Social Engineering

Module 09

Social Engineering

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

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.

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 2016
- Kali Linux virtual machine

- Windows 10 virtual machine
- A Web browser with Internet access
- Administrative privileges to run the tools

Lab Duration

Time: 30 Minutes

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)
- Phishing User Credentials using **SpeedPhish Framework** (SPF)

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.

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 an 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 to the 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:

- You can 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 2016
- 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

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

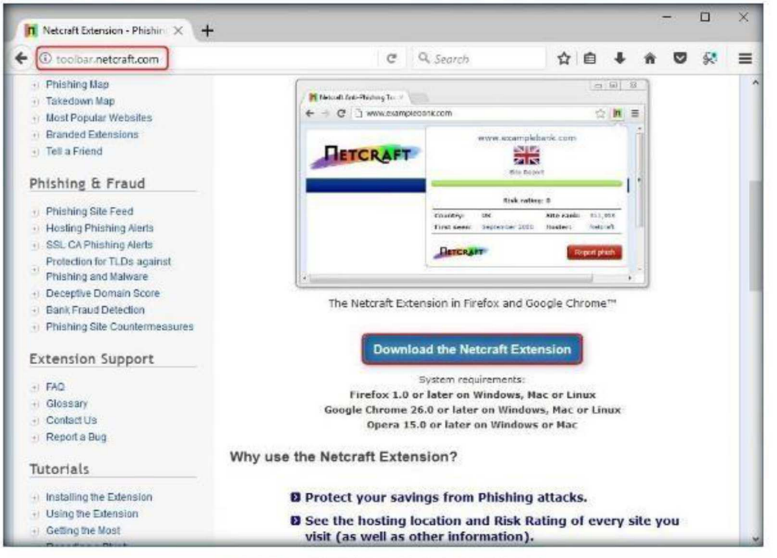


FIGURE 1.1: Netcraft toolbar downloading Page

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

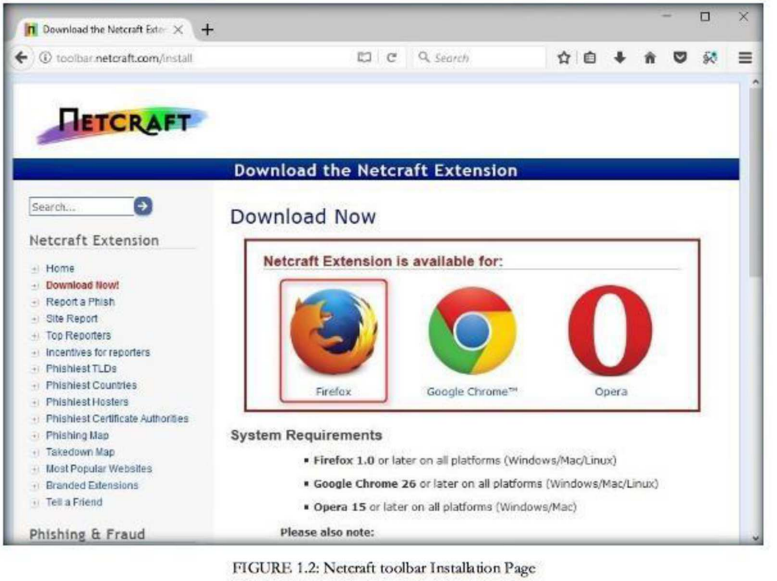


FIGURE 1.2: Netcraft toolbar Installation Page

5. Click **Add to Firefox** to download Netcraft Toolbar.

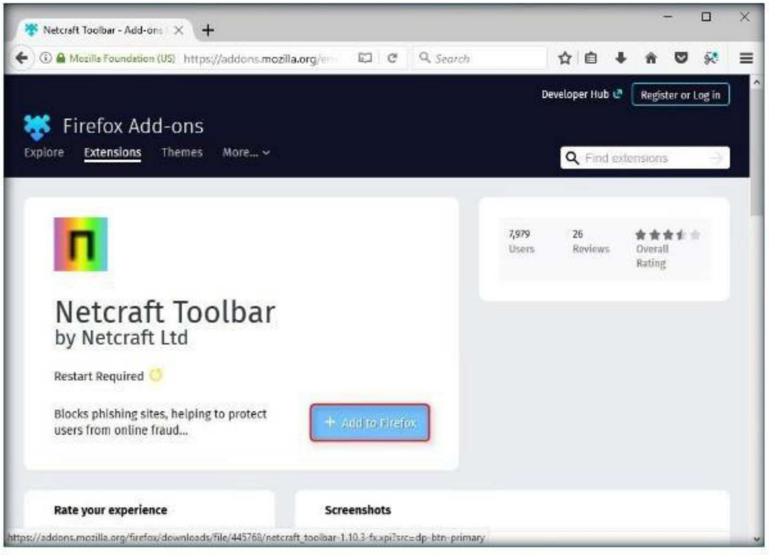


FIGURE 1.3: Netcraft toolbar Installation- Add to Firefox button

6. Click **Add**.

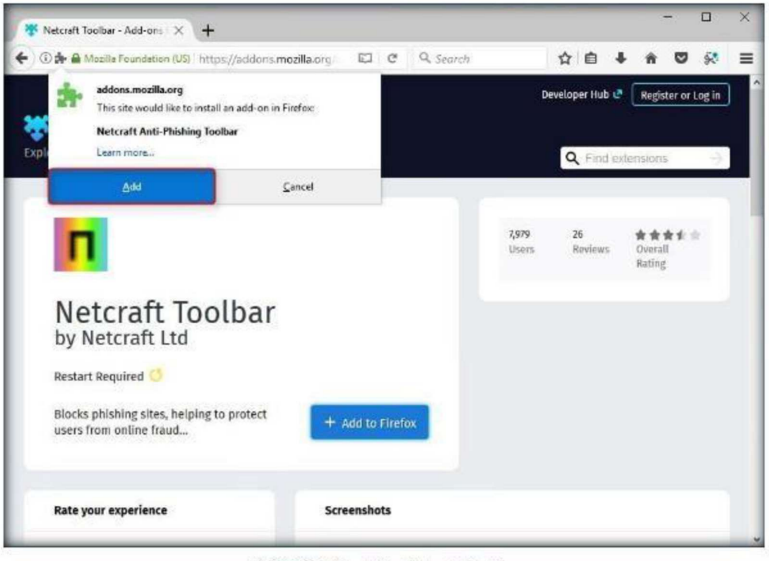


FIGURE 1.4: Installing Netcraft Toolbar

7. To complete the installation, if you are asked to restart the browser; click **Restart Now**.

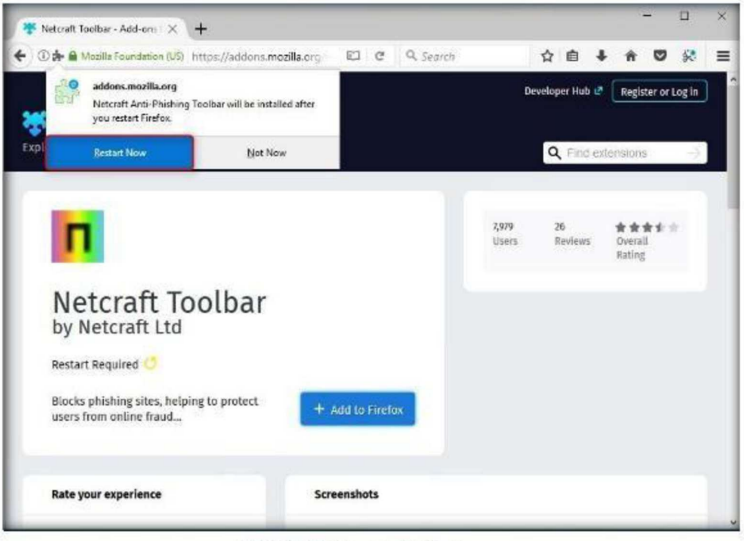


FIGURE 1.5: Restarting Firefox browser

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

Note: Screenshots may differ with newer versions of Firefox.

