output file
- specify a proxy
- determine whether to use the offsite parameter
- search for metadata and save to a file
- search for email addresses and save to a file

The large number of words (13,325) and email addresses (82) discovered by the process run in the example can be used with a password cracking tool, and those results will be used in your Social Engineering audit.

```
cd /usr/share/cewl
./cewl.rb --write outputfile.txt --email --email_file email.txt http://tools.kali.org --verbose
```

Shodan Lab:

In this lab, Subject Matter Expert Dean Pompilio demonstrates the features and the uses for a Web site called Shodan (www.shodan.io). You need to register and create an account to fully use this Web site. Shodan crawls the Internet and identifies IP addresses that have a service running. Then it does a banner grab of the service that is running, and it saves the banner information. You can search on a keyword or an IP address to find the services that are running.

You will learn how to use the explore link to find out more about popular recent searches, and you are encouraged to read the site's blog. The blog is for people who want more information or who want to share their projects

SME Pompilio describes the idea of gathering IP addresses of your target in the context of Shodan. He demonstrates using the Web site for a penetration test or audit by identifying your target organization and their IP addresses. Then Shodan can be used to find the location and all the services that are running.

You will be working within the IP address range that your target is using and you will not be working randomly. Shodan helps to define the attack surface for your particular penetration test of an audit target.

Popular searches: webcam, cams, Netcam, dreambox, default password, spy, Hidden camera, Matrix VoiPServer

Scythe Lab:

In this lab, Subject Matter Expert Dean Pompilio demonstrates Scythe, an interesting **account enumerator tool that allows you to do account harvesting**. You will use this tool to find out where your target has accounts on various Web sites.

You install Scythe into your Kali instance from GitHub using the following steps:

- **Go to www.GitHub.com**

- **Enter Scythe into the site's search function**

- **Choose ChrisJohnRiley/*Scythe* from the list that is returned**

In this lesson, you will learn:

- how to run the program and understand the list of modules it supports
- what the current settings are
- how to set a directory for where all the modules are located
- about the different modules
- how to search on user name and/or email address
- how to edit the account file
- about options you can specify, such as the list option, directory for the modules, sorting by category
- how to specify the ability to run threads
- how to specify the retry time
- how to specify how the summary is shown
- how to specify how to save the output

SME Pompilio demonstrates the system with two different sets of specifications and notes that the summary gives information on where the accounts are located on all the various Web sites. He notes that it is important to consider the value of aggregation – that a Social Engineer gathers bits and pieces about the target from various places around the Internet and then may be able to infer certain information about their target's interests. This can provide fodder for engaging in Social Engineering techniques such as phishing and spearphishing.

```
./scythe.py --category social --summary --output outfile.txt
```

```
./scythe.py --single slideshare.net --summary
```

Creepy Lab:

In this lab, Subject Matter Expert Dean Pompilio demonstrates a tool called Creepy. The Web site www.geocreepy.com provides a useful tool that allows you to do geolocation for a target by using various social networking platforms to track individuals. Creepy works with Twitter, Flickr, Instagram, and Google Plus. Creepy is available to use within Kali, but Windows is used for this demonstration.

SME Pompilio demonstrates a person-based geolocation using himself as the target. (You need to be aware when using this tool that a target may have disabled geolocation).

In this lesson you will learn:

- how to launch the tool
- the need to configure the plug-ins for the Web sites you want to use
- the need to create accounts on the platforms you want to use
- how to log in and get a pin number that authorizes sites to allow Creepy read-only access
- how to select multiple targets and select a project
- the available options such as including re-tweets and including replies in the information Creepy returns
- that the program sends the geolocation data to Google Maps
- that a map is returned showing the target's tweet locations and showing the tweets with a date and time stamp
- how to use the analysis link, which will give other statistics and further information about the tweets
- other things you can do such as filter by location, date, or position (distance from the point of interest) to narrow things down
- how to remove your filters

SME Pompilio states that Creepy is one tool to add to your bag of tricks to correlate information and to use with the built-in features of many social networking sites to get information about your target. He also says that the information returned by Creepy may not be 100 percent correct and may need to be correlated with other information to verify it.

