Module 09: Social Engineering

Lab 1: Perform Social Engineering using Various Techniques

Lab Scenario

As a professional ethical hacker or penetration tester, you should use various social engineering techniques to examine the security of an organization and the awareness of employees.

In a social engineering test, you should try to trick the user into disclosing personal information such as credit card numbers, bank account details, telephone numbers, or confidential information about their organization or computer system. In the real world, attackers would use these details either to commit fraud or to launch further attacks on the target system

Lab Objectives

- Sniff credentials using the Social-Engineer Toolkit (SET)

Overview of Social Engineering Techniques

There are three types of social engineering attacks: human-, computer-, and mobile-based.

- **Human-based social engineering** uses interaction to gather sensitive information, employing techniques such as impersonation, vishing, and eavesdropping
- **Computer-based social engineering** uses computers to extract sensitive information, employing techniques such as phishing, spamming, and instant messaging
- **Mobile-based social engineering** uses mobile applications to obtain information, employing techniques such as publishing malicious apps, repackaging legitimate apps, using fake security applications, and SMiShing (SMS Phishing)

Task 1: Sniff Credentials using the Social-Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. SET is particularly useful to attackers, because it is freely available and can be used to carry out a range of attacks. For example, it allows attackers to draft email messages, attach malicious files, and send them to a large number of people using spear phishing. Moreover, SET's multi-attack method allows Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing to be used simultaneously. SET categorizes attacks according to the attack vector used such as email, web, and USB.

Although many kinds of attacks can be carried out using SET, it is also a must-have tool for penetration testers to check for vulnerabilities. For this reason, SET is the standard for social engineering penetration tests, and is strongly supported within the security community.

As an ethical hacker, penetration tester, or security administrator, you should be familiar with SET and be able to use it to perform various tests for network vulnerabilities.

Here, we will sniff user credentials using the SET.

1. Click on Parrot Security to switch to the **Parrot Security** machine. Login using **attacker/toor**.

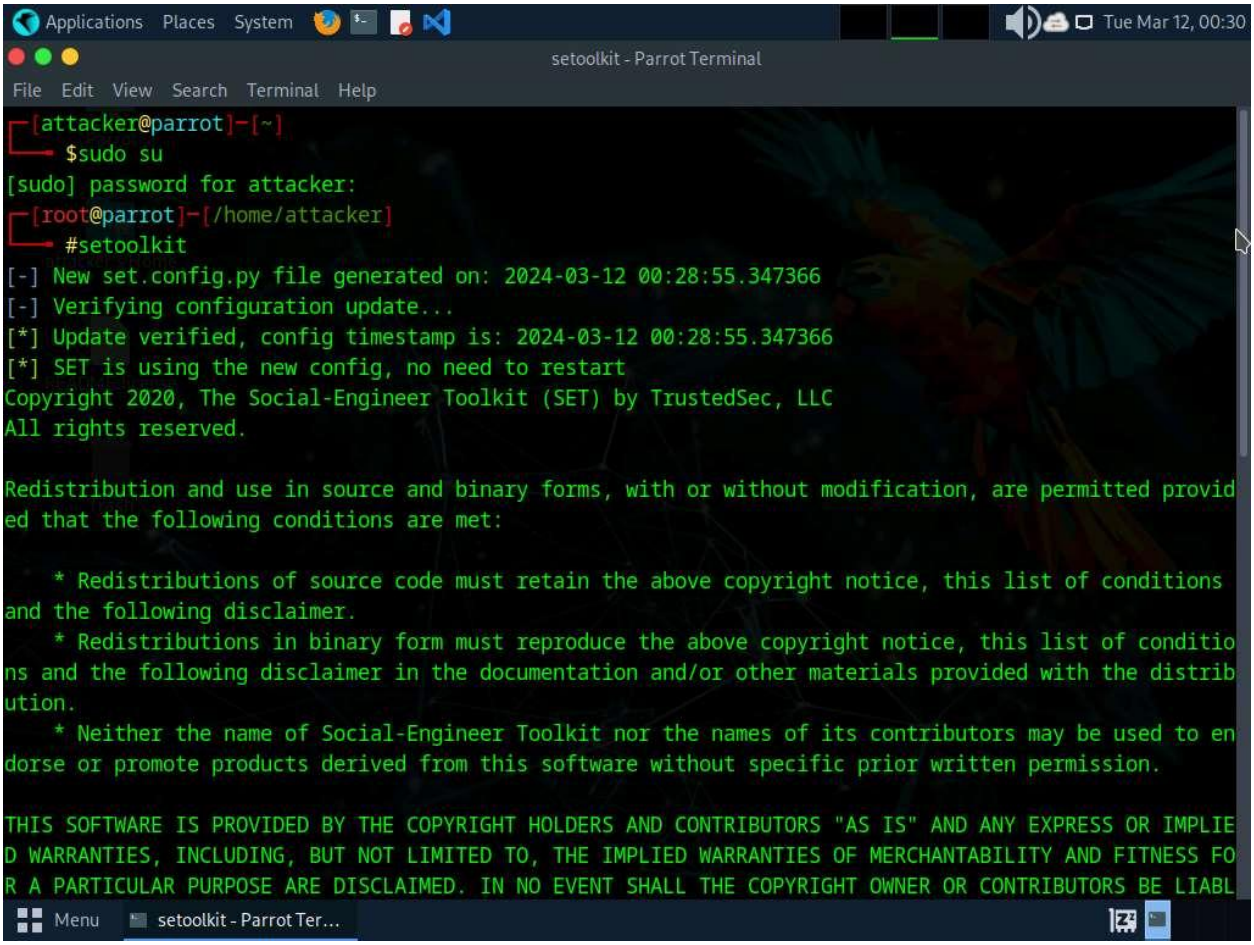
If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

2. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

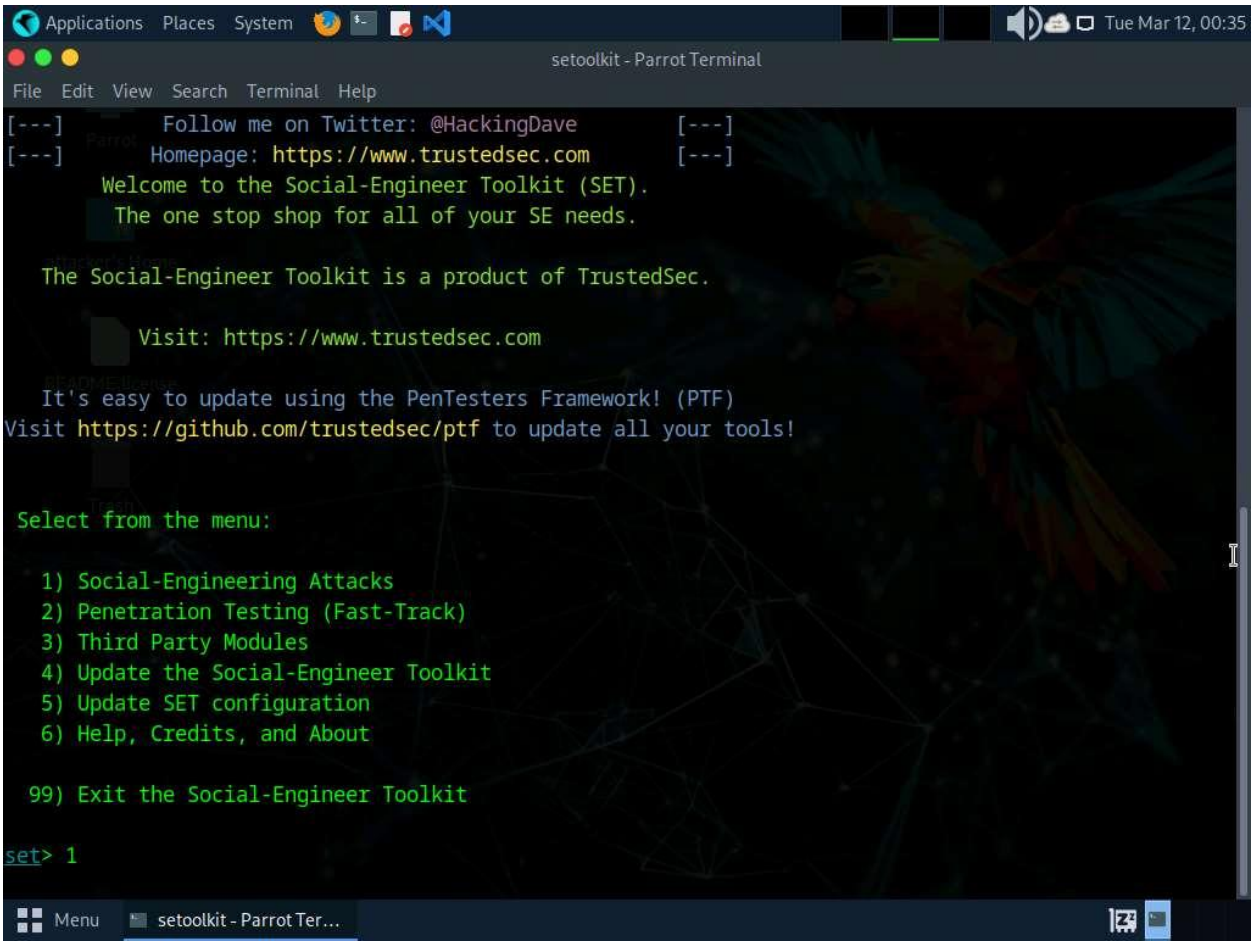
The password that you type will not be visible.

3. Run **setoolkit** to launch **Social-Engineer Toolkit**.

