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.

---

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.

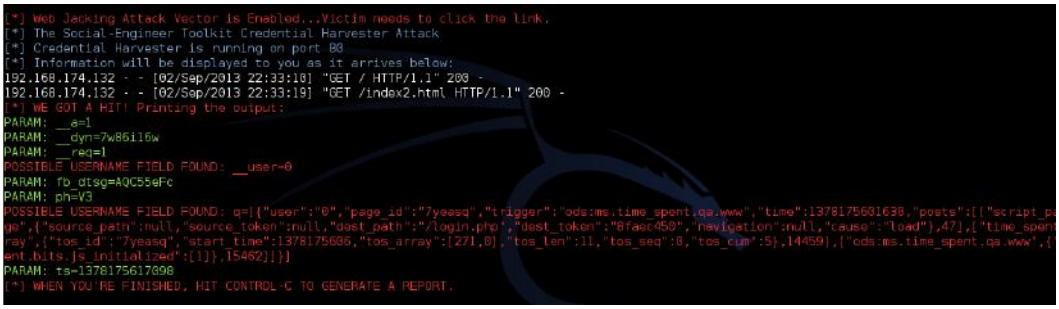
2
Understanding Website Attack Vectors

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!

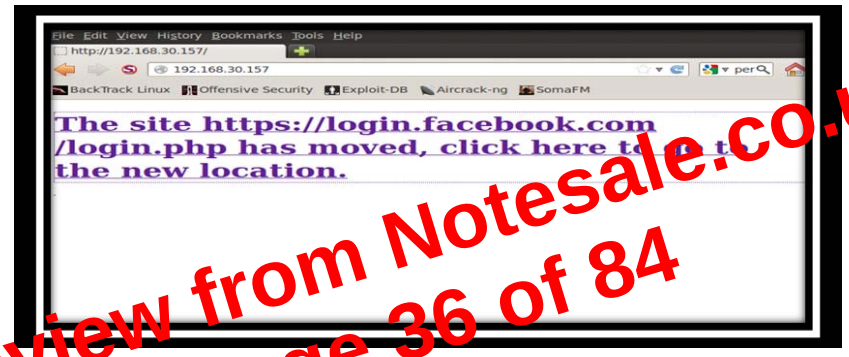
In this chapter, we will be covering different attacks that can be performed on the application layer to compromise a system. The topics discussed in this chapter will come in use when you decide you want to test the security of an organization against social engineering attacks. Such attacks provide 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



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:

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.

Defense against these attacks

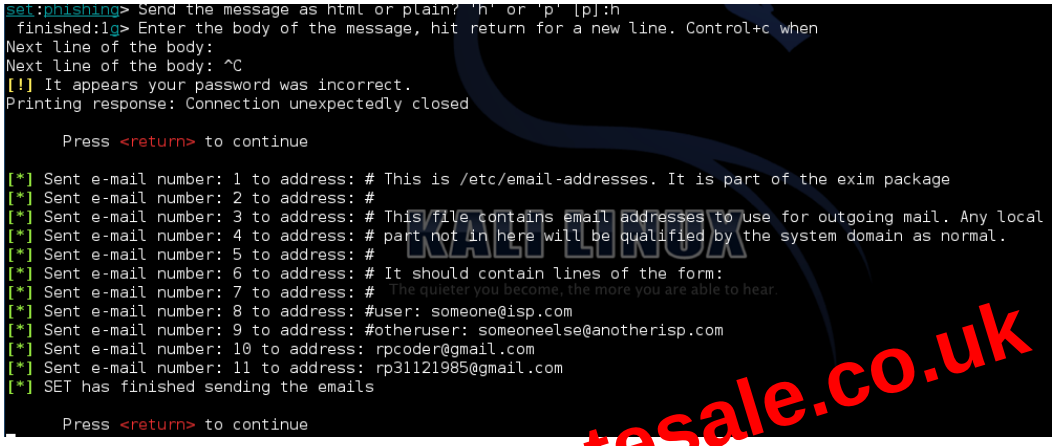
The attacks that we have covered in this chapter can mostly be avoided by keeping our web browser updated and not opening any suspicious links and documents. Also ensure that the passwords/credentials used are changed frequently and retained secretly.

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.