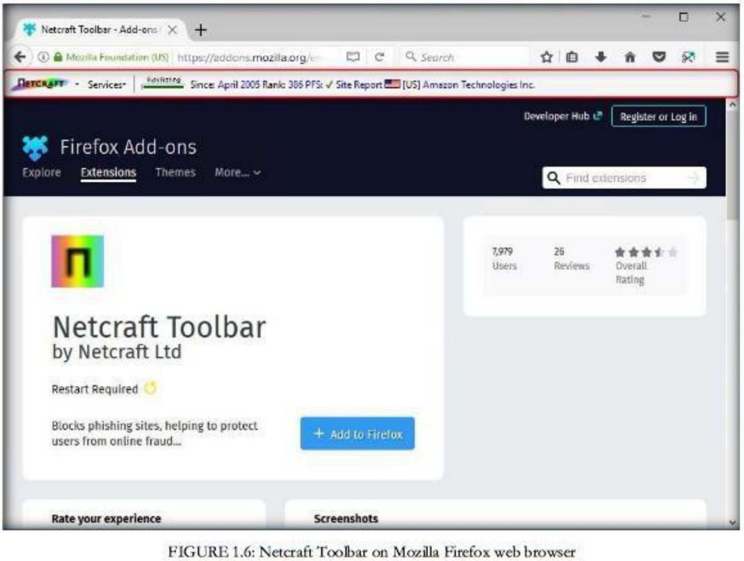


FIGURE 1.6: Netcraft Toolbar on Mozilla Firefox web browser

9. Open a new tab, type the URL **http://www.certifiedhacker.com** in the address bar, and press **Enter**.

10. 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**.

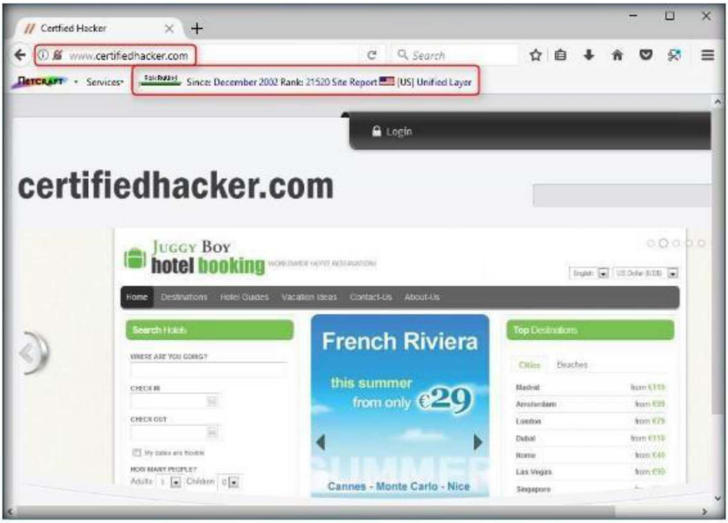


FIGURE 1.7: Netcraft Toolbar on Mozilla Firefox web browser

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

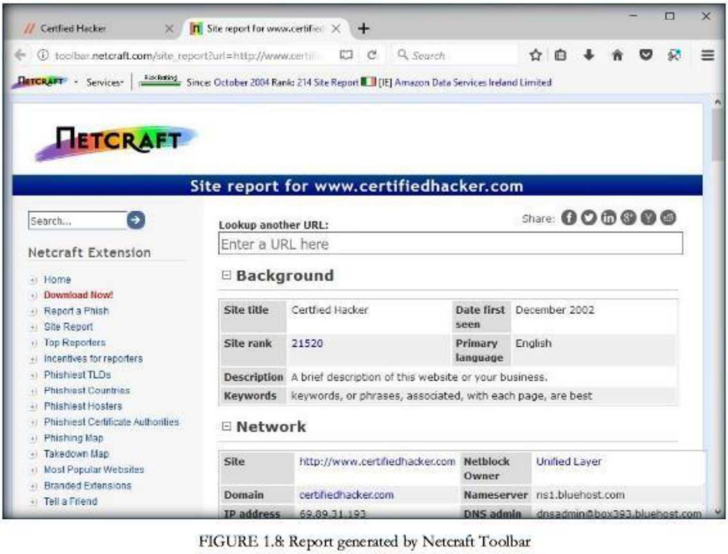


FIGURE 1.8: Report generated by Netcraft Toolbar

12. 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:

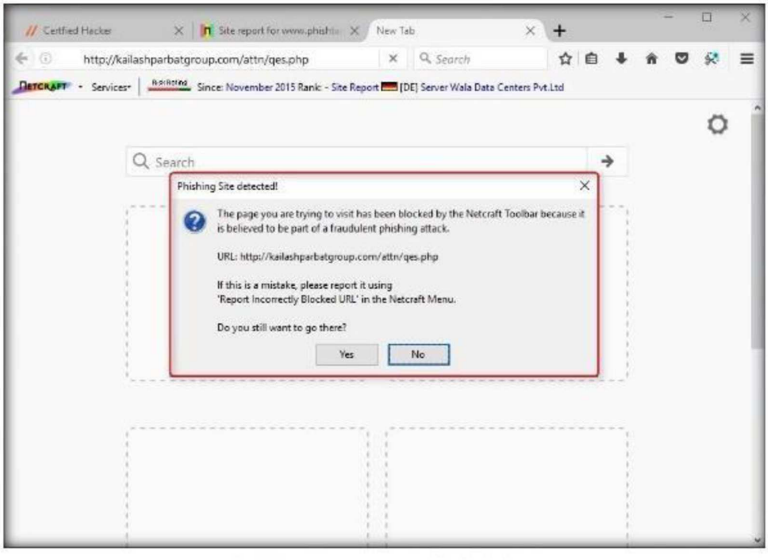


FIGURE 1.9: Warning pop-up for blocked site

13. If you trust the site, click **Yes** to browse it; otherwise, click **No** (Recommended) to block it.

14. 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.

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

Lab Environment

To carry out this lab, you will need:

- A computer running Windows Server 2016
- A Web browser (Firefox, Internet Explorer, etc.) with Internet access

Lab Duration

Time: 5 Minutes

Overview of PhishTank

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

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:

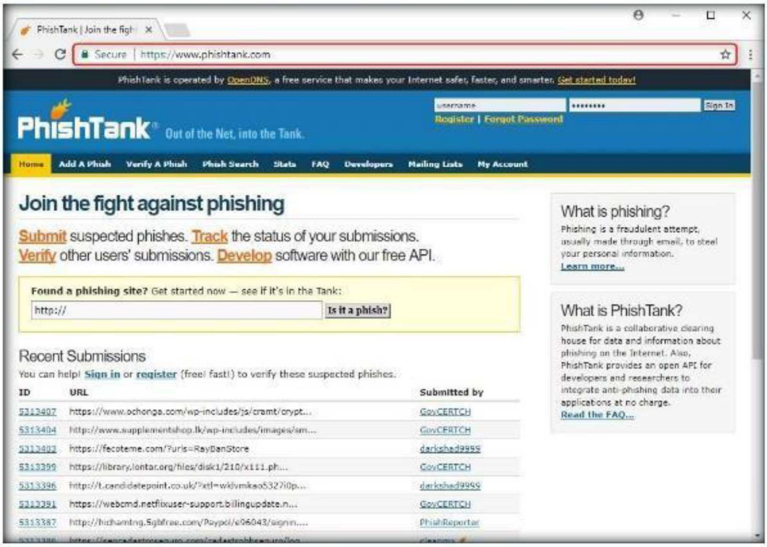


FIGURE 2.1: Welcome screen of PhishTank

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?**

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:

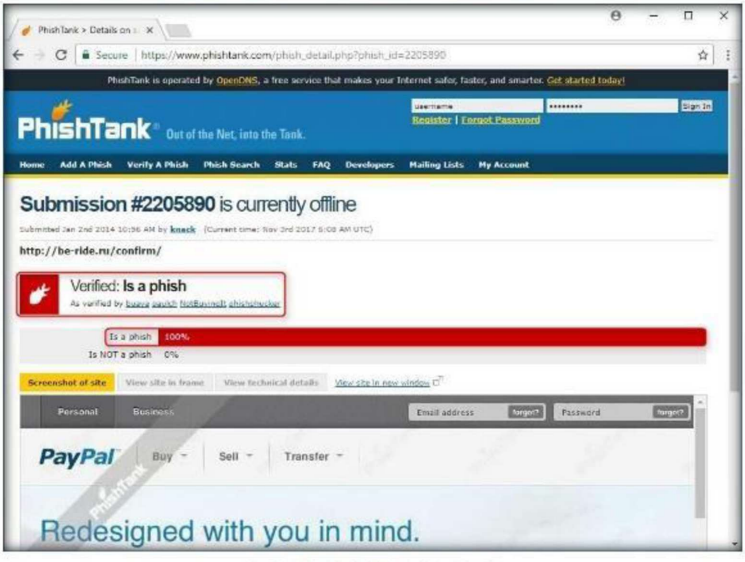


FIGURE 2.3: Phishing website found

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

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

To carry out this lab, you will need:

- Kali Linux Virtual Machine
- Windows Server 2016 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. Log in to **Kali Linux** virtual machine.
2. Go to **Applications → 08 - Exploitation Tools → social engineering toolkit**.