In order to use this tool with its APIs, you need to create accounts on those platforms that you will interrogate with Creepy, so that they can give you Read access to their database to interrogate it!

A person can have GeoLocation (in Twitter) disabled or enabled, it depends on how security minded they are.

Detection and Prevention:

In this lesson, Subject Matter Expert Dean Pompilio discusses ways to detect and prevent Social Engineering. Not everything about Social Engineering is in offensive mode; some of it is defensive — if you are the victim, you need to know how to take defensive measures.

SME Pompilio explains that while effective Social Engineers do not want their target to feel suspicious, potential Social Engineering victims need to be suspicious of anything out of the ordinary, especially when their gut tells them something is not right. Victims need to perform due diligence, trust but verify, and become digitally quiet – adhering to the Kali slogan that the quieter you are the more you are able to hear.

In this lesson, you will learn techniques to lessen your exposure to Social Engineering (such as enabling privacy settings on all social networking sites), and you will learn:

- that becoming unpredictable can benefit the Social Engineer and the target
- the kind of physical security controls that can thwart the Soc Eng
- how User Awareness training should be required for everyone in an organization
- that Advanced Security Awareness training is necessary for some employees
- that it is important to pay attention to the legal aspects of ethical Social Engineering
- that proper documentation is necessary for carrying out ethical Social Engineering
- how Search Engine Optimization can elicit good clues for the Social Engineer
- the definitions of and the differences between all of the "—bie" (eg: newbie, koolbie, maturbie) classifications of Social Engineers
- become digitally quiet
- be suspicious of anything out of the ordinary (always perform due diligence)
- maintain sent items folder
- enable all Facebook privacy settings
- un-tag all photos
- delete Google blogspots, Tumblr, Wordpress, etc
- Consider DuckDuckGo, StartPage and another search alternative
- use anonymizer or proxy websites

New-bie:

"Hang around web based chat, watches what hackers are doing to befriend them and intelligence on how they hack."

Concluding this course on Social Engineering, SME Pompilio reiterates that Social Engineering is an art and a science. He reminds us that our use of language maps to our experiences that can be manipulated by a Social Engineer. He suggests that to not be a victim of Social Engineering it is necessary to learn the thresholds for a Human Buffer Overflow and to practice becoming vague in a deliberate way.

Curious-bie:

"Starts wanting to dismantle the tools they've been using; wants to have the popularity, and respect the real-bies have in the scene."

Real-bie:

"Real hacker, has finally been reading mailing lists and news articles for a while, starts thinking about Linux distros, joining internet relay chat (IRC), joining real discussion about technical emphasis of vulnerabilities, wants to start hacking."

True-bie:

"Has successfully penetrated an online application; gets interested in forming views. The industry discovers the person, the true-bie becomes vocal on online communities."

Student-bie:

"Has formed strong views and believes, now wants to make money in a career of information security. Goes to college to become professional. Hides hacking background from student peers, feels guilty about part of the underground, keeps it secret."

Pro-bie:

"Graduates from university, expect a full pay and a successful life, end up just working in the local supermarket, starts acting as a security professional online anyway, at this point the government become concerned."

Job-bie:

"Through exposure of releasing vulnerabilities and getting talked about in news articles, is offered a job at a real vendor company."

Mature-bie:

"Is known names company for a while; known as an expert; may start a blog; commentary is often seen in quotes in news articles; the government actually listens to what mature-bie says in his/her blog."

In conclusion:

- social engineering is an art and a science
- our use of language maps to our experiences, which can be manipulated by a skilled SE
- learn the thresholds for a Human Buffer Overflow
- practice becoming vague in a deliberate way

Advanced Social Engineering

In this lesson, Subject Matter Expert Dean Pompilio discusses the next series of videos for this course: Advanced Social Engineering. In those lessons he will cover system access techniques and tools including Metasploit and Veil. He will talk more about physical security considerations, and he will present live demonstrations of physical security methods.

You may contact Dean Pompilio (username Polymath) through the Cybrary blog to let him know what techniques and tools you are using and what might be useful to the community.

Learn system access techniques and tools:

- Metasploit
- Veil
- Physical security

Stay tuned for the next class in the series!