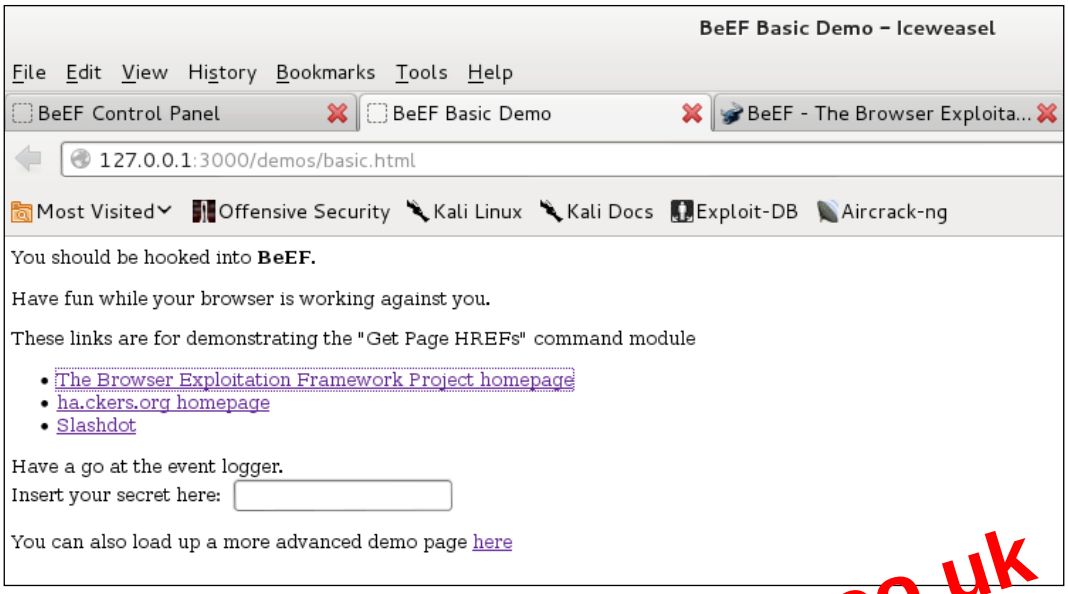
7. As you can see in the preceding screenshot, the attacker e-mail ID is `rpcoder@gmail.com`. The **FROM** field specifies by which name the e-mail needs to be sent. The next thing we need to specify is the priority of this message and whether it needs to be sent in plain text or HTML format and also 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.



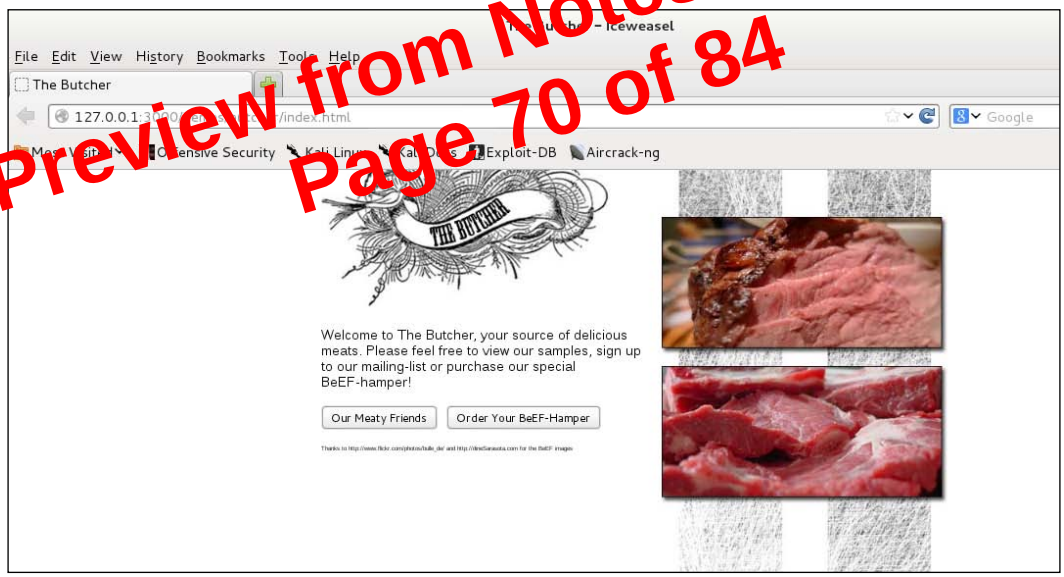
8. Once all the required information is given, SET will start sending the e-mails sequentially as presented in the preceding screenshot. Once SET finishes sending the e-mail to all the targets, it will prompt us to return to.