FIGURE 3.1: Launching SET in Kali Linux

3. 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**.

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

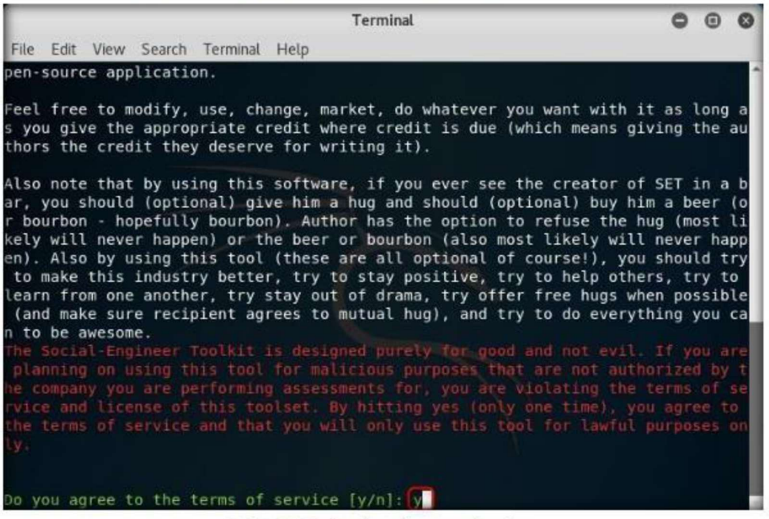


FIGURE 3.2: Agreeing to the terms of services

5. You will be presented with the SET menu.

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

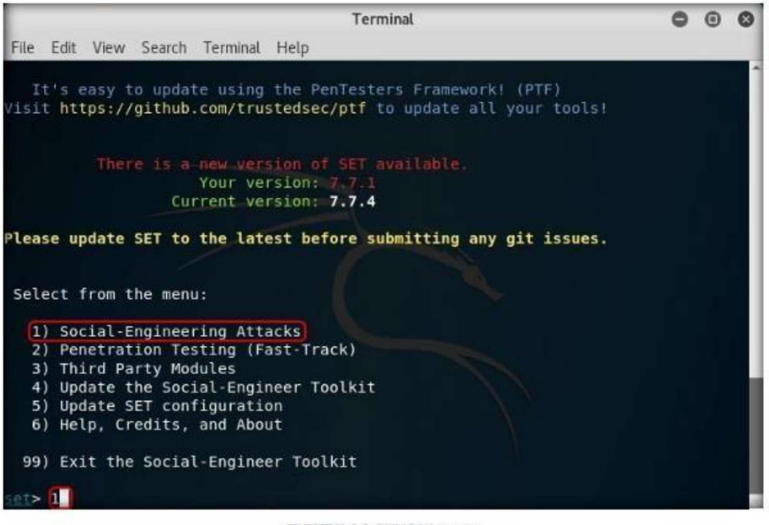


FIGURE 3.3: SET Main menu

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

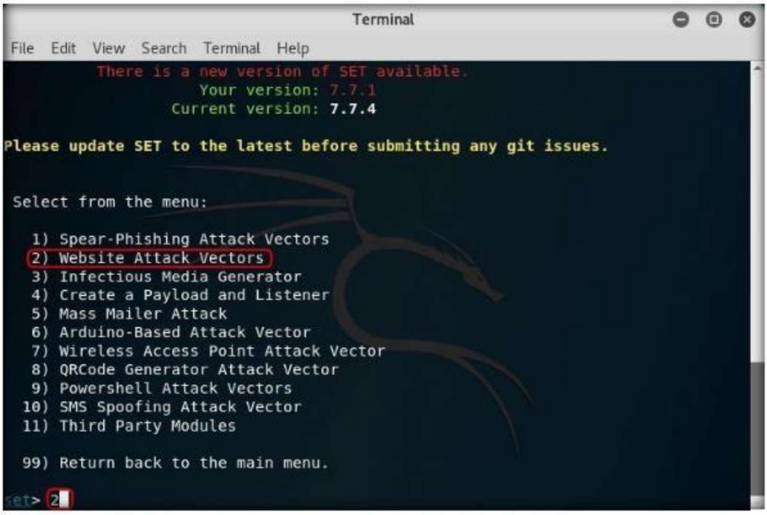


FIGURE 3.4: Choosing Website Attack Vectors

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

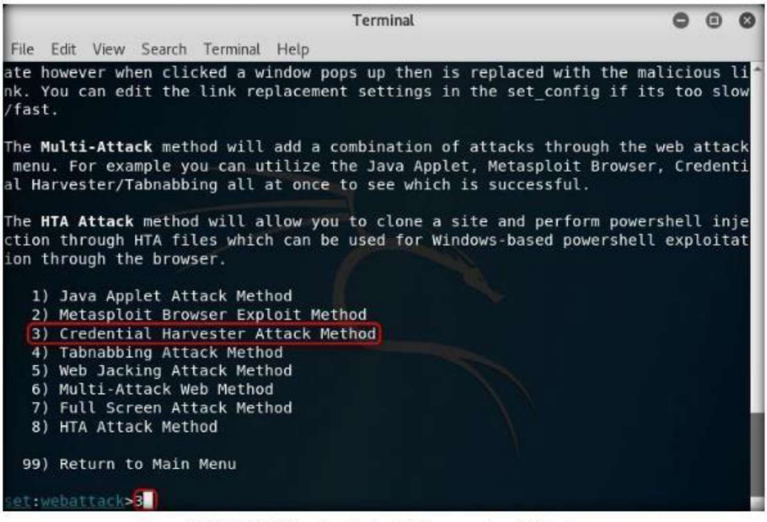


FIGURE 3.5: Choosing Credential Harvester Attack Method

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

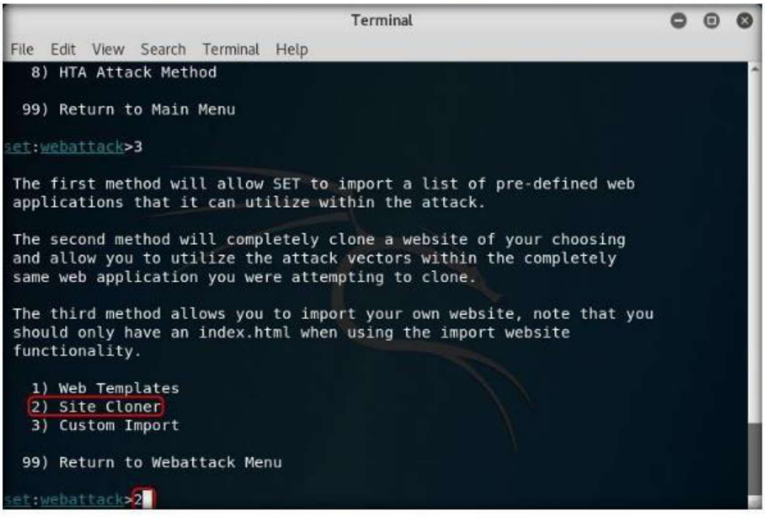


FIGURE 3.6: Choosing Site Cloner

10. 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 **10.10.10.11**, which may vary in your lab environment.

FIGURE 3.7: Providing IP address in Harvester/Tabnabbing

11. 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 **https://www.facebook.com**. This will initiate the cloning of the specified website.

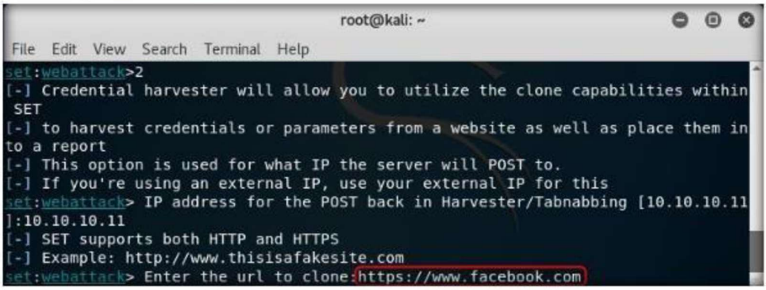


FIGURE 3.8: Providing URL to be cloned

Note: If you are prompted to start apache server:

12. After cloning is completed, the highlighted message as in the below screenshot will appear on the **Terminal** screen of **SET**. Press **Enter** to continue.

13. It will start Credential Harvester.

FIGURE 3.9: SET Website Cloning

14. Now, you must send the **IP address** of your **Kali Linux** machine to a victim, and trick him or her to **click to browse** the IP address.

