Social Engineering

Module 08

Social Engineering

Social engineering is the art of convincing people to reveal confidential information.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Social engineering is the art of convincing people to reveal sensitive information in order to perform some malicious action. Organizations fall victim to social engineering tricks despite having security policies and best security solutions in place, as social engineering targets people's weaknesses or good nature. Reconnaissance and social engineering is generally an essential component of any information security attack.

Cybercriminals are increasingly utilizing social engineering techniques to exploit the most vulnerable link in information system security: employees. Social engineering can take many forms, including phishing emails, fake sites, and impersonation.

McAfee's new "Hacking the Human Operating System" whitepaper focuses on the use of social engineering to attack home and business users, and finds once again that people are the weakest link. The McAfee report points out that there are many organizations who develop and deliver user awareness programs into their business areas, but the effectiveness of such programs varies, and in some identified cases, even after the security training has been delivered, it has done very little to educate their end users with any valued security awareness to mitigate the threat of the social engineering attack.

It is essential for you as an expert Ethical Hacker and Penetration Tester, to assess the preparedness of your organization or the target of evaluation against the social engineering attacks. Though social engineering primarily requires soft skills, the labs in this module demonstrate some techniques that facilitate or automate certain facets of social engineering attacks.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 08 Social Engineering

Lab Objectives

The objective of this lab is to:

- Detect phishing sites
- Protect network from phishing attacks
- Perform Credential Harvesting
- Perform security assessment on a machine using a payload generated by SET

Lab Environment

To carry out this lab, you will need:

- A computer running Window Server 2012
- Kali Linux virtual machine

- Windows 8.1 virtual machine
- A Web browser with Internet access
- Administrative privileges to run the tools

Lab Duration

Time: 35 Minutes

TASK 1

Overview

Overview Social Engineering

Social engineering is the art of convincing people to reveal confidential information. Social engineers depend on the fact that people know certain valuable information yet are generally careless in protecting it.

Lab Tasks

Recommended labs to assist you in Social Engineering:

- Detecting Phishing Using **Netcraft**
- Detecting Phishing Using **PhishTank**
- Sniffing Facebook Credentials using **Social Engineering Toolkit** (SET)
- Creating a **Malicious Payload** Using **SET** and Exploiting a Windows Machine

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Detecting Phishing Using Netcraft

Netcraft provides web-server and web-hosting market-share analysis, including web-server and operating-system detection.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

According to Verizon's 2015 "Data Breach Investigations Report," over two-thirds of all corporate espionage cases involved phishing attacks. The report shows that about 23% of recipients now open phishing messages and 11% click on attachments. The report further adds that it takes only 82 seconds, on average, for hackers to trick their first victim in a phishing campaign.

Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies.

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications claiming to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Phishers target the customers of banks and online payment services. They send messages to bank customers by manipulating URLs and website forgery. The messages sent claim to be from a bank and look legitimate. Users, not realizing that it is a fake website, provide their personal information and bank details. Recent trend shows that hackers are now increasingly engaging in spear phishing campaigns against bank *employees*, rather than bank customers.

As you are an expert Ethical Hacker and Penetration Tester, you must be aware of phishing attacks occurring on the network, and implement Anti-phishing measures. In an organization, proper training must be provided people to help them deal with phishing attacks. In this lab, you will be learning to detect phishing using Netcraft.

Lab Objectives

This lab provides phishing sites via web browser and shows you how to use them. It will teach you how to:

- Detect phishing sites
- Protect the network from phishing attack

Lab Environment

To carry out this lab, you will need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 08 Social Engineering

- **Netcraft** is located at **D:\CEH-Tools\CEHv9 Module 08 Social Engineering\Anti-Phishing Toolbar\Netcraft Toolbar**
- You can also download the latest version of Netcraft Toolbar from the link http://toolbar.netcraft.com/
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012
- A web browser (Firefox, Internet explorer, etc.) with Internet access
- Administrative privileges to run the Netcraft toolbar

Lab Duration

Time: 5 Minutes

Overview of Netcraft Toolbar

Netcraft Toolbar provides Internet security services, including anti-fraud and anti-phishing services, application testing, code reviews, automated penetration testing, and research data and analysis on many aspects of the Internet.

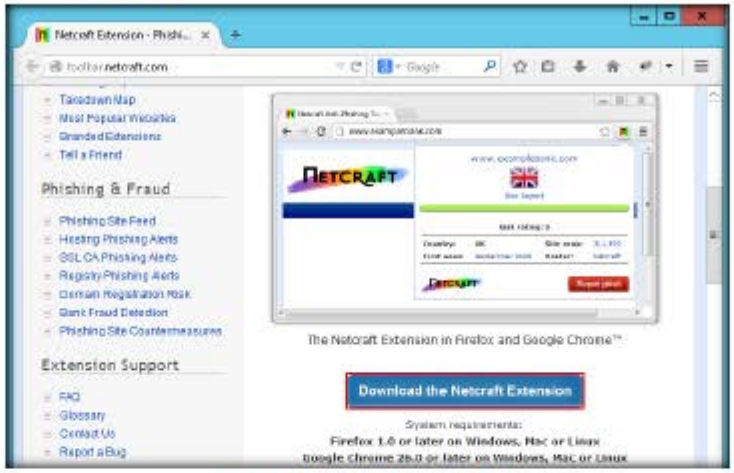
Lab Tasks

TASK 1

Install Netcraft Toolbar

1. Before beginning this lab, you need to launch a web browser. In this lab we have used **Mozilla Firefox**.
2. To download the **Netcraft Toolbar** for **Mozilla Firefox**, type in this URL http://toolbar.netcraft.com in the address bar of the browser and press **Enter**.
3. Alternatively, you can drag and drop the **netcraft_toolbar-1.8.3-fx.xpi** file in Firefox.
4. In this lab we are downloading the toolbar from Internet.

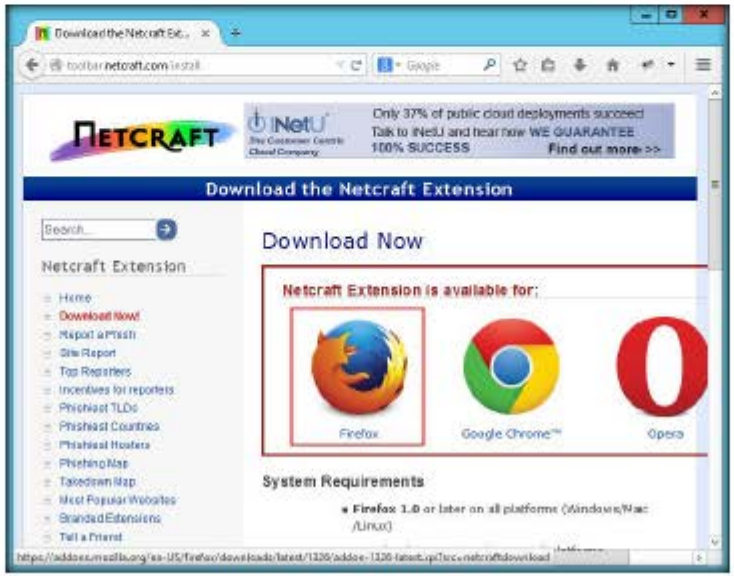
5. In Firefox browser, click on **Download the Netcraft Toolbar** to install as Add-on.



Netcraft provides Internet security services, including anti-fraud and anti-phishing services.

FIGURE 1.1: Netcraft toolbar downloading Page

6. On the download page of the Netcraft Toolbar site, click on **Firefox** to continue the installation.



Netcraft is an Internet services company based in Bath, England.

FIGURE 1.2: Netcraft toolbar Installation Page

7. Click **Allow** to download Netcraft Toolbar.

Netcraft Toolbar provides a wealth of information about the sites you visit.

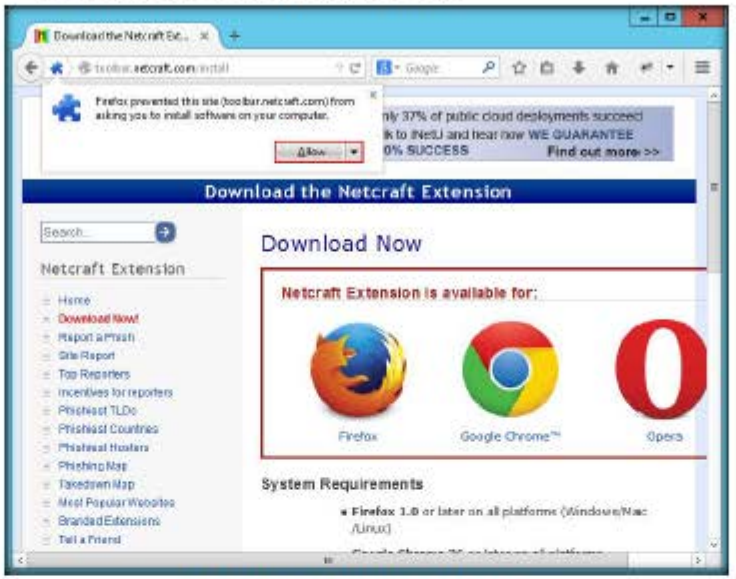


FIGURE 1.3: Netcraft toolbar Installation-Allow button

8. When the **software installation** dialog box appears, click **Install Now**.

Risk Rating displays the trustworthiness of the current site.