Understanding the SMS spoofing attack vector

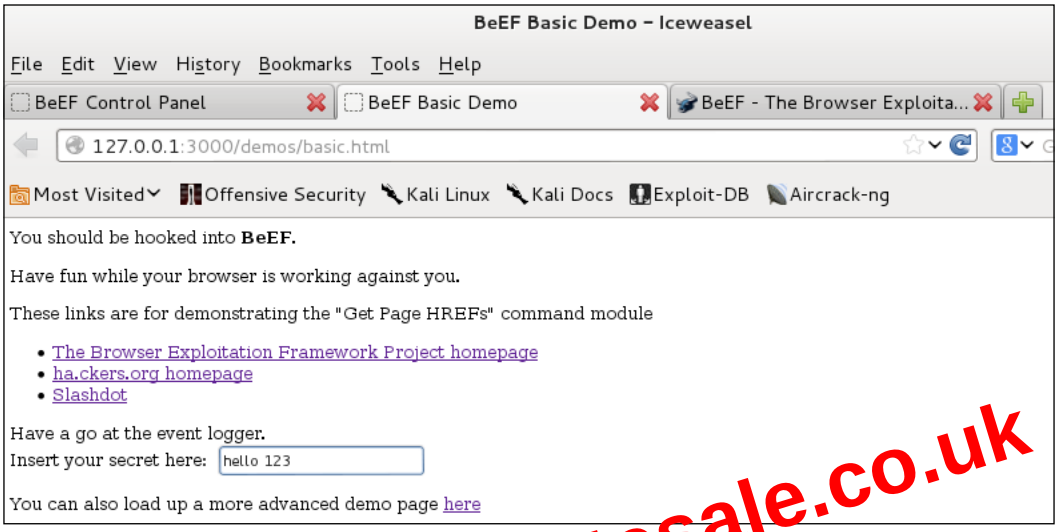
The SMS spoofing attack allows the attacker to send a text SMS using SET without revealing his/her true identity or by using someone else's identity.



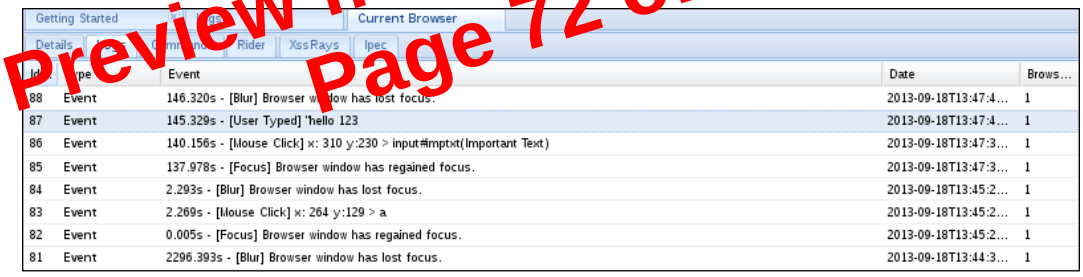
The second demo page, also known as the Butcher demo page, looks like this:



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 panel in the **Logs** menu. We will check whether it identified the **click** event even though I did not submit it.



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:

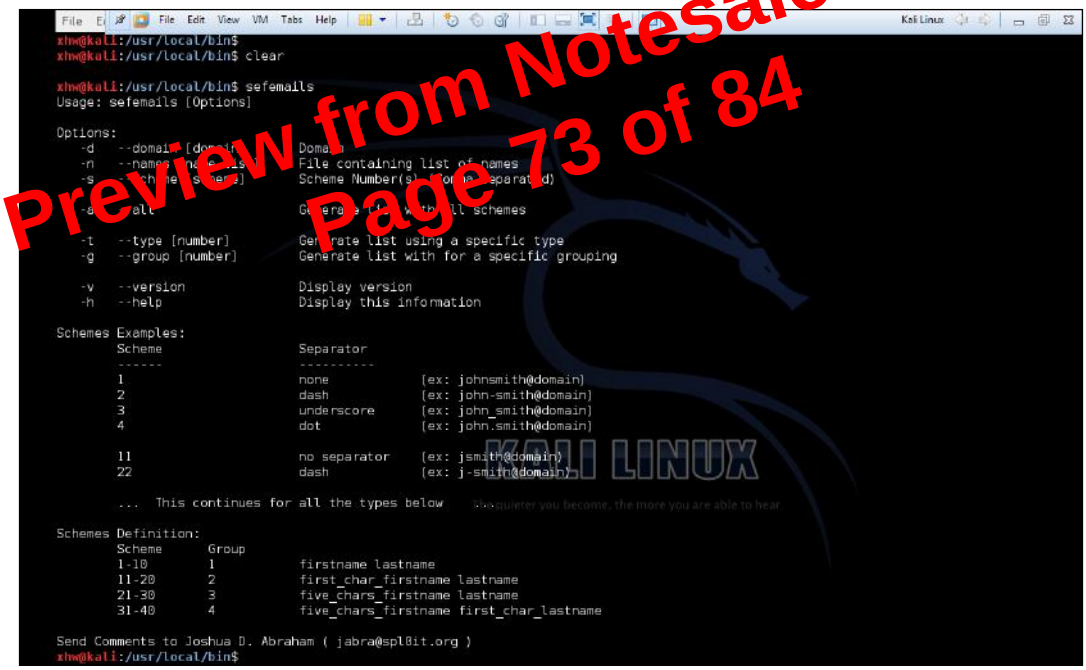
- Sefemails
- Sefphish
- Sefnames
- SefPayload