15. For this demo, launch a web browser in the **Kali Linux** machine, and launch an email service of your interest. In this lab, we have used **Gmail**. Login to a Gmail account and compose an email.

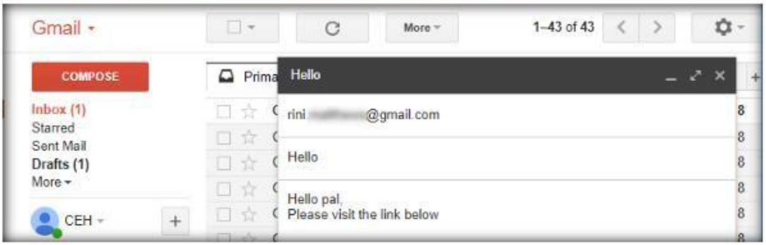


FIGURE 3.10: Composing email in Gmail

16. In the body of the email, place the cursor where you wish to place the fake URL. Then, click the **Insert link** icon.

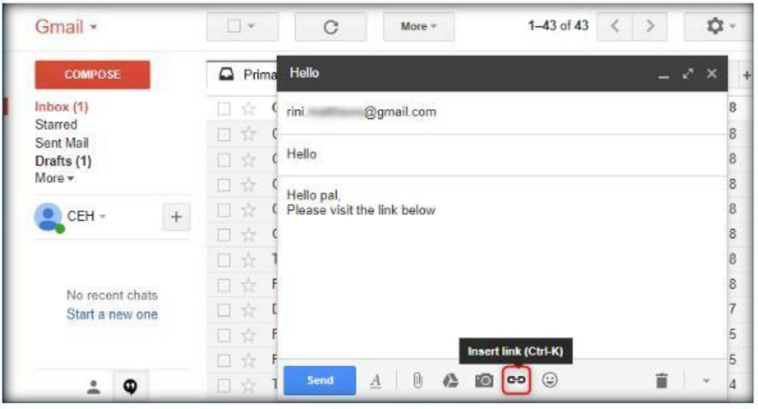


FIGURE 3.11: Linking Fake URL to Actual URL

17. 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://10.10.10.11** and Text to display is **https://www.facebook.com/party_pics**. Click **OK**.

FIGURE 3.12: Edit Link window

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

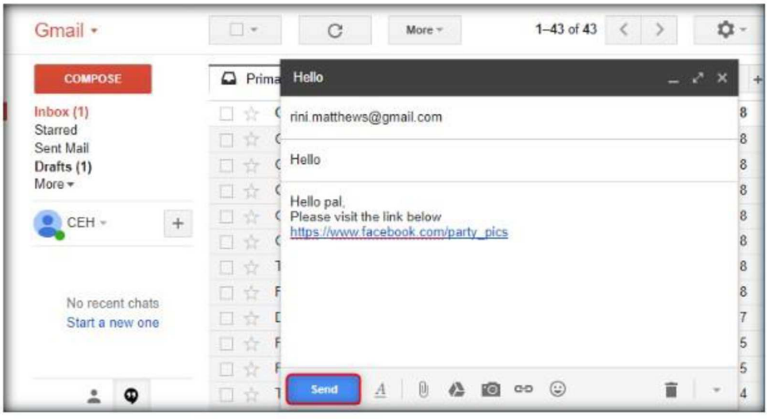


FIGURE 3.13: Adding Fake URL in the email content

19. 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.

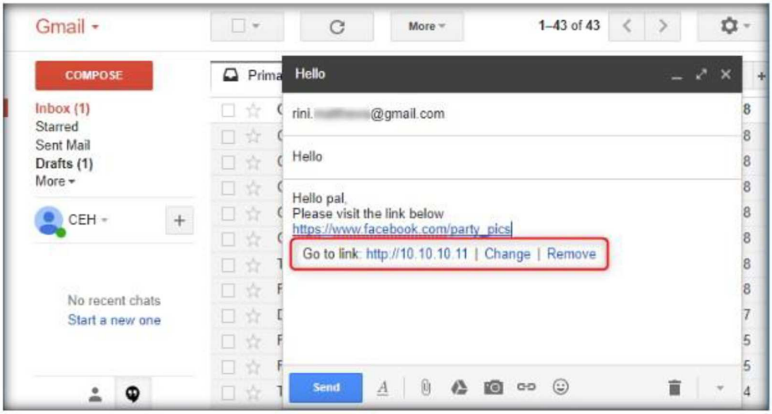
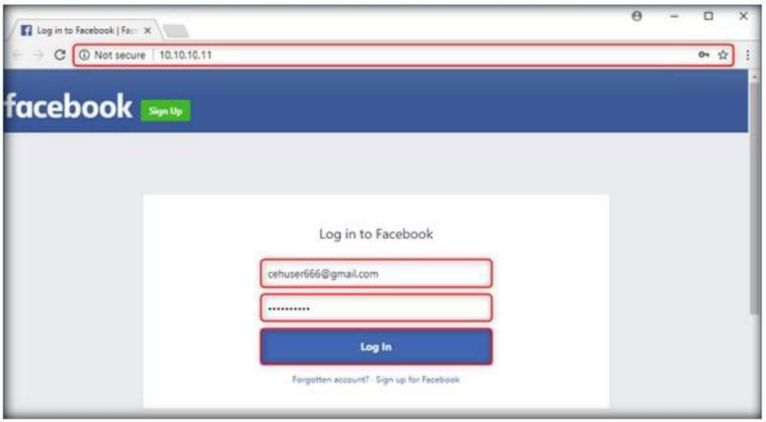


FIGURE 3.14: Actual URL linked to Fake URL

20. Now, log in to Windows Server 2016 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.

21. When the victim (here, you) clicks the URL, he/she will be presented with a **replica** of **facebook.com**.

22. 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.



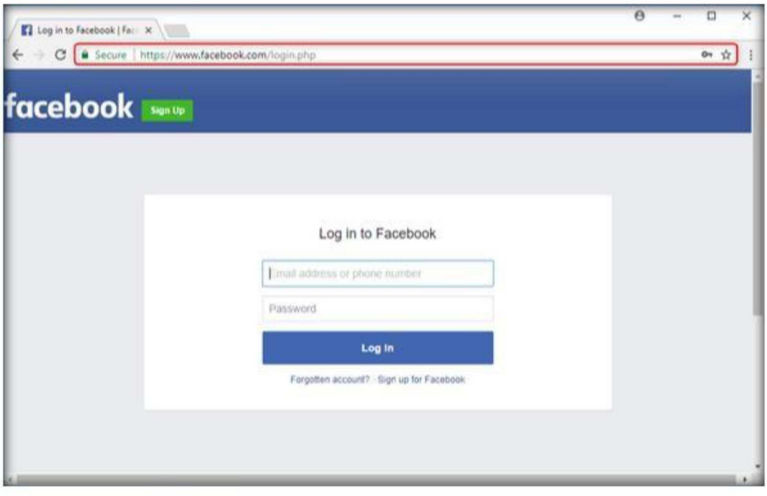


FIGURE 3.15: Fake and Legitimate Facebook login pages

23. As soon as the victim types in the Email address and Password and clicks **Log In**, the **SET** 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.