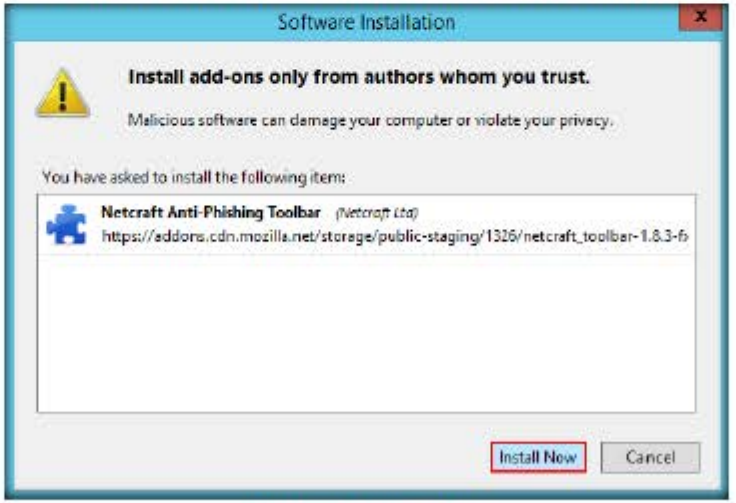


FIGURE 1.4: Installing Netcraft Toolbar

9. To complete the installation, you will be asked to restart the browser. Click **Restart Now**.

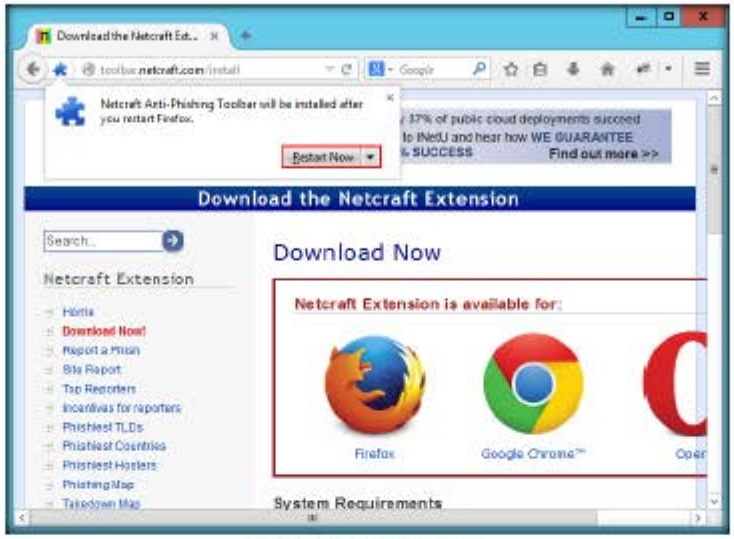


FIGURE 1.5: Restarting Firefox browser

10. The **Neteraft Toolbar** is now visible in the browser window, as displayed in the screenshot:

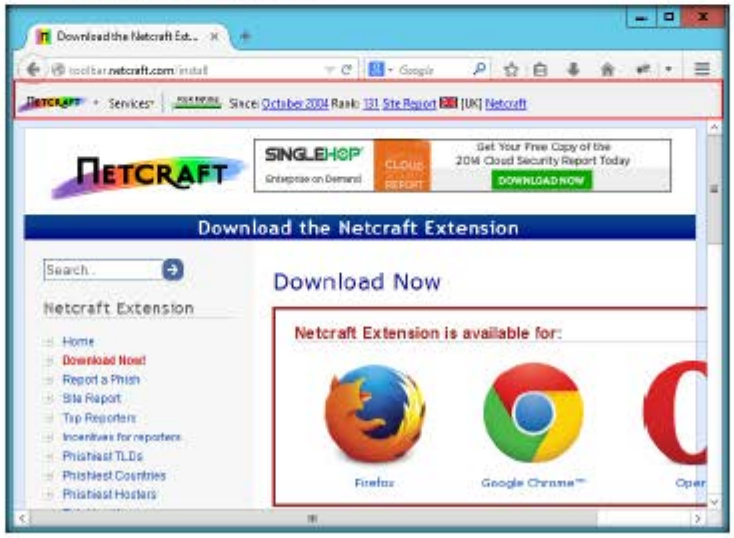


FIGURE 1.6: Netcraft Toolbar on Mozilla Firefox web browser

TASK 2

Examine Websites

11. Open a new tab, type the URL http://www.certifiedhacker.com in the address bar, and press **Enter**.
12. The Certified Hacker webpage appears, and the following information is displayed in the toolbar (unless the page has been blocked): **Risk rating, Rank**, the **year the website was launched,** and **Flag**.

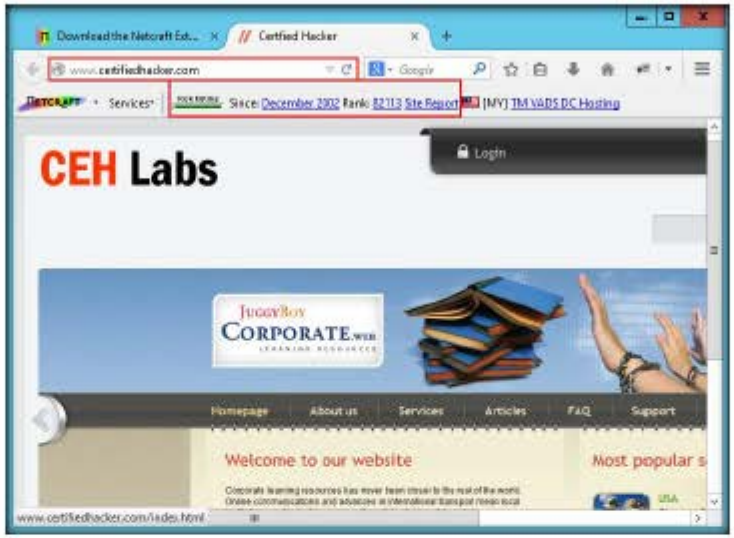


FIGURE 1.7: Netcraft Toolbar on Mozilla Firefox web browser

13. Click **Site Report** to view a report of the site.

Site report links to a detailed report for the current site.

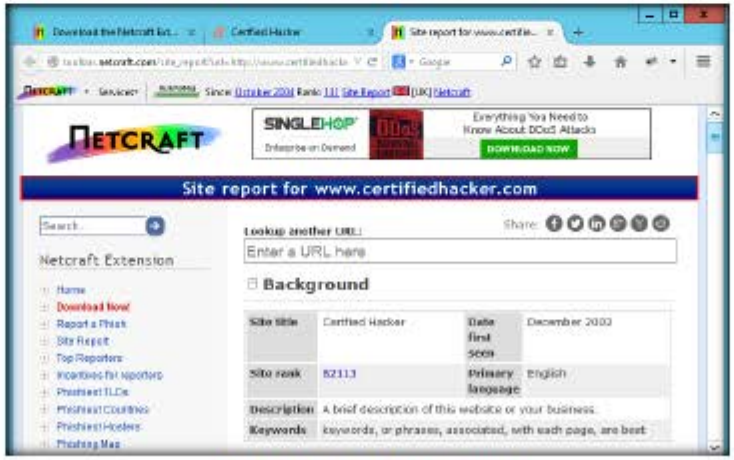
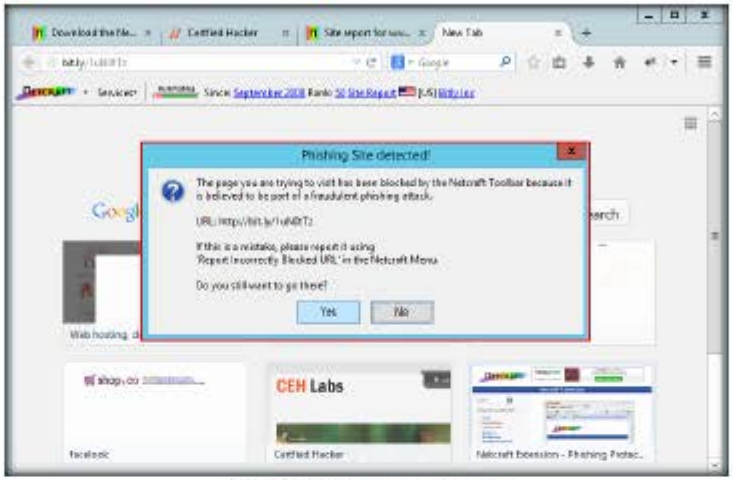


FIGURE 1.8: Report generated by Netcraft Toolbar

14. If you attempt to visit a website that has been identified as a phishing site by Netcraft Toolbar, you will see a pop-up stating that **Phishing Site Detected!** as shown in the screenshot:



Phishing's site feeds continuously updated encrypted database of patterns that match phishing URLs reported by the Netcraft Toolbar.

FIGURE 1.9: Warning pop-up for blocked site

15. If you trust the site, click **Yes** to browse it; otherwise, click **No** (Recommended) to block it.
16. If you click **No**, Netcraft blocks the phishing site, as shown in the screenshot:

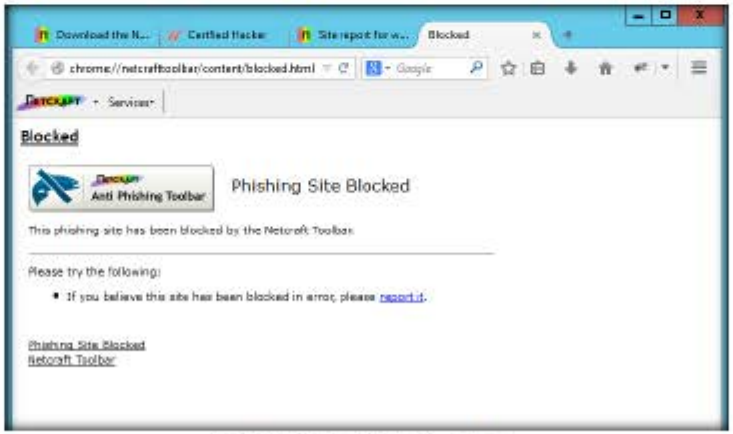


FIGURE 1.10: Website blocked by Netcraft Toolbar

Lab Analysis

Document all the results and report gathered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab 2

Detecting Phishing Using PhishTank

PhishTank is a collaborative clearinghouse for data and information regarding Internet phishing.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from legitimate organizations or known individuals. These emails often attempt to entice users to click on a link that leads to a fraudulent website that appears legitimate. Users may then be asked to provide personal information such as account usernames and passwords that can further expose them to subsequent compromises. Additionally, these fraudulent websites may contain malicious code.

With the tremendous increase in the use of online banking, online shares trading, and ecommerce, there has been a corresponding growth in the incidents of phishing being used to carry out financial fraud. Phishing involves fraudulently acquiring sensitive information (e.g., passwords, credit card details etc.) by masquerading as a trusted entity.

