**Lab 5-01: Sniff Credentials using the Social-Engineer Toolkit (SET)**

**Scenario**

PAMTech Corporation, a financial services firm, has recently observed an increase in phishing attempts targeting its employees. Despite implementing robust security controls, attackers continue to exploit human vulnerabilities through deceptive emails, impersonation, and malicious websites to harvest credentials. To assess the organization’s preparedness against such threats, the IT security team has commissioned a social engineering penetration test focusing on credential sniffing.

**Solution**

PAMTeach Corporation hired you as a Certified Penetration Tester. As an ethical hacker, your task in this demonstration is to utilize the Social-Engineer Toolkit (SET) to simulate a credential-harvesting attack. Using SET’s credential harvester attack module, you will create a phishing webpage that mimics a legitimate corporate login portal to trick employees into entering their credentials. Additionally, you will explore various social engineering techniques, such as email phishing and malicious web cloning, to understand how attackers deceive employees into revealing sensitive information.

By conducting this controlled security assessment, you will help PAMTech Corporation’s security team identify weaknesses in employee awareness, improve their phishing detection mechanisms, and implement stronger security policies such as employee training, Multi-Factor Authentication (MFA), and email filtering.

The Social-Engineer Toolkit (SET) is an open-source Python-based application for penetration testing using social engineering. SET is very valuable to attackers since it is publicly available and may be used to launch a variety of attacks. For example, it enables attackers to create email messages, attach malicious files, and distribute them to a huge number of individuals via spear phishing. Furthermore, SET’s multi-attack technique allows Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing to be utilized concurrently. SET categorizes attacks according to the attack vector used, which includes email, the web, and USB.

Although SET may be used to carry out a wide range of attacks, it is also an essential tool for penetration testers looking for weaknesses. As a result, SET is the industry standard for social engineering penetration testing. It has widespread support in the security community.

As an ethical hacker, penetration tester, or security administrator, you should be proficient with and able to utilize SET to execute multiple assessments for network vulnerabilities.

**Note:** In this lab, we use two virtual machines: ParrotOS and Windows 10. The ParrotOS, as an attacker machine, has an IP address of **10.10.1.13**. The Windows 10, as a victim machine, has an IP address of **10.10.1.18**. When you perform this lab, use your virtual machine IP addresses, not the lab IP addresses.

|  |
| --- |
| 1. Turn on **ParrotOS** and **Windows 10** virtual machines. Switch to the **ParrotOS** virtual machine, open a Terminal, and execute the **sudo su** command to run programs with root privileges. Execute the following command: **setoolki**t to launch **Social-Engineer Toolkit.** If a **Do you agree to the terms of service [y/n]** question appears, enter **y** and press **Enter**.    2. The SET menu appears. Type **1** and **press** Enter to select **Social-Engineering Attacks**.    3. A list of options for Social-Engineering Attacks appears; type **2** and press **Enter** to select **Website Attack Vectors**.    4. A list of options in **Website Attack Vectors** appears; type **3** and press **Enter** to select **Credential Harvester Attack Method**.    5. Type **2** and press **Enter** to select **Site Cloner** from the menu.    6. Type the IP address of the local machine **10.10.1.13** in the prompt for an **IP address for the POST back in Harvester/Tabnabbing** and press **Enter**. In this case, we are targeting the ParrotOS virtual machine IP address **10.10.1.13**.    7. Now, you will be prompted for the URL to be cloned; type the desired URL in **Enter the url to clone** and press **Enter**. In this lab, we will clone the URL **http://testphp.vulnweb.com/login.php**. You can clone any URL of your choice.    8. If a message appears that reads **Press {return} if you understand what we’re saying here**, press **Enter**.  9. After cloning is completed, a highlighted message appears. The credential harvester starts, as indicated in the screenshot.    10. Having successfully cloned a website, you must now send the IP address of your ParrotOS virtual machine to a victim and try to trick him/her into clicking on the link.  11. Click the **Firefox** icon from the top section of the **Desktop** to launch a web browser window and open your email account. In this lab, we are using **Outlook**. Log in and compose an email. You may log in to any email account you choose.  12. After logging into your email account, click the **New Mail** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.  **Note:** A good way to conceal a malicious link in a message is to insert text that looks like a legitimate Acuaart URL, in this case, but that actually links to your malicious cloned Acuart page.  13. Position the cursor just above Regards to place the fake URL, then click the **Insert link** icon.    14. In the **Insert link** window, first type the fake URL in the **Display as** field. Then, type the actual address of your cloned site in the **Web address (URL)** field and click **OK**. In this case, the text that will be displayed in the message is **www.acuart.com/account-information,** and the actual address of our cloned Acuart site is **http://10.10.1.13**.    15. The fake URL should appear in the message body.  16. Verify that the fake URL is linked to the correct cloned site: in Outlook, hover over the link; the actual URL will be displayed. Once validated, forward the email to the desired recipient.    17. Switch to the **Windows 10** virtual machine. Open any web browser and sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link. In this lab, we use a Gmail account as a victim.    18. When the victim, in this case, clicks the URL, a new tab opens up, and he/she will be presented with a replica of **www.acuart.com**.  19. The victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, he/she will be redirected to the legitimate **Acuart** login page. Take note of the differences in URLs in the browser address bar between the cloned and actual sites. If a save credentials notification appears, click **Don't Save**.    20. Now, switch back to the **ParrotOS** virtual machine and switch to the terminal window. As soon as the victim enters his or her **Username** and **Password** and clicks **Login**, SET retrieves the entered credentials. The attacker can now use these to gain unauthorized access to the victim’s account. Scroll down to see your username and password displayed in plain text, as seen in the screenshot. This ends the demonstration of phishing user credentials with the SET. |