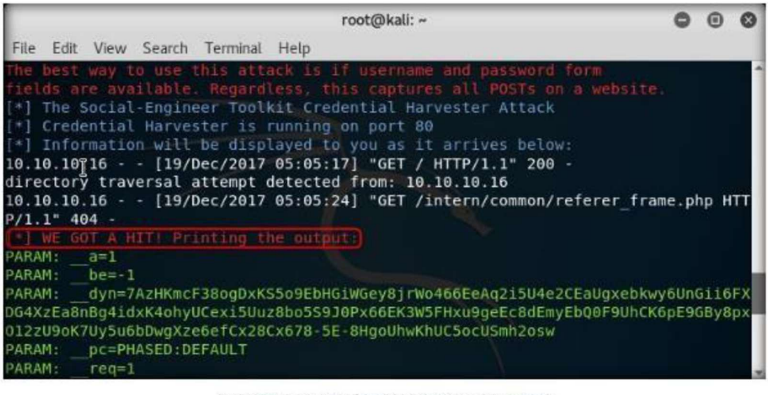


FIGURE 3.16: SET found Username and Password

24. The username and password are displayed as shown in the screenshot.

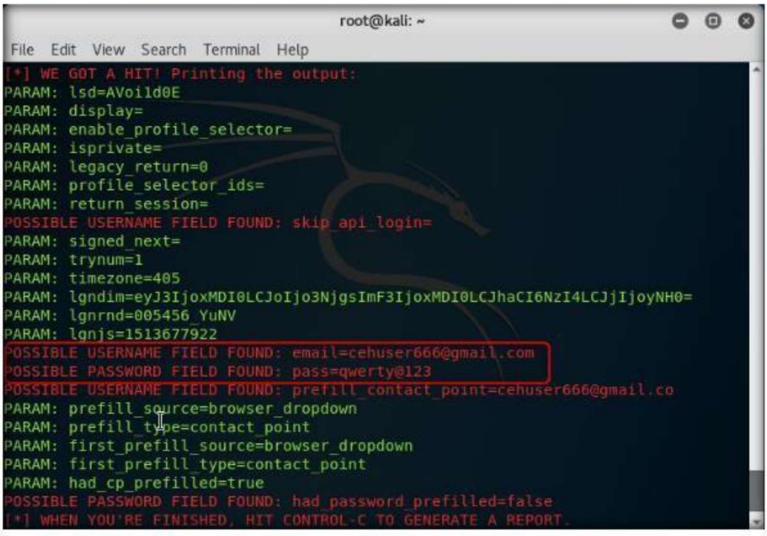


FIGURE 3.17: Generating Reports through SET

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

Phishing User Credentials using SpeedPhish Framework (SPF)

SPF (SpeedPhish Framework) is a python tool designed to allow for quick recon and deployment of simple social engineering phishing exercises.

Lab Scenario

Social Engineering attacks are used to compromise companies every day. They are an increasing threat to organizations all over the globe. Even though there are many hacking tools available throughout hacking communities, SpeedPhish Framework (SPF) 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 numerous people using SPF.

As an Ethical Hacker, Penetration Tester, or Security Administrator, you should be familiar with the SpeedPhish Framework to perform various tests for assessing the security posture of an organization.

Lab Objectives

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

- Clone a website
- Obtain username and passwords
- Generate reports for conducted penetration test

Lab Environment

To carry out this lab, you will need:

- Kali Linux Virtual Machine
- Windows Server 2016 machine
- Windows 10 running as virtual machine
- Web browser with Internet access

- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of the SpeedPhish Framework

The SpeedPhish Framework (SPF) is an open-source Python-driven tool aimed at penetration testing. The SPF is specifically designed to perform advanced phishing attacks. The attacks built into the framework are designed to be targeted and focused against a person or organization used during a penetration test. It includes many features that allow you to quickly configure and perform effective phishing attacks.

Lab Tasks

1. Log in to **Kali Linux** virtual machine with the following credentials: **root/toor.**
2. Launch a Terminal window and type **pip install dnspython** and press **Enter.**

Note: If the dependencies are already installed, skip to **step 6.**

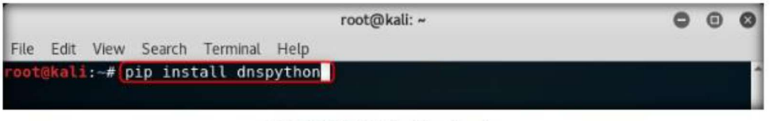


FIGURE 4.1: Installing Dependencies

3. Now type **pip install pycrypto** and hit **Enter.**

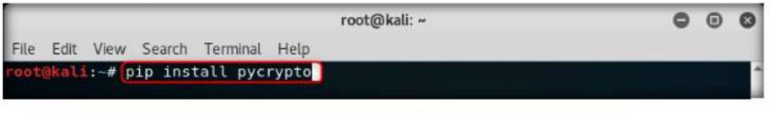


FIGURE 4.2: Installing Dependencies

4. Now to install python-twisted-web, type **apt-get install python-twisted-web** in the terminal window and hit **Enter.**

FIGURE 4.3: Installing Dependencies

5. To install phantomjs, type **apt-get install phantomjs** in the terminal window and hit **Enter**.

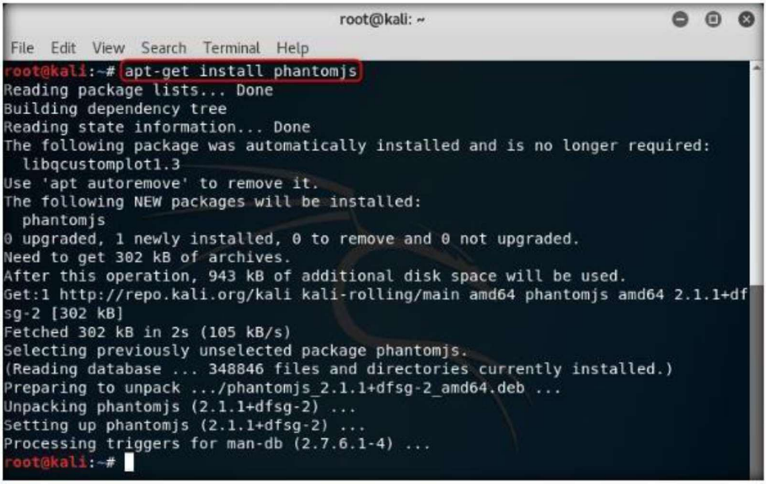


FIGURE 4.4: Installing Dependencies

6. After the dependencies have finished installing, in the terminal window type **git clone --recursive https://github.com/tatanus/SPF.git** and hit **Enter**.

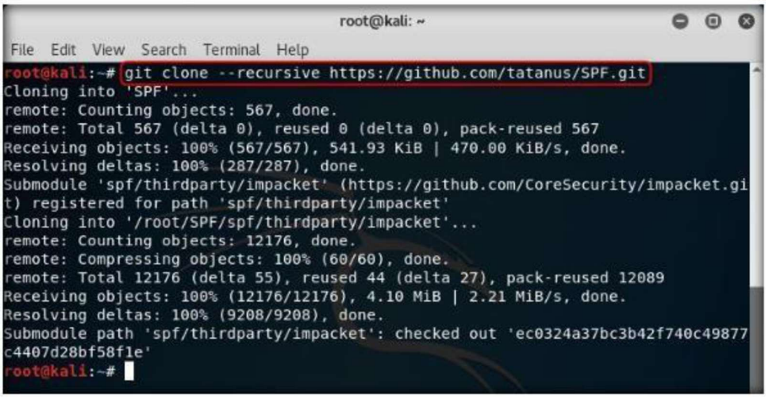


FIGURE 4.5: Cloning SPF to Kali machine

7. After the cloning is finished, type **cd SPF** and hit **Enter**.

FIGURE 4.6: Changing Directory

8. Again, type **cd spf** and hit **Enter**.

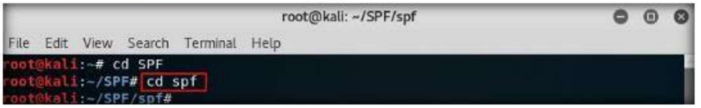


FIGURE 4.7: Changing directory

9. Now to launch SPF, type **./spf.py -h** and hit **Enter**. Help page of SPF appears as shown in the screenshot.

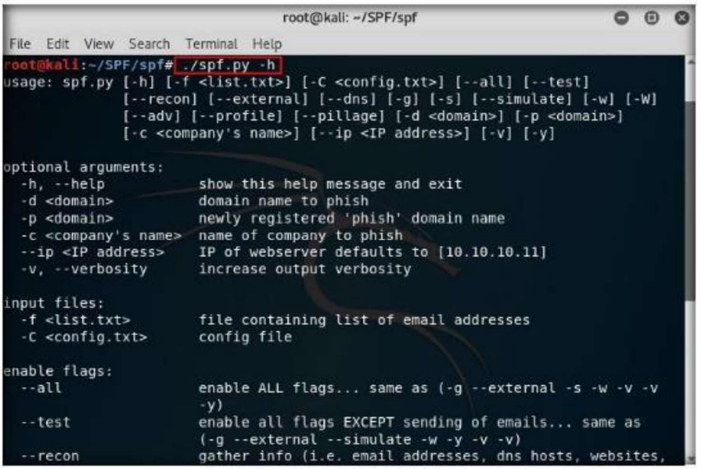


FIGURE 4.8: Viewing help options

10. To check the configuration of SPF, type **cat default.cfg** and hit **Enter**. The configuration details appear as shown in the screenshot.