In the previous lab, you already saw how a phishing site can be detected using Netcraft.

The usual scenario is that the victim receives an email that appears to have been sent from the victim's bank. The email urges the victim to click on the link in the email. When the victim does so, he/she is taken to "a secure page on the bank's website." The victim believes the web page to be authentic, and enters his/her username, password, and other sensitive information. In reality, the website is a fake. The victim's information is then stolen and misused.

As an administrator or penetration tester, you may have implemented the most sophisticated and expensive technology solutions in the world, but all of it can be bypassed and compromised if employees fall for simple social engineering scams. Thus, it becomes your responsibility to educate employees regarding best practices for protecting systems and information.

Lab Objectives

This lab will show you how to use phishing sites using a web browser. It will teach you how to:

- Detect phishing sites
- Protect the network from phishing attacks

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 08 Social Engineering

Lab Environment

To carry out this lab, you will need:

- A computer running Windows Server 2012
- A Web browser (Firefox, Internet Explorer, etc.) with Internet access

Lab Duration

Time: 5 Minutes

Overview of PhishTank

PhishTank URL: http://www.phishtank.com

PhishTank is a free community site on which anyone can submit, verify, track, and share phishing data. PhishTank is a collaborative clearing house for data and information regarding phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications, at no charge.

Lab Tasks

TASK 1

Detect Phishing Sites using PhishTank

1. Before beginning this lab, you need to launch a web browser. In this lab we have used **Google Chrome**.
2. Type the URL http://www.phishtank.com in address bar and press **Enter**

3. The **PhishTank** webpage appears, as shown in the screenshot:

PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.

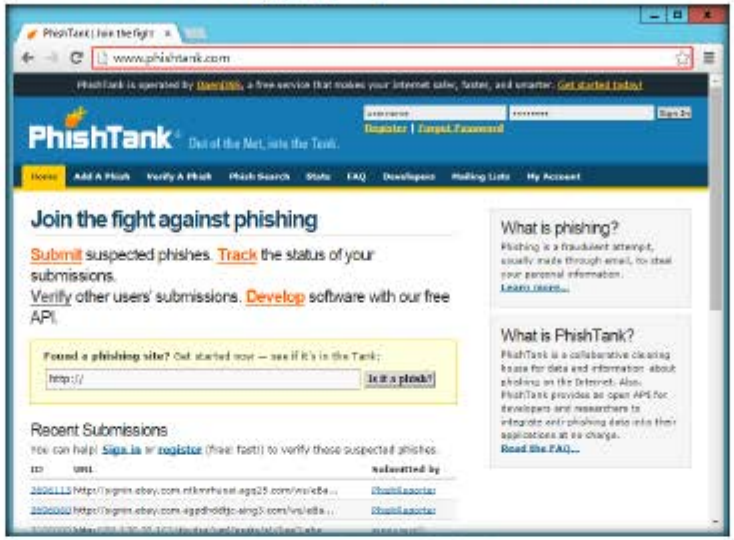


FIGURE 2.1: Welcome screen of PhishTank

4. Type the **website URL** to be checked for phishing. In this lab, the URL entered is http://be-ride.ru/confirm.

5. Click **Is it a phish?**

PhishTank is operated by Open DNS to improve the Internet through safer, faster, and smarter DNS.

FIGURE 2.2: Checking for site

6. If the site is a **phishing site**, PhishTank returns a result stating that the website "Is a phish," as shown in the screenshot:

Open DNS is interested in having the best available information about phishing websites.

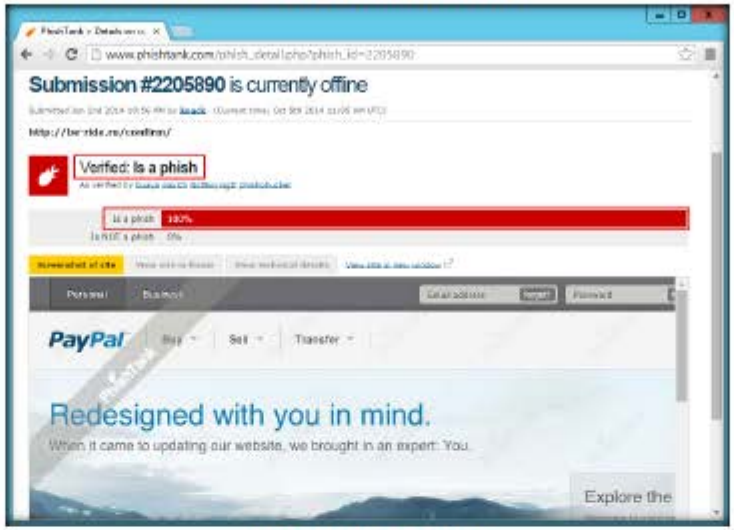


FIGURE 2.3: Phishing website found

Lab Analysis

Document all the websites, and verify whether they are phishing sites.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab 3

Sniffing Facebook Credentials Using Social Engineering Toolkit (SET)

The Social Engineering Toolkit (SET) is an open-source Python-driven tool designed for penetration testing.

Lab Scenario

ICON KEY
- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Social Engineering is an ever-growing threat to organizations all over the world. Social Engineering attacks are used to compromise companies every day. Even though there are many hacking tools available throughout underground hacking communities, Social Engineering Toolkit (SET) is a boon to attackers, as it is freely available and applicable to Spear-phishing attacks, website attacks, and many others. Attackers can draft email messages, attach malicious files, and send them to a large number of people using spear phishing. In addition, the multi-attack method allows utilization of Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing all at once.

Though numerous sort of attacks can be performed using SET, it is also a must-have tool for penetration testing to check for vulnerabilities. SET is the standard for social-engineering penetration tests, and is supported heavily in the security community.

As an Ethical Hacker, Penetration Tester, or Security Administrator, you should be familiar with the Social Engineering Toolkit to perform various tests for network vulnerabilities.

Lab Objectives

The objective of this lab is to help students learn how to:

- Clone a website
- Obtain username and passwords using Credential Harvester method
- Generate reports for conducted penetration test

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 08 Social Engineering

To carry out this lab, you will need:

- Run this tool in Kali Linux Virtual Machine
- Windows Server 2012 host machine
- Web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of the Social Engineering Toolkit

The Social Engineering Toolkit is an open-source Python-driven tool aimed at penetration testing. The SET is specifically designed to perform advanced attacks against human by exploiting human behavior. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

Lab Tasks

1. Ensure that the Apache server is turned ON before running this lab.
2. Log in to **Kali Linux** virtual machine.

TASK 1

Launch Social Engineering Toolkit

3. Go to **Applications → Kali Linux → Exploitation Tools → Social Engineering Tools → se-toolkit**.

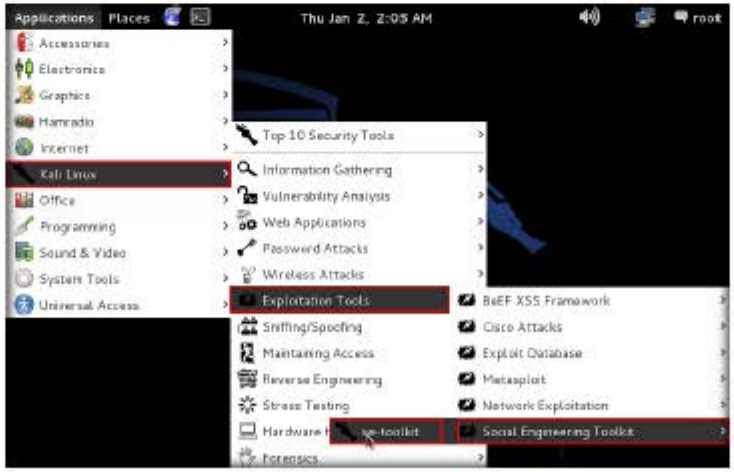


FIGURE 3.1: Launching SET in Kali Linux

4. If you are launching se-toolkit for the first time, you may be asked whether to enable bleeding-edge repos. Type **no** and press **Enter**.

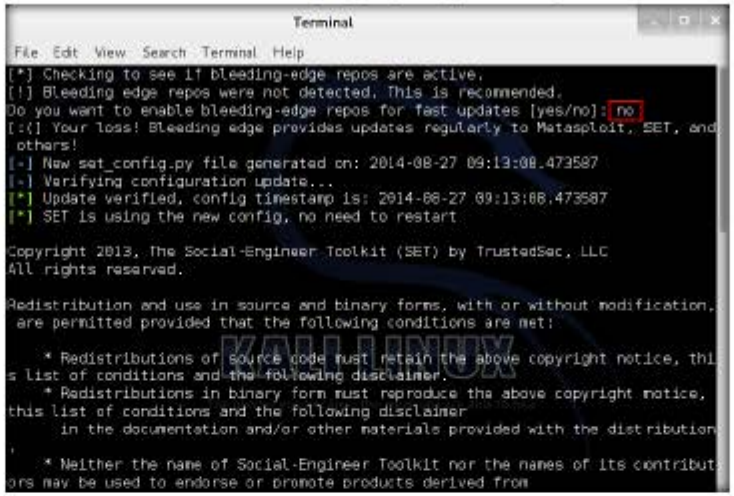


FIGURE 3.2: Disable bleeding-edge repos

5. Type **y** and press **Enter** to agree to the terms of services.

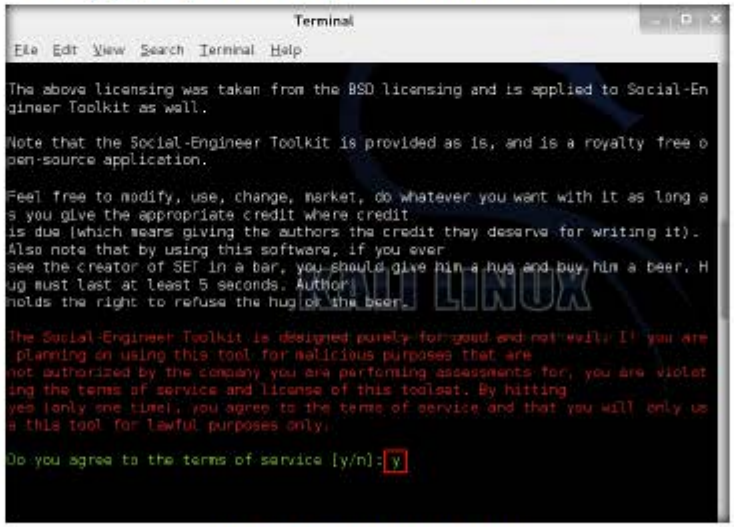


FIGURE 3.3: Agreeing to the terms of services

TASK 2

Create a Cloned Website

6. You will be presented with an SET menu.

Note: If se-toolkit exits without launching the menu, repeat **steps 3–5** before continuing.