Sefemails

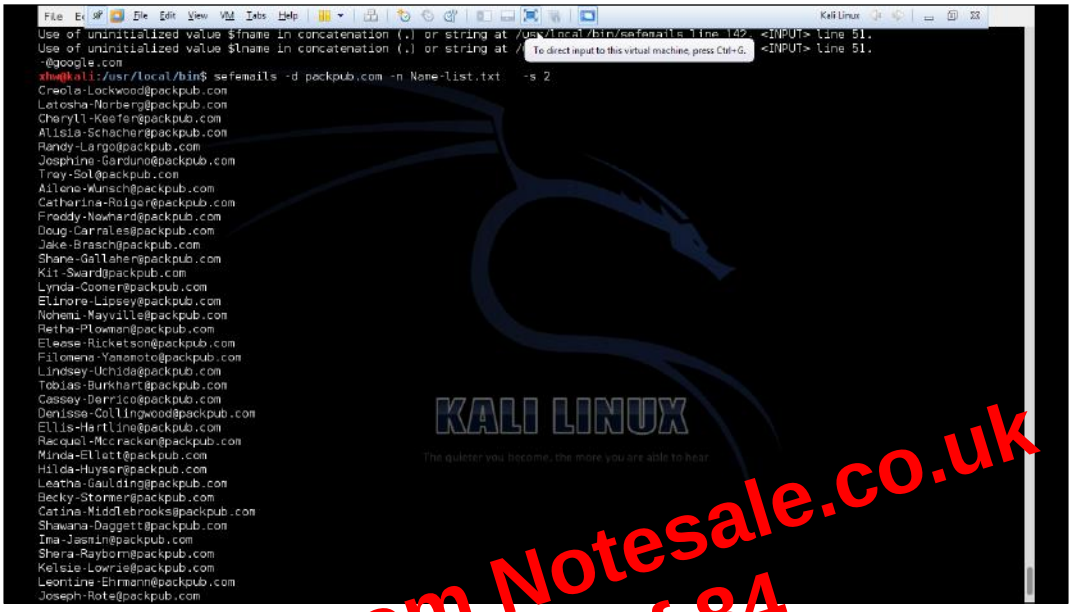
Sefemails is used to generate a list of e-mail addresses for the purpose of performing a phishing attack in bulk against a specific organization. The syntax to run this tool in Kali Linux is as follows:

```
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
```

Index

J

L

M

N

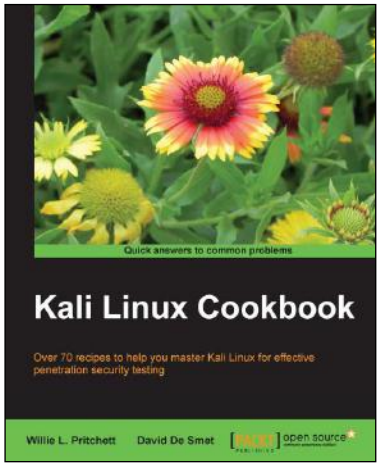
O

P

R

S

[PACKT] open source
community experience distilled
PUBLISHING



Kali Linux Cookbook

ISBN: 978-1-78328-959-2 Paperback: 260 pages

Over 70 recipes to help you master Kali Linux for effective penetration security testing

1. Recipes designed to educate you extensively on the penetration testing principles and Kali Linux tools
2. Learning to use Kali Linux tools, such as Metasploit, Wire Shark, and many more through in-depth and structured instructions
3. Teaching you in an easy-to-follow style, full of examples, illustrations, and tips that will suit experts and novices alike

---

Instant Kali Linux

ISBN: 978-1-84969-566-4 Paperback: 68 pages

A quick guide to learn the most widely-used operating system by network security professionals

1. Learn something new in an Instant! A short, fast, focused guide delivering immediate results
2. Covers over 30 different tools included in Kali Linux
3. Easy guide to sett up and install Kali Linux under different hardware sets
4. Step by step examples to get started with pen-testing tools