**Lab 5-02: Detect Phishing using Netcraft**

**Scenario**

You are working for a Social Media marketing company. Company employees must perform their tasks on social media platforms like Facebook and YouTube. With the tremendous increase in social media websites, there has been a corresponding growth in incidents of phishing used to carry out financial fraud. The company also decided to provide awareness of how to detect phishing websites; hence, employees would not be fooled by hackers in the future.

**Solution**

The company hires you as a Certified Penetration Tester because it wants you to hack and find vulnerabilities ethically. All the employees in the company must know the technique of how to detect phishing websites. Being unable to identify phishing websites will harm your social media marketing campaigns; if an employee runs a social media campaign without knowing that this website is a phishing website, customer satisfaction will decrease. In this lab, we use the **Netcraft** tool to detect a phishing website.

|  |
| --- |
| 1. Open the browser to install the **Netcraft** extension. Type the following URL: [**https://www.netcraft.com/apps-extensions/**](https://www.netcraft.com/apps-extensions/) and press **Enter**. The Netcraft website opens.    2. Click on the **Accept** button in the cookie notification. Scroll down and click on the **LEARN MORE** button under **Browser Protection.**    3. You will be directed to the **Browser Extension** page. Scroll down to **Download the extension today** and click on any browser icon that you are using. In this lab, we are using the **Chrome** browser.    4. It navigates you to the next page. Click on the **Add to Chrome** button to install the Netcraft Extension.    5. When the **Add Netcraft Extension?** notification pop-up appears on the top of the window; click the **Add extension** button.    6. The **Netcraft Extension** icon appears in the browser's top-right corner.    7. Now, in a new tab, type the following URL [**https://www.certifiedhacker.com/**](https://www.certifiedhacker.com/) and press **Enter**.    8. The **certifiedhacker.com** webpage appears. Click on the **Netcraft Extension** icon in the top-right corner of the browser. A dialog box displays the website’s information, such as **Risk Rating**, **Site rank**, **First seen**, and **Host**.    9. Click on the **Site Report** link from the dialog box to view a site report.    10. The **Site report for certifiedhacker.com** page shows detailed information about the site, such as **Background**, **Network**, **IP Geolocation**, **SSL/TLS,** and **Hosting History**.      11. If you attempt to visit a website identified as a phishing site by the Netcraft Extension, you will see a pop-up alerting you to Suspected Phishing. In the browser, type the URL **http://metamask.verficaton-app.com/us/** and press **Enter**. You can use any phishing website to check.    12.You will get a **Suspected Phishing** page on the browser.  **Note:** Updated Chrome browsers also detect malicious URLs and give suspected phishing pages.    13. It concludes the demonstration of detecting phishing using the Netcraft extension. |

**Lab 5-03: Audit an Organization's Security for Phishing Attacks**

**Scenario**

You work for a social media marketing firm where all employees engage on platforms like Facebook and YouTube. With the rise of social media sites, phishing incidents for financial fraud have increased. To counter social engineering, the firm evaluates attack risks, estimates potential losses, and educates employees. The company audits phishing attacks to prevent future vulnerabilities.

**Solution**

As a Certified Penetration Tester, you are hired by the company hires you to ethically hack its server and find vulnerabilities. All employees must be aware of any phishing attacks on the network and implement anti-phishing measures. You use OhPhish to audit phishing attacks. A web-based tool called OhPhish can be used to assess an employee's vulnerability to social engineering attacks. The organization can use this phishing simulation tool to launch phishing simulation campaigns for its employees. The platform gathers the data and offers Management Information System (MIS) reports and trends (in real-time) that the user, department, or designation can follow.