7. Type **1** and press **Enter** to choose **Social-Engineering Attacks**.

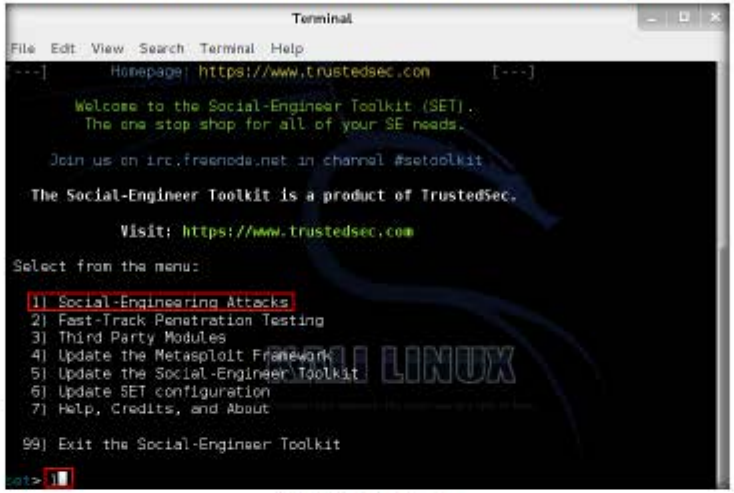
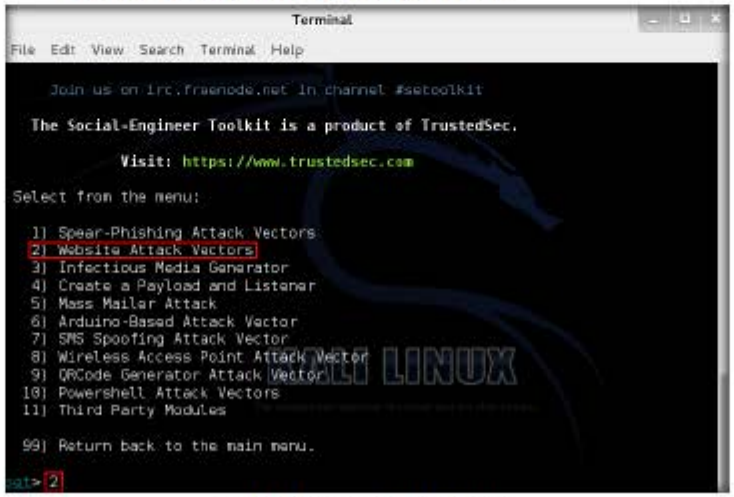


FIGURE 3.4: SET Main menu

SET allows you to specially craft email messages and send them to a large (or small) number of people with attached file format malicious payloads.

8. A list of menus in Social-Engineering Attacks will appear; type **2** and press **Enter** to choose **Website Attack Vectors**.



The webjacking attack is performed by replacing the victim's browser with another window that is made to look and appear to be a legitimate site.

The Social-Engineer Toolkit "Web Attack" vector is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

FIGURE 3.5: Choosing Website Attack Vectors

9. In the next menu that appears, type **3** and press **Enter** to choose **Credential Harvester Attack Method**.

The Credential Harvester Method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

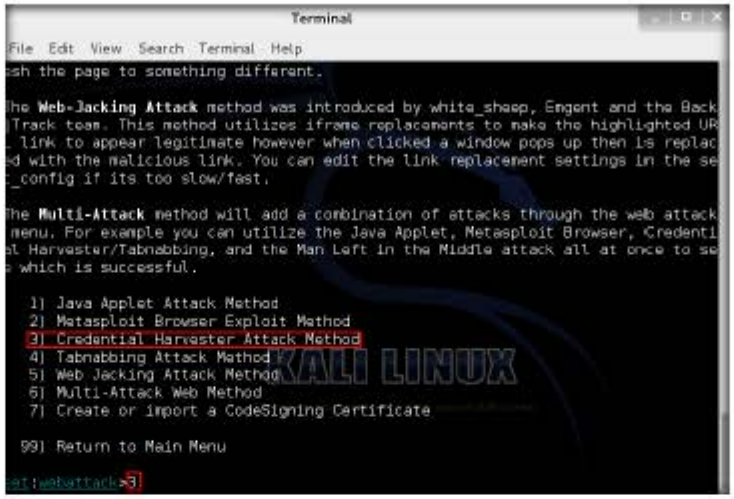
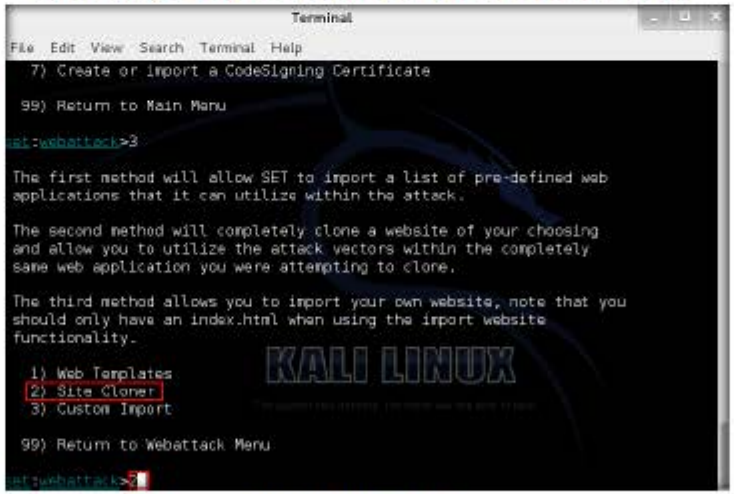


FIGURE 3.6: Choosing Credential Harvester Attack Method

10. Now, type **2** and press **Enter** to choose **Site Cloner** from the menu.

The Site Cloner is used to clone a website of your choice.



SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon.

FIGURE 3.7: Choosing Site Cloner

11. Type the **IP address** of Kali Linux virtual machine in the prompt for "**IP address for the POST back in Harvester/Tabnabbing,**" and press

Enter. In this lab, the IP address of Kali Linux is **10.0.0.6**, which may vary in your lab environment.

The tabnabbing attack method is used when a victim has multiple tabs open, when the user clicks the link, the victim will be presented with a "Please wait while the page loads". When the victim switches tabs because he/she is multi-tasking, the website detects that a different tab is present and rewrites the webpage to a website you specify. The victim clicks back on the tab after a period of time and thinks they were signed out of their email program or their business application and types the credentials in. When the credentials are inserts, they are harvested and the user is redirected back to the original website.

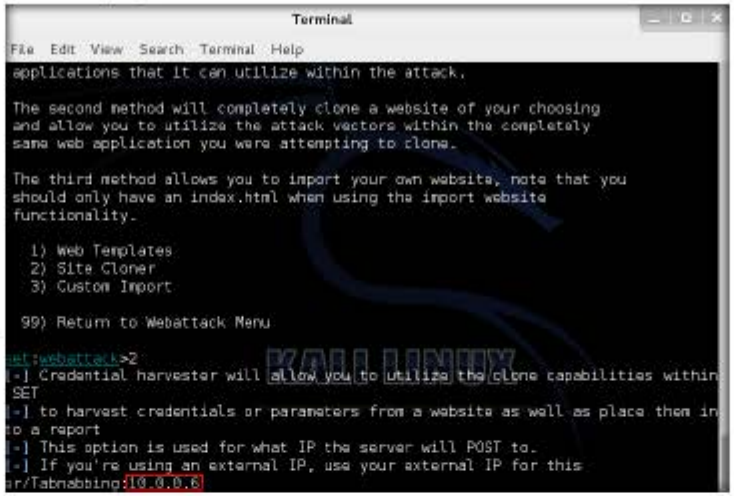


FIGURE 3.8: Providing IP address in Harvester/Tabnabbing

12. Now, you will be prompted for a URL to be cloned; type the desired URL for "**Enter the url to clone**" and press **Enter**. In this example, we have used **www.facebook.com**. This will initiate the cloning of the specified website.

The web jacking attack method will create a website clone and present the victim with a link stating that the website has moved. This is a new feature to version 0.7.

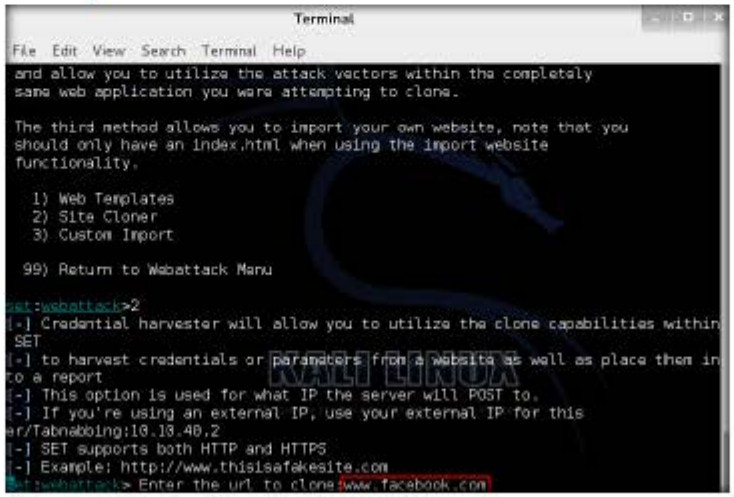


FIGURE 3.9: Providing URL to be cloned

Note: If you are prompted to start apache server:

13. After cloning is completed, the highlighted message as in the below screenshot will appear on the **Terminal** screen of **SET**. Press **Enter** to continue.
14. It will start Credential Harvester.