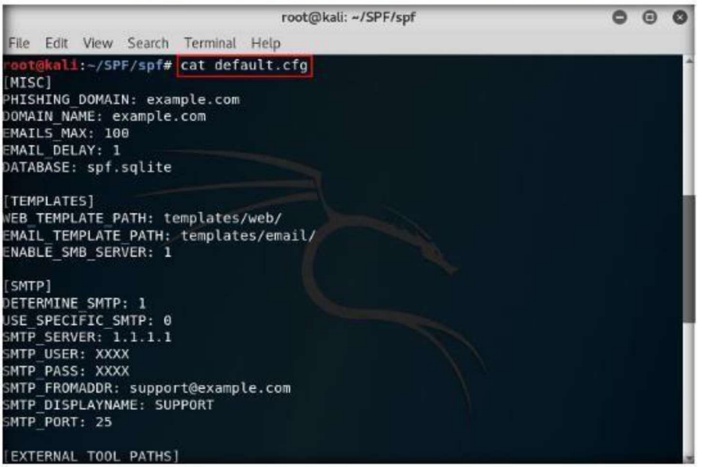


FIGURE 4.9: Viewing the configuration file

11. In the terminal window type **./spf.py -d example.com --test** and hit **Enter** to run SPF.

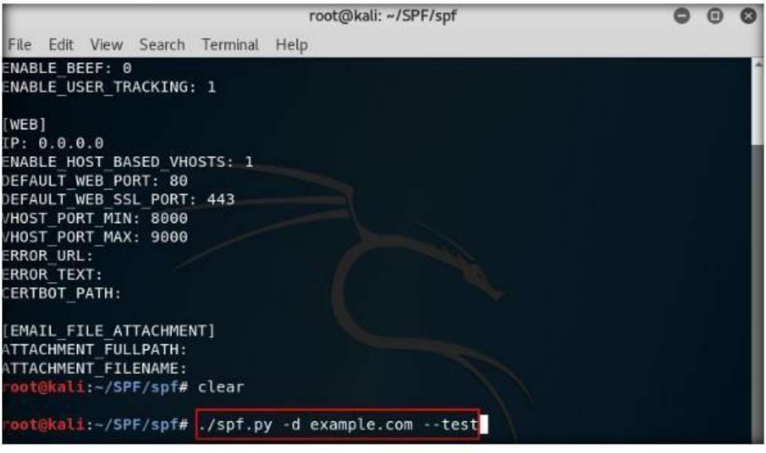


FIGURE 4.10: Running spf.py

12. SPF starts by showing you the **TEMPLATE LIST** first, and then it proceeds to **Starting the phishing webserver** as shown in the screenshot.

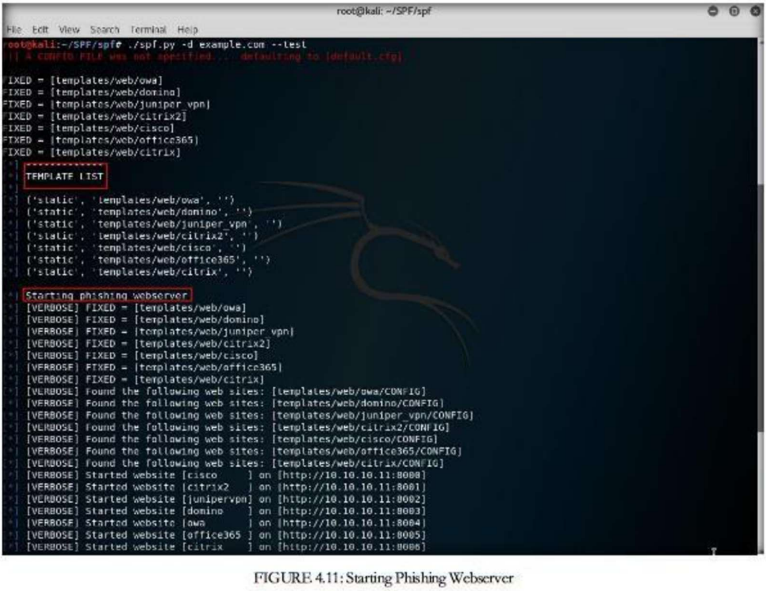


FIGURE 4.11: Starting Phishing Webserver

13. SPF then proceeds to **Starting the SMB server**, and then it obtains the **List of email targets** and displays them as shown in the screenshot.

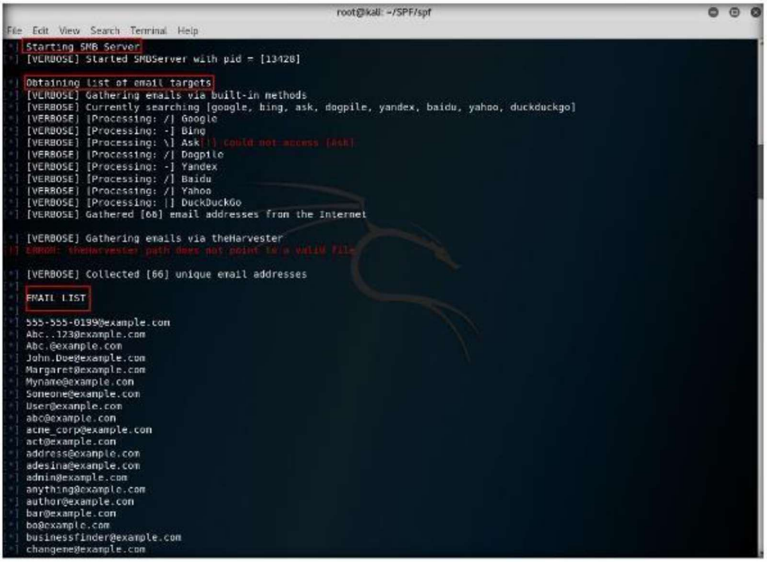


FIGURE 4.12: Obtaining Email List

14. Then SPF starts **Locating phishing email templates** and starts **Sending phishing emails** one by one as shown in the screenshot.

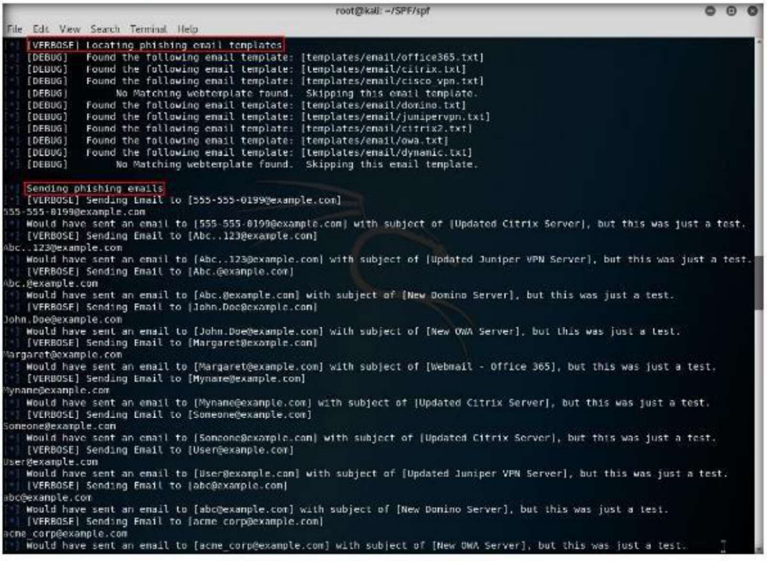


FIGURE 4.13: Locating and Sending Phishing emails

15. After SPF finishes sending phishing emails, it starts **Monitoring Services** as shown in the screenshot.

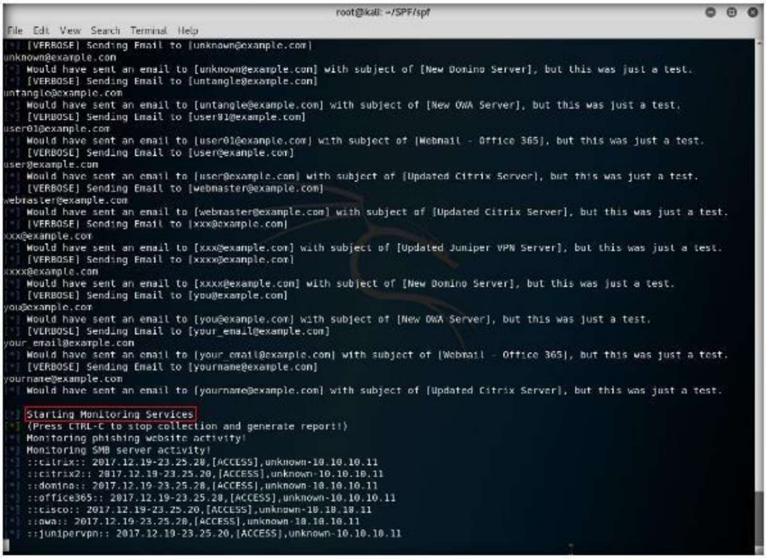


FIGURE 4.14: Starting Monitoring Services

16. Locate and note down the website address of **Office 365** as shown in the screenshot.

Note: The website addresses may differ in your lab environment.