|  |
| --- |
| 1. Before starting this lab, you must activate your OhPhish account. Go to the **Click here** hyperlink in the OhPhish notification above the **My Courses** section.    2. You will be redirected to the OhPhish **Sign Up** page. Enter the remaining personal details, check the **I'm not a robot** checkbox, and click the **Complete Signup** button.    3. Open your email account given during the registration process. Open an email from **OhPhish**, and click the **CLICK HERE TO LOGIN** button in the email.    4. The OhPhish login page appears. Log in using the credentials received in the email.    5. You will be redirected to the **Reset Password** page. Enter the new password in both fields and click the **Reset Password** button to reset the password.    6. Once you log in to your OhPhish account, you will be redirected to the OhPhish **Dashboard**. Then, click on the **Entice to Click** option.    7. The **Create New Email Phishing Campaign** form appears. Enter any name in the **Campaign Name** field (here, **Test - Entice to Click**). In the **Select Template Category** field, select **Coronavirus/COVID-19** from the drop-down list. In the **Select Country** field, leave the default option selected (**All**). In the **Select Template** field, click the **Select Template** button and select **Corona Virus Advisory** from the drop-down list.    8. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot. In the **Import users** field, click **Select Source**.    9. The **Import Users** pop-up appears. Click to select the **Quick Add** option from the list of options.    10. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.    11. Similarly, you can add the details of multiple users. Here, we added two users. Add the users' details and click **Import**.    12. In the **Batch Count** and **Batch Interval** fields, set the values to **1**. Leave the **Landing Page** field set to its default value. Scroll down to the end of the page and click **Create** to create the phishing campaign.    13. **Add to your Whitelist** pop-up appears; click **Done**.    14. The **Confirm?** pop-up appears; click **SURE**.    15. A countdown timer appears, and the phishing campaign initiates in ten seconds. The **Alert!** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.    16. Open the phishing email on the victim's PC. In this case, we use **Windows Server 2019** as a victim.    17. Click on **Ctrl+Alt+Delete** to activate it. By default, the **Administrator** profile is selected; enter the password into the machine and press **Enter** to log in.    18. Open any web browser and then open the email client provided while creating the phishing campaign (here, Gmail). After you log in to your Gmail account, search for an email with the subject **COVID 19 Advisory** in the **Inbox**. Click on the **Safety Measures** link in the email.    19. If a **Suspicious link** pop-up appears, click **Proceed**. The landing page **Oh You've been Phished** appears, as shown in the screenshot.    20. Go back to the **Windows 10** machine. Click on the **Test – Entice to Click** campaign present on the **OhPhish Dashboard**.    21. The **Campaign Detailed Report** page displays the **Campaign Details** and **Summary** sections. In the **Campaign Summary** section, you can observe that the values of **No. of targets who have clicked the link (defaulters)** and **No. of Targets who have opened the mail** is both **1** (here, we have opened only one email account).    22. Click **Home** in the left pane to navigate to the OhPhish **Dashboard**. In the OhPhish **Dashboard**, click on the **Send Attachment** option.    23. The **Create New Email Phishing Campaign** form appears. Enter any name in the **Campaign Name**field (here, **Test – Send to Attachment**). In the **Select Template Category** field, select **Office Mailers** from the drop-down list. In the **Select Country** field, leave the default option selected (**All**). In the **Select Template** field, select the **PF Amount Credited** option from the drop-down list and then click the **Select** button. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot. In the **Attachment** field, enter any name (here, **Additional Information**).    24. Click the **Select Source** button under the **Import users** field.    25. The **Import Users** pop-up appears. Click to select the **Quick Add** option from the list of options.    26. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.    27. Similarly, you can add the details of multiple users. Here, we added two users. Add the users' details and click **Import**. In the **Batch Count** and **Batch Interval** fields, set the values to **1**. Leave the **Landing Page** field set to its default value. Scroll down to the end of the page and click **Create** to create the phishing campaign.    28. **Add to your Whitelist** pop-up appears; click **Done**. The **Confirm?** pop-up appears; click **SURE**. A countdown timer appears, and a phishing campaign initiates in ten seconds. The **Alert!** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.    29. Go back to the **Windows Server 2019** victim machine. In the Gmail account opened previously, navigate to the **Inbox** folder. You will find an email from **HR – ABP News**, as shown in the screenshot. Click on the **EPF – KYC Documents Upload Centre** hyperlink present in the email.    30. If a **Suspicious** link pop-up appears, click **Proceed**. You will be redirected to the **Oh You've been Phished** landing page, as shown in the screenshot.    31. Go back to the **Windows 10** machine. Click on the **Test – Send to Attachment** campaign present on the **OhPhish Dashboard**.    32. The **Campaign Detailed Report** page displays the Campaign Details and **Summary** sections. In the **Campaign Summary** section, you can observe that the value of **No. of targets who have clicked the link (defaulters)** is **1**. Click on the **1** icon to see the defaulter.    33. The **Campaigns Users** page appears, displaying the details of the defaulter, such as **Risk Score**, **Credentials**, **IP Address**, **Location**, etc., as shown in the screenshot.    34. Click to expand the **Reports** section in the left pane and select the **Executive Summary Report** option.    35. The **Campaign Report** page appears; select any phishing campaign from the drop-down list (here, **Test – Send to Attachment**) and click on the **Export** icon to export the report.    36. The **Opening Phishing-Simulation-Test** window appears; select the **Save File** radio button and click **OK**.    37. The file is downloaded to the default location (here, **Downloads**). Navigate to the download location and double-click the **Phishing-Simulation-Test---Send-Attachment** file to open it.    38. The executive phishing report appears in the document, as shown in the screenshot. |