If you're doing a penetration test, register a name that's similar to the victim, for Gmail you could do gmail.com (notice the I), something similar that can mistake the user into thinking it's the legitimate site.

FIGURE 3.10: SET Website Cloning

TASK 3

Send a Crafted Email

15. Allow the Credential Harvester Attack to fetch information from the victim machine.
16. Now, you have to send the **IP address** of your Kali Linux machine to a victim and trick him or her to **click to browse** the IP address.
17. For this demo, launch your web browser in the Kali Linux machine; launch your favorite email service. In this example we have used **www.gmail.com**. Login to your Gmail account and compose an email.

When you hover over the link, the URL will be presented with the real URL, not the attacker's machine. So for example if you're cloning gmail.com, the URL when hovered over it would be gmail.com. When the user clicks the moved link, Gmail opens and then is quickly replaced with your malicious webserver. Remember you can change the timing of the webjacking attack in the config/set_config flags.

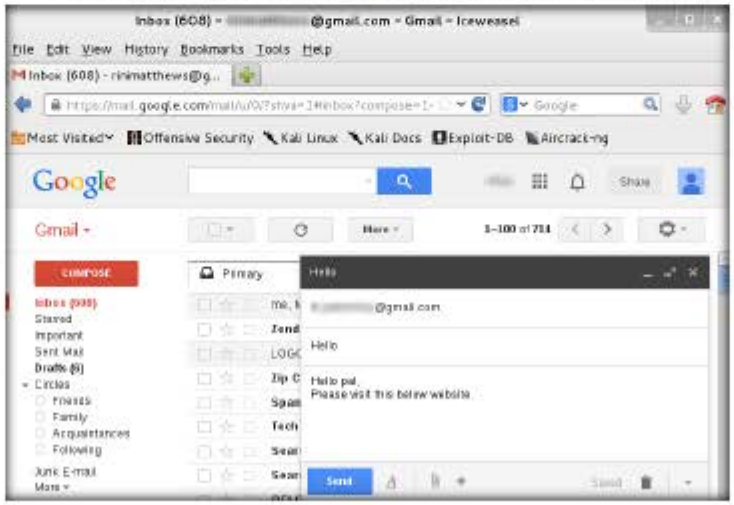
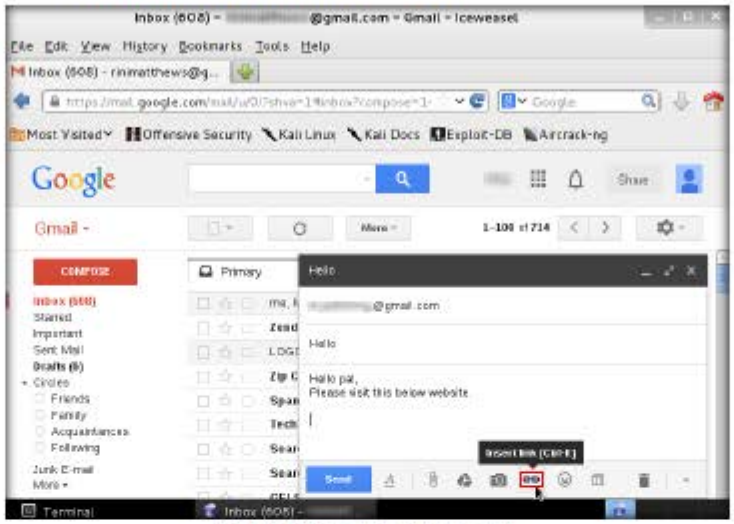


FIGURE 3.11: Composing email in Gmail

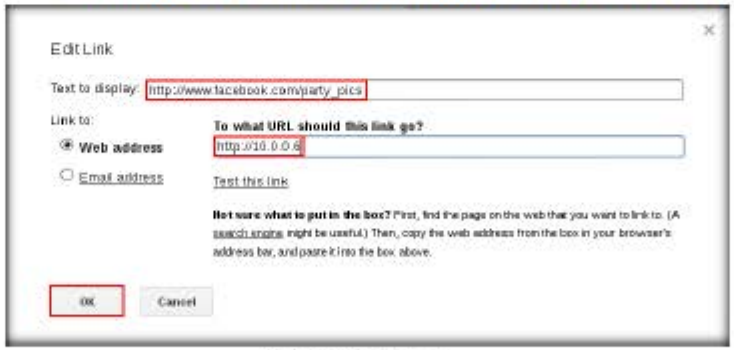
18. In the body of the email, place the cursor where you wish to place the fake URL. Then, click the **Link** icon.



Most of the time they won't even notice the IP but it's just another way to ensure it goes on without a hitch. Now that the victim enters the username and password in the fields, you will notice that we can intercept the credentials now.

FIGURE 3.12: Linking Fake URL to Actual URL

19. In the **Edit Link** window, first type the actual address in **Web address,** under **Link to,** and then type the fake URL in the **Text to display** field. In this example, the Web address we have used is **http://10.0.0.6** the and Text to display is **http://www.facebook.com/party_pics**. Click **OK**.



The multi attack vector utilizes each combination of attacks and allows the user to choose the method for the attack. Once you select one of the attacks, it will be added to your attack profile to be used to stage the attack vector. When you're finished be sure to select the 'I'm finished' option.

FIGURE 3.13: Edit Link window

20. The fake URL should appear in the message body, as shown in the screenshot.

The Credential Harvester Method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

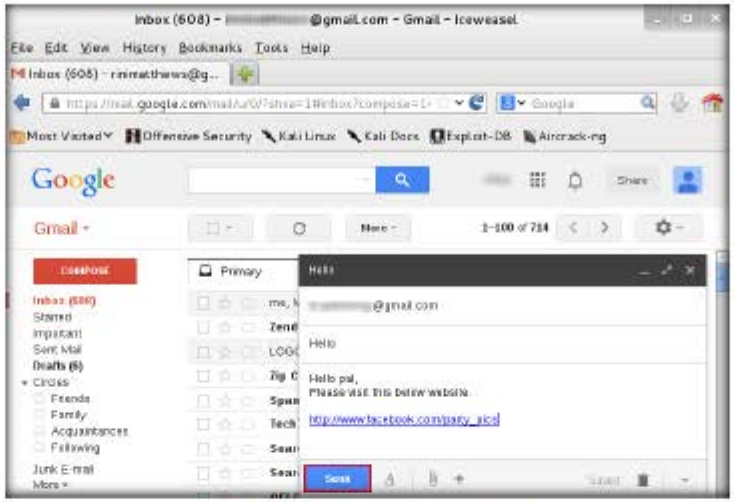


FIGURE 3.14: Adding Fake URL in the email content

21. To verify that the fake URL is linked to the real one, click the fake URL; it will display the actual URL as "**Go to link:**" followed by the actual URL. Send the email to the intended user.

In some cases when you're performing an advanced social-engineer attack you may want to register a domain and buy an SSL cert that makes the attack more believable. You can incorporate SSL based attacks with SET. You will need to turn the WEBATTACK_SSL to ON. If you want to use self-signed certificates you can as well however there will be an "**untrusted**" warning when a victim goes to your website.

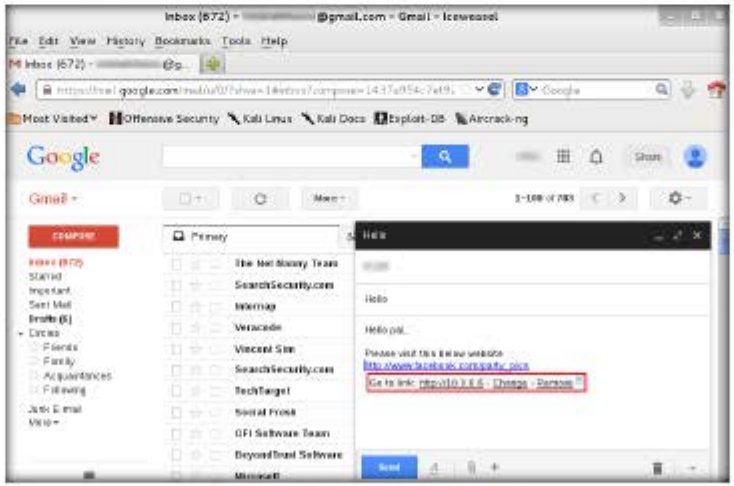


FIGURE 3.15: Actual URL linked to Fake URL

TASK 4

Log in to the Cloned Website

22. Now, log in to Windows Server 2012 as a victim, launch a web browser, sign in to your email account (the account to which you sent the phishing mail as an attacker), and click the malicious link.
23. When the victim (here, you) clicks the URL, he/she will be presented with a **replica** of **facebook.com**.
24. The victim will be prompted to enter his/her username and password into the form fields, being that this appears to be a genuine website. When the victim enters the **Username** and **Password** and clicks **Log In**, it does not allow logging in; instead, it redirects him/her to the legitimate Facebook login page. Observe the URL in the browser.

The multi-attack vector allows you to turn on and off different vectors and combine the attacks all into one specific webpage. So when the user clicks the link he will be targeted by each of the attack vectors you specify. One thing to note with the attack vector is you can't utilize Tabnabbing, Cred Harvester, or Web Jacking with the Man Left in the Middle attack.