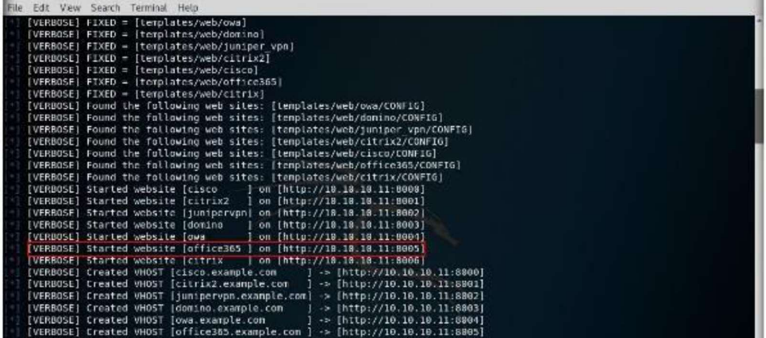


FIGURE 4.15: Phishing webpage link

17. Also locate and note down the location of the **email template** for **Office 365** as shown in the screenshot.

Note: The file location may differ in your lab environment.

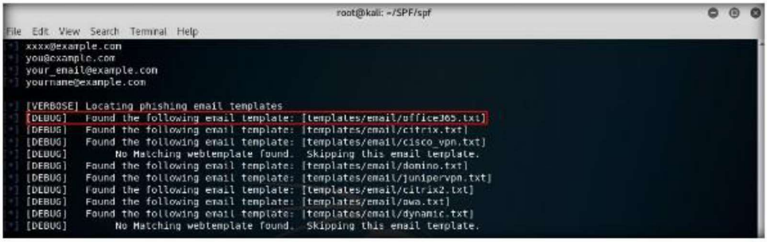


FIGURE 4.16: Location of the phishing email template

18. Now navigate to the location of the phishing email template and open **office 365.txt**. The file opens giving you a template, which you will use to send a phishing email to the victim. Use the content of this template to compose a phishing email.

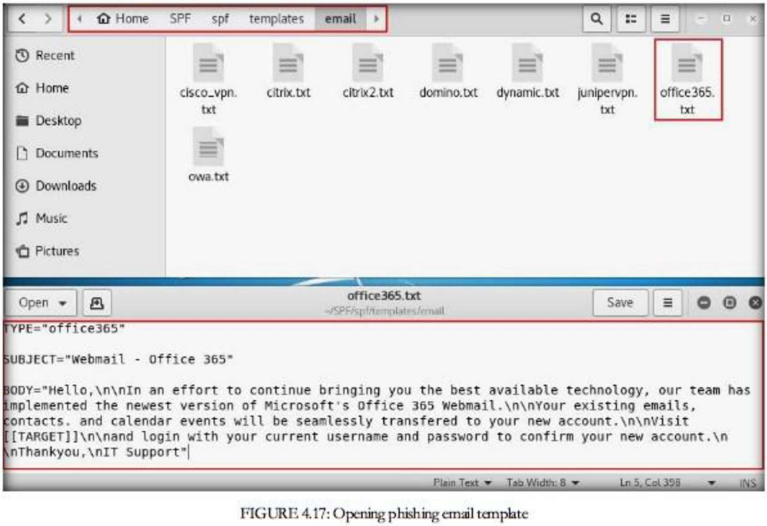


FIGURE 4.17: Opening phishing email template

19. Masquerading as an IT Support professional, you write an email to the victim with the purpose of making him/her click on the phishing link obtained in step 16.

20. After composing the email, select **Click here** and click the **Insert link** option as shown in the screenshot.

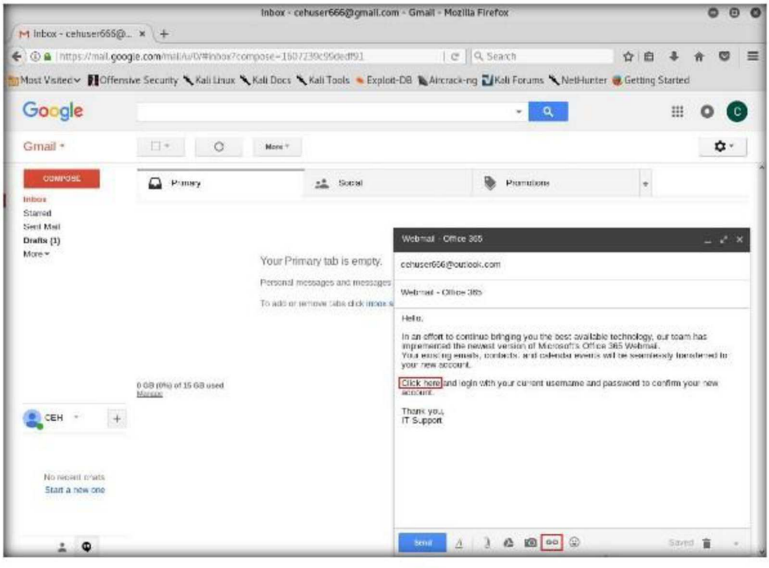


FIGURE 4.18: Composing phishing email

21. When the **Edit Link** window appears, enter the phishing URL in **Web address** box and click **OK** as shown in the screenshot.