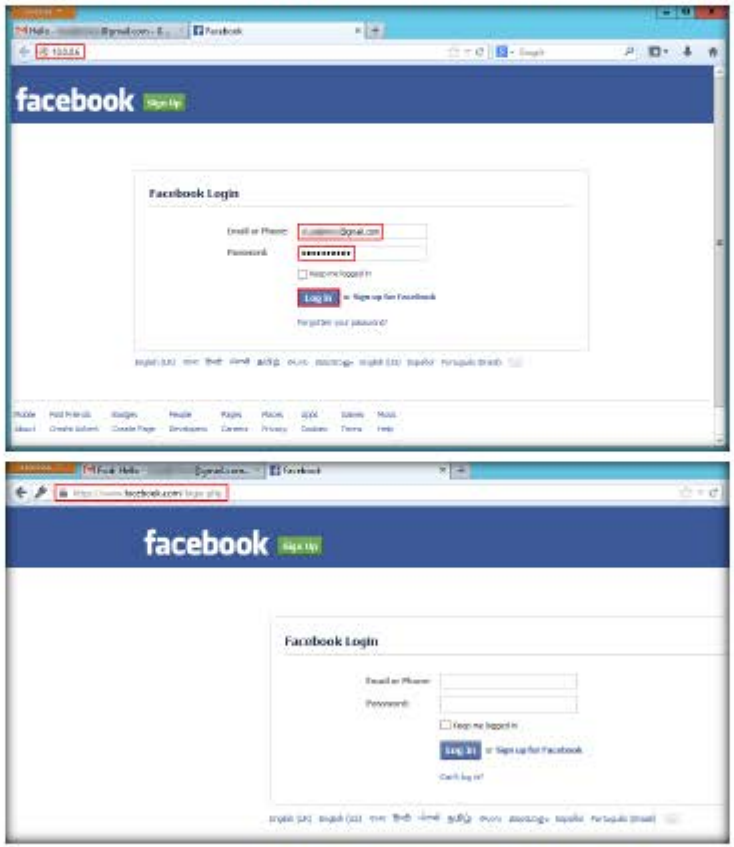


FIGURE 3.16: Fake and Legitimate Facebook login pages

TASK 5

Obtain the Credentials

25. As soon the victim types in the Email address and Password and clicks **Log In**, the **SET Terminal** in Kali Linux **fetches** the typed **Username and Password,** which can then be used by the attacker to gain unauthorized access to the victim's account.

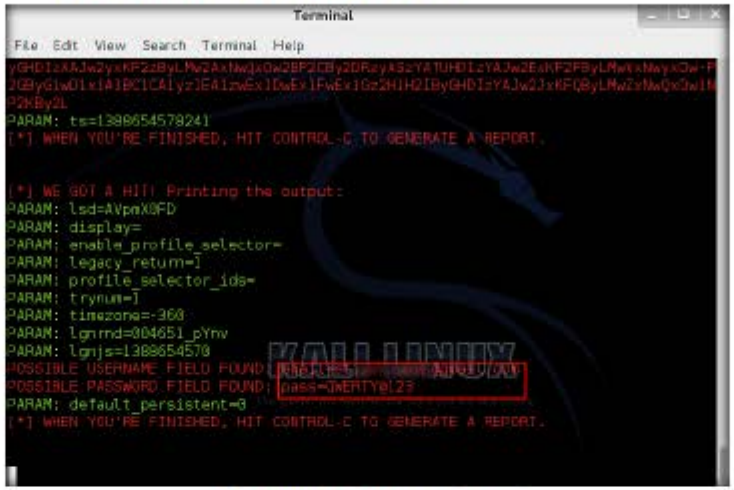


FIGURE 3.17: SET found Username and Password

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

26. Press **CTRL+C** to generate a report for the attack you just performed.

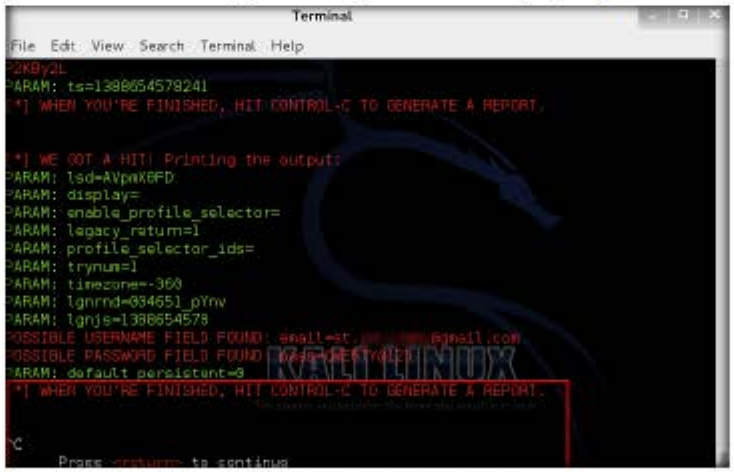


FIGURE 3.18: Generating Reports through SET

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

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 4

Creating a Malicious Payload Using SET and Exploiting a Windows Machine

Metasploit Framework is a tool for developing and executing exploit code against a remote target machine.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Though organizations provide strong security for their networks, there might be insiders who can open up a single gateway, which could possibly impose a drastic effect on the network. Social engineering is one effective technique that allows intruders/attackers to lead unsuspecting victims to reveal sensible information about themselves or their organization. Social engineering not only allows attackers to gain information such as user credentials or credit and debit card numbers, but also control over victims' machines.

You are a Security Administrator of your company, and your responsibilities include protecting your network and cultivating awareness among employees regarding social engineering.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of this lab include:

- Creating a server and testing the network for attack
- Attacking a network using sample backdoor and monitor the system activity

Lab Environment

To complete this lab, you will need:

- A computer running Window Server 2012

- Kali Linux running in virtual machine
- Windows 8.1 running in virtual machine (Victim machine)
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains a malicious or harmful code inside apparently harmless programming or data, in such a way that it can take control and cause damage, such as ruining the file allocation table on a hard drive.

Lab Tasks

Note: Before performing this lab, log in to Kali-Linux virtual machine, click **Places → Computer**. Navigate to **File System → etc → apache2**, open **apache2.conf**, enter the command **servername localhost** in a new line and save the file. If you already did, skip to **Step no. 2**.

TASK 1

Start postgresql and metasploit services

1. Log on to your **Kali Linux** virtual machine.
2. Open terminal console by navigating to **Accessories → Terminal**.

Note: You can either click (**Terminal** icon) in the menu bar to launch the command-line terminal.

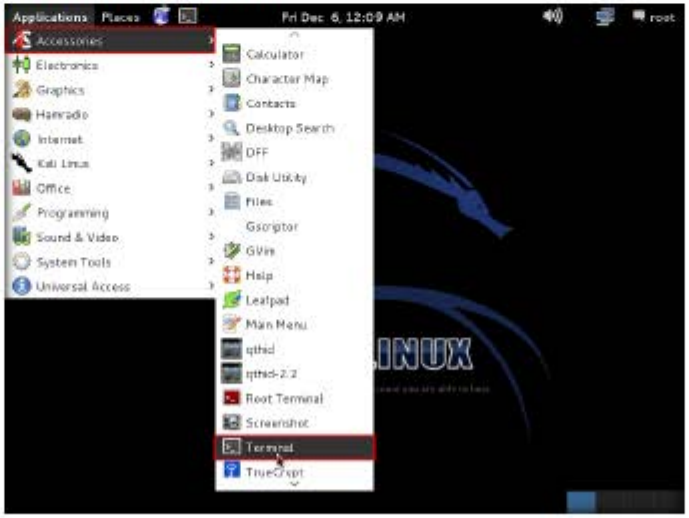


FIGURE 4.1: Launching command line terminal

3. Type the command **service postgresql start** and press **Enter**.

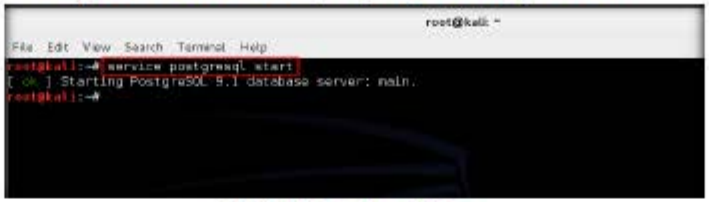


FIGURE 4.2: Starting PostgreSQL Service

4. Type **service metasploit start** and press **Enter**.

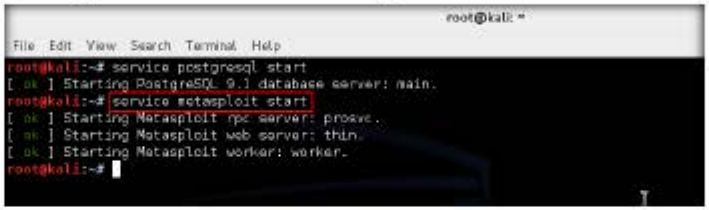


FIGURE 4.3: Starting metasploit Service

TASK 2

Create payload.exe file and Share it

5. Open a new command-line terminal, type **mkdir /var/www/share** and press **Enter** to create a new directory named **share**.

Note: If the directory is already created, skip to the next step.

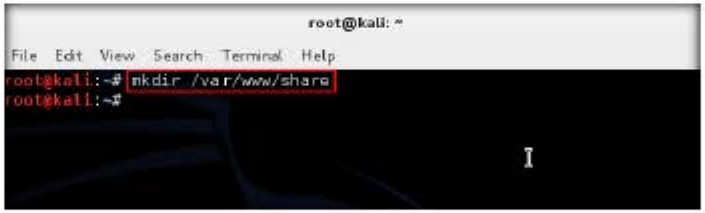


FIGURE 4.4: Creating the directory

6. Change the permissions of the **share** folder to **755** by typing the command **chmod -R 755 /var/www/share/** and pressing **Enter**.

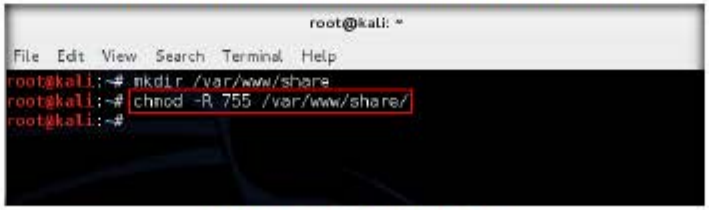


FIGURE 4.5: Changing the folder mode into 755

7. Change the folder ownership to **www-data** by typing **chown -R www-data:www-data /var/www/share/** and pressing **Enter**.

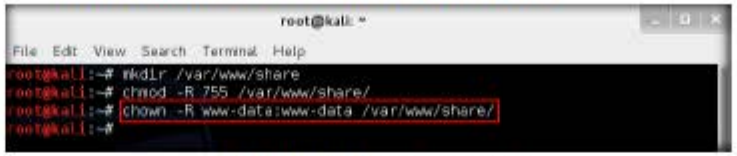


FIGURE 4.6: Change the ownership of the folder

8. Type **ls -la /var/www/ | grep share** and press **Enter**.

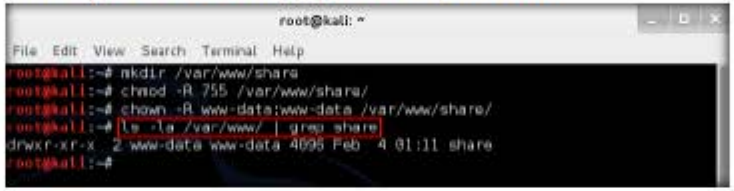


FIGURE 4.7: Sharing the directory

9. Go to **Applications → Kali Linux → Exploitation Tools → Social Engineering Toolkit → se-toolkit**.

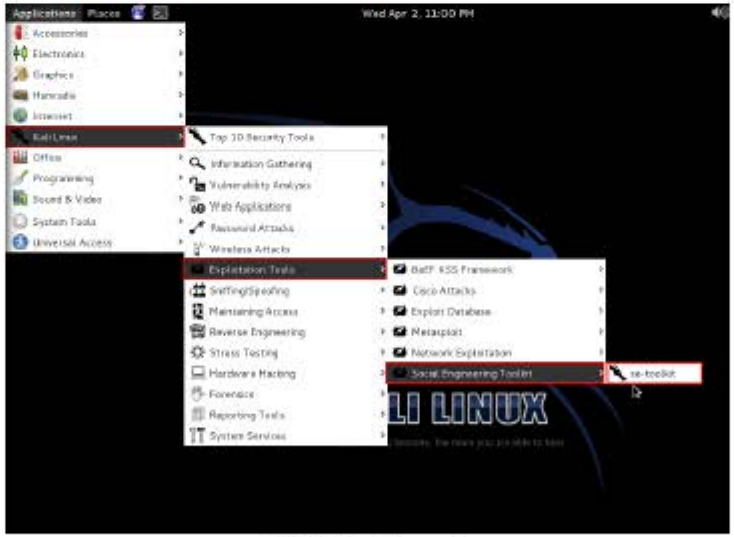


FIGURE 4.8: Launching se-toolkit

10. Social Engineering Toolkit UI appears; type **1** and press **Enter** to choose **Social - Engineering Attacks**.

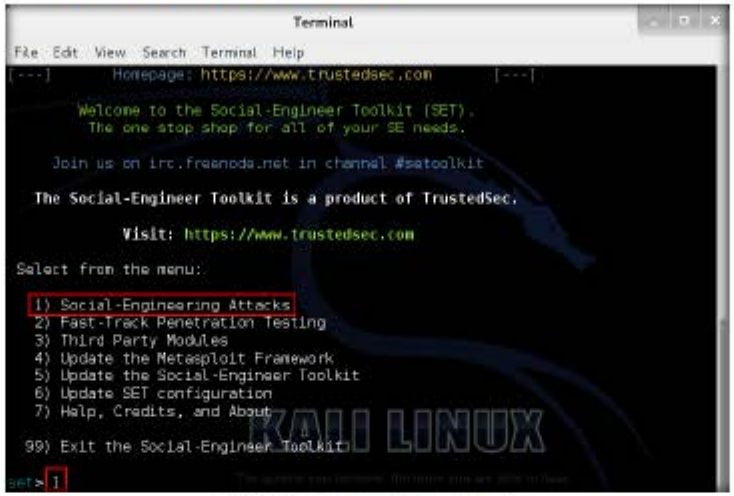


FIGURE 4.9: choosing Social Engineering Attacks

11. SE Toolkit displays a list of social engineering attacks. Type **4** and press **Enter** to **Create a Payload and Listener**.

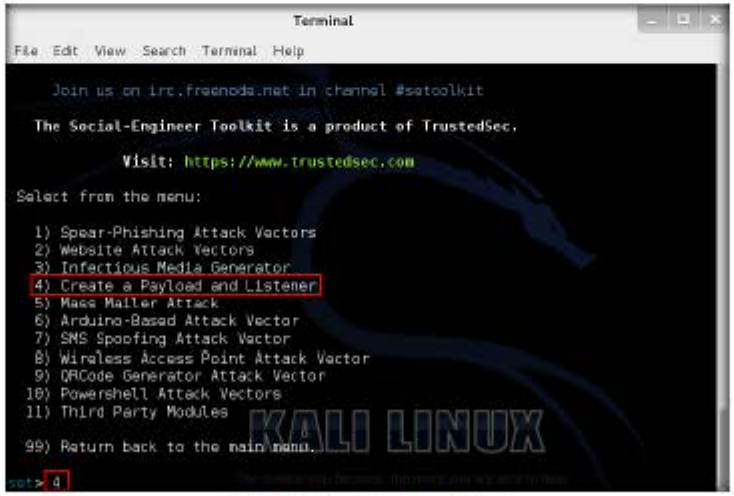


FIGURE 4.10: Creating a Payload and Listener

12. Type the IP address for the payload (here, **10.0.0.5**) and press **Enter**.

Note: **10.0.0.5** is the IP address of **Kali Linux** virtual machine, which may vary in your lab environment.

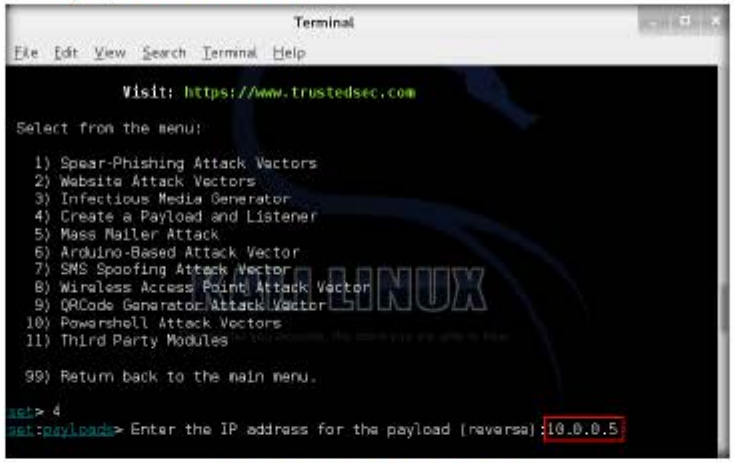


FIGURE 4.11: Entering IP address for the payload

13. You will be provided with a list of payloads. Type **7** and press **Enter** to choose **Windows Meterpreter Reverse_TCP X64** payload.

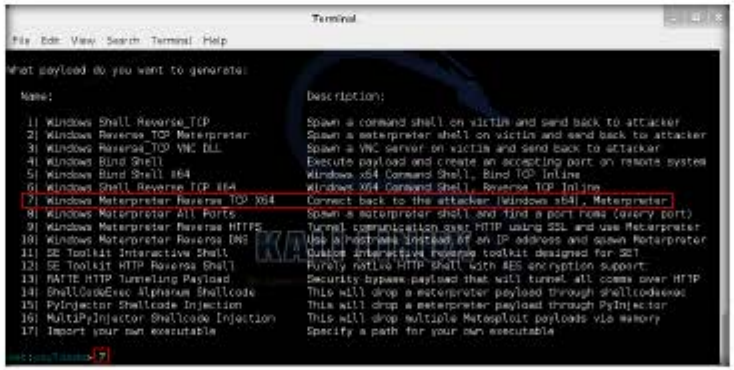


FIGURE 4.12: Choosing Windows Meterpreter Reverse_TCP X64 payload

14. Press **Enter** to choose the default port (i.e, **443**).

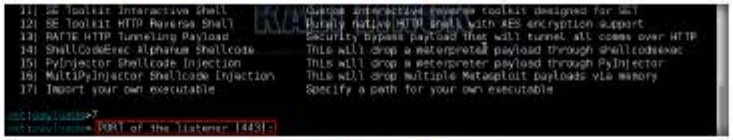


FIGURE 4.13: Choosing default port

15. The payload is created in the name **payload.exe** and is stored in the location **usr/share/set**.

16. Type **yes** and **press** Enter. This initiates the listener.

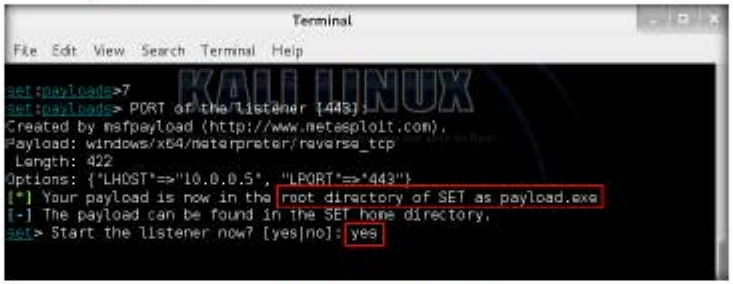


FIGURE 4.14: Starting the listener

17. The payload handler starts, as shown in the following screenshot:

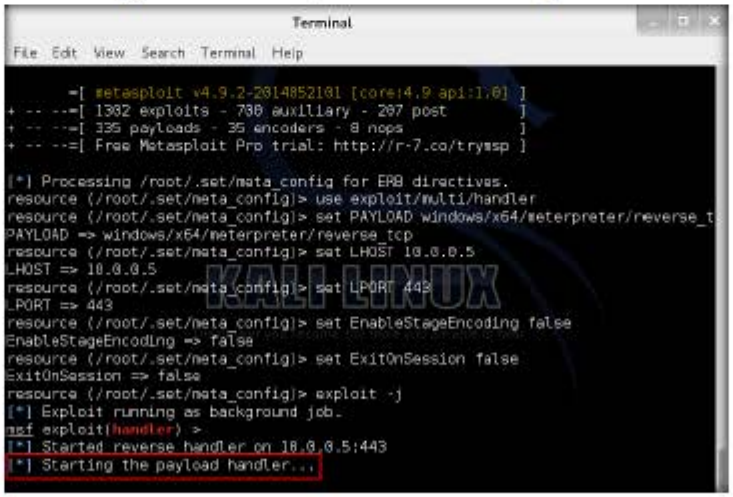


FIGURE 4.15: Payload handler begun

18. Go to **Computer → File System,** and navigate to **usr/share/set**. Copy **payload.exe,** and paste it to **var/www/share**.