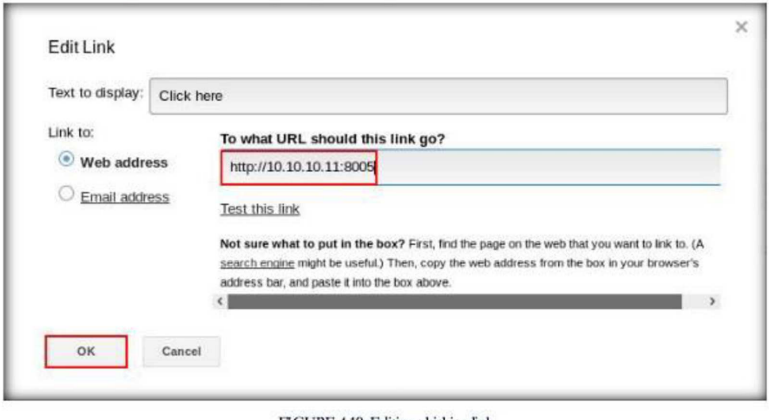


FIGURE 4.19: Editing phishing link

22. The URL has been linked to **Click here** text as shown in the screenshot. Now send the e-mail to the victim.

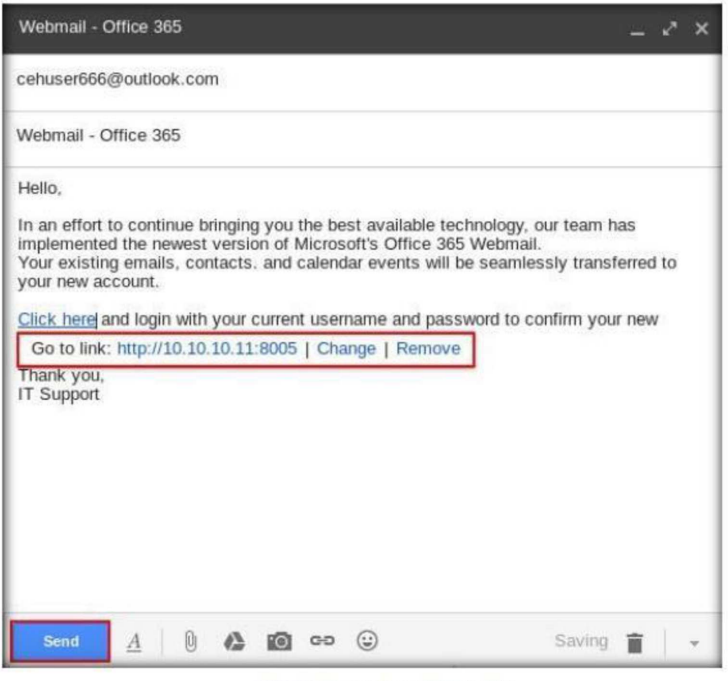


FIGURE 4.20: Sending the phishing email

23. Switch to **Windows 10** machine as the victim and open the victim email account.

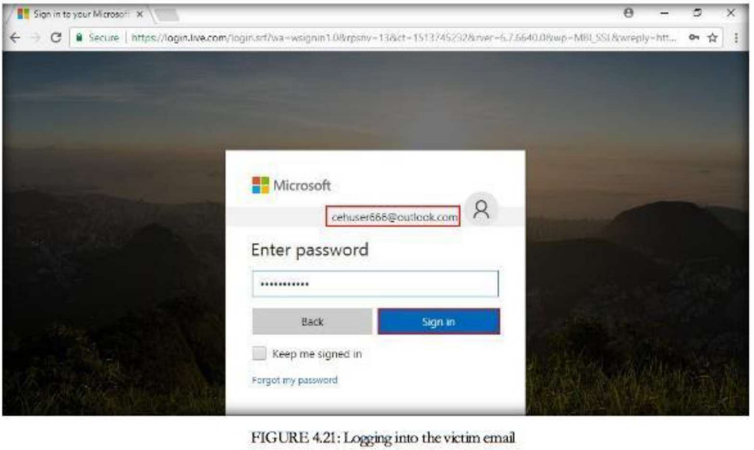


FIGURE 4.21: Logging into the victim email

24. You will see an email from the attacker as shown in the screenshot.

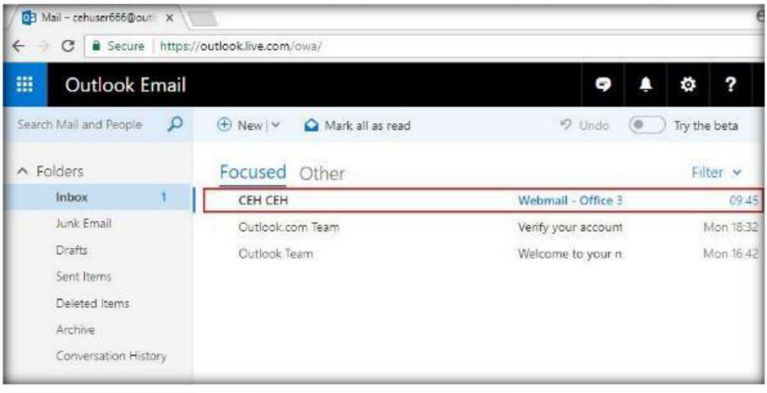


FIGURE 4.22: Phishing email Received

25. Open the email and move your mouse over the **Click here** text, you can see the browser shows the link to which it redirects to, as given in the screenshot. An unsuspecting user may not be aware of this and will visit the malicious webpage.

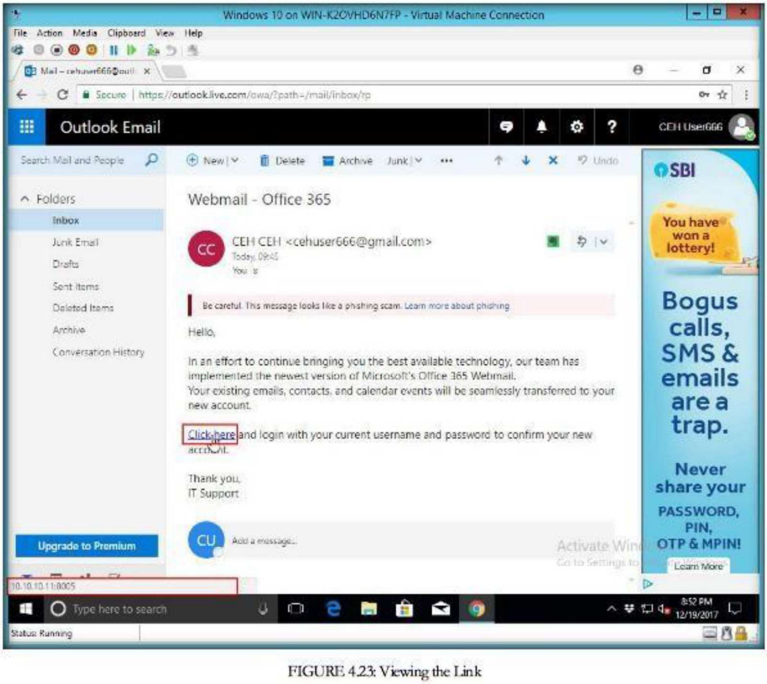


FIGURE 4.23: Viewing the Link

26. When you click the link, you are taken to a webpage which looks exactly like the Office 365 login page, but if you take a closer look at the URL you will notice that it is the malicious phishing link. Enter your user credentials and click **Sign In**.

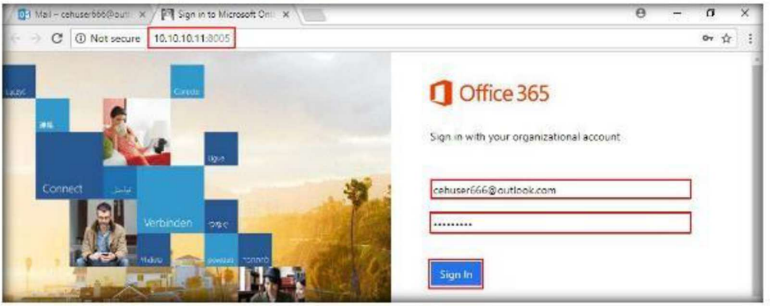


FIGURE 4.24: Malicious Login Page

27. You will get a message on your browser that an error has occurred, as shown in the screenshot. At this point, your credentials have been successfully hacked by the attacker.

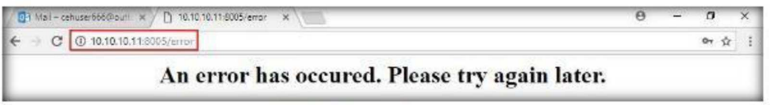


FIGURE 4.25: Error Page after Login

28. Now when you switch back to **Kali Linux** machine and open the **terminal**, you will see that SPF has obtained the victim's credentials as shown in the screenshot.

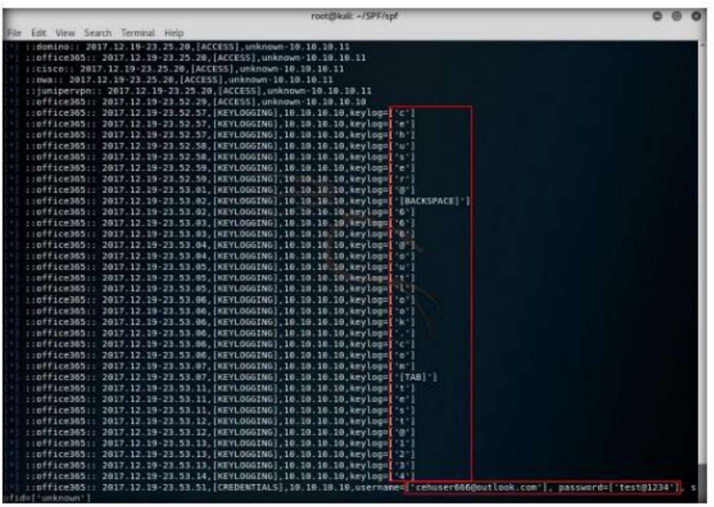


FIGURE 4.26: SPF Displaying Captured User Credentials

29. Press **Ctrl+C** to stop SPF and generate a **report**. SPF exits and displays the location of the report file as shown in the screenshot.

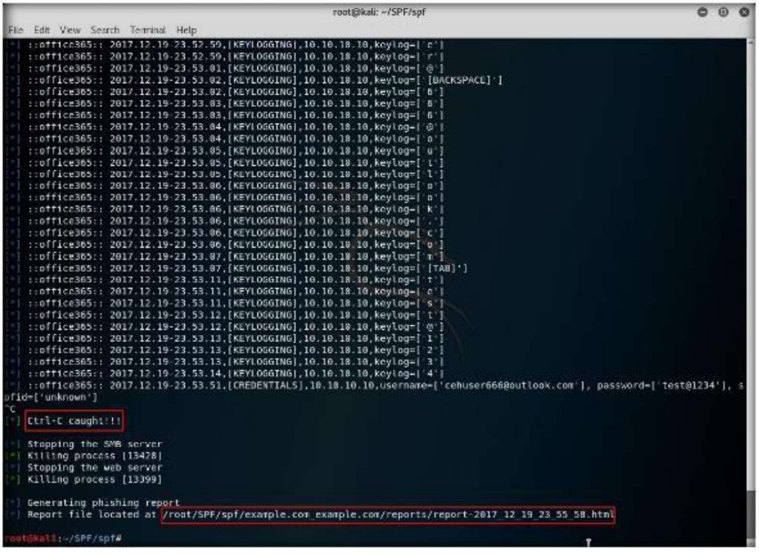


FIGURE 4.27: Exiting and Generating Report

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