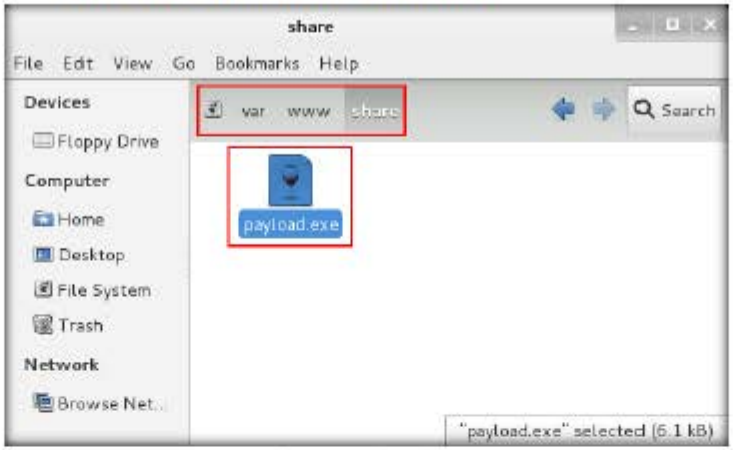


FIGURE 4.16: Pasting payload.exe

19. Open a new command-line terminal, type **service apache2 start** and press **Enter** to start the apache server.

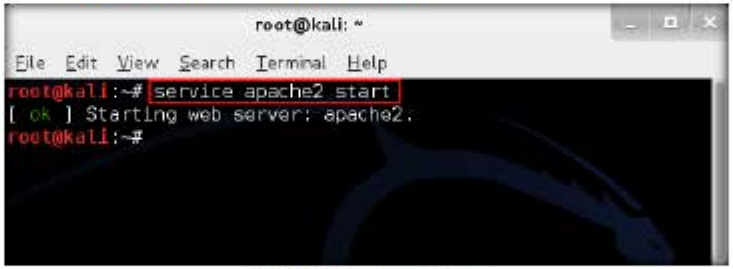


FIGURE 4.17: Starting apache2 server

20. **Close** the terminal.
21. Now, craft an email containing the direct download link of this file, and send it to the intended victim. In this lab, assume that you are only the victim who has Windows 8.1 installed on his/her machine.
22. Log in to **Windows 8.1** virtual machine as the victim.

TASK 3

Execute the payload

23. Launch Firefox or any web browser, type **http://10.0.0.5/share/** in URL field, and press **Enter**.
24. In real time, the victim clicks on the malicious link that was sent in the crafted mail.

    Note: Here **10.0.0.5** is the IP address of **Kali Linux**, which may vary in your lab environment.
25. Click **payload.exe** link to download the payload.

FIGURE 4.18: Downloading the payload

26. The **Opening payload.exe** pop-up appears; click **Save File**.

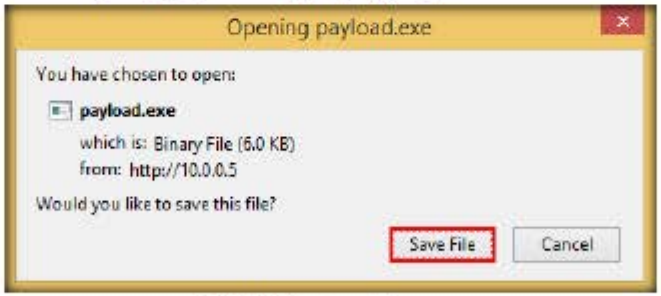


FIGURE 4.19: Opening payload.exe pop-up

27. By default, this file is stored in **C:\Users\Admin\Downloads**.

28. On completion of the download, a download notification appears in the browser. Click the **download** icon, and click **Open Containing Folder**.

FIGURE 4.20: Opening the folder where payload is downloaded

29. Double-click **payload.exe**. The **Open File - Security Warning** appears; click **Run**.

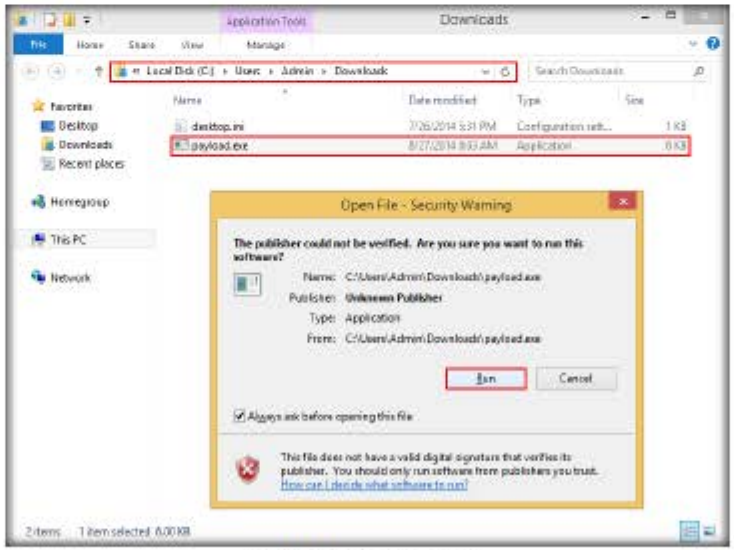


FIGURE 4.21: Executing the payload

30. Switch back to Kali Linux machine. The Meterpreter session has been successfully opened.
31. Type **sessions -i** and press **Enter** to view the active sessions.

Note: The active sessions and session IDs may vary in your lab environment.

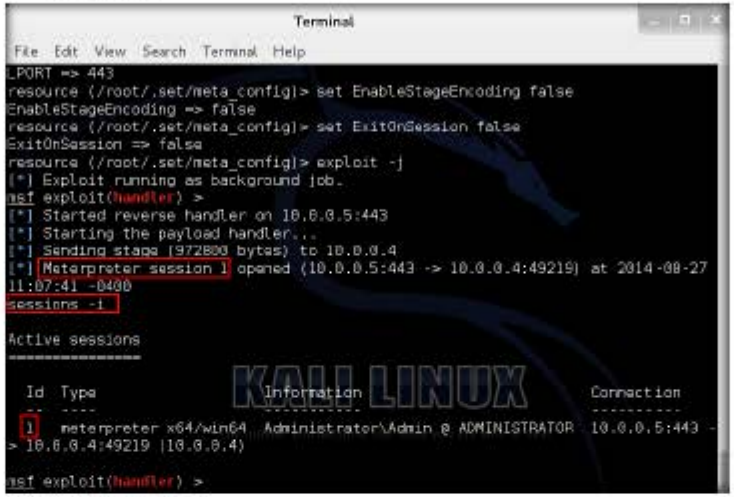


FIGURE 4.22: Viewing the active sessions

32. Type **sessions –i 1** command and press **Enter** (**1** in **sessions –i 1** command is the id of the session). **Meterpreter** shell is launched, as shown in the following screenshot:

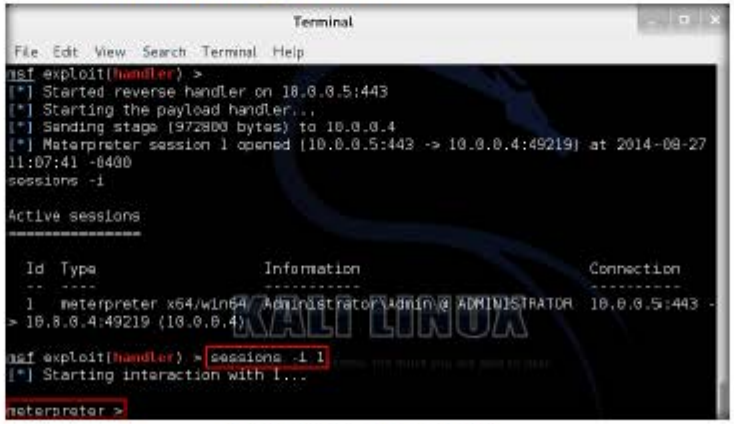


FIGURE 4.23: Launching meterpreter shell

TASK 4

Perform Post Exploitation

33. Type **help** and press **Enter**.

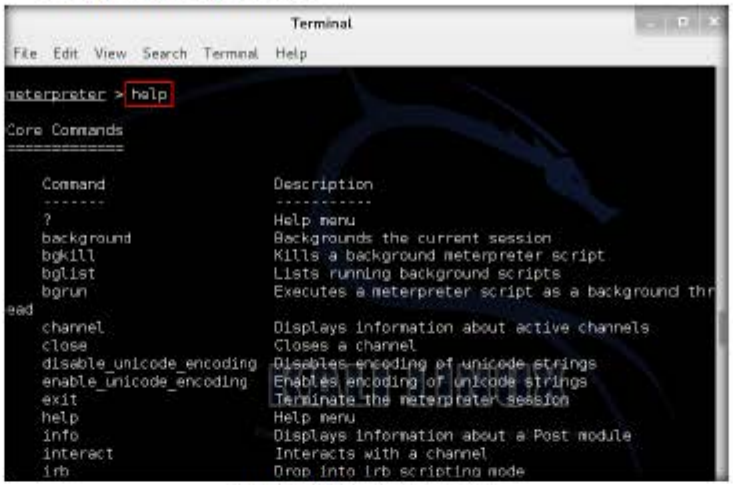


FIGURE 4.24: Meterpreter help commands

34. You may issue any of these commands to interact, explore, or exploit the victim machine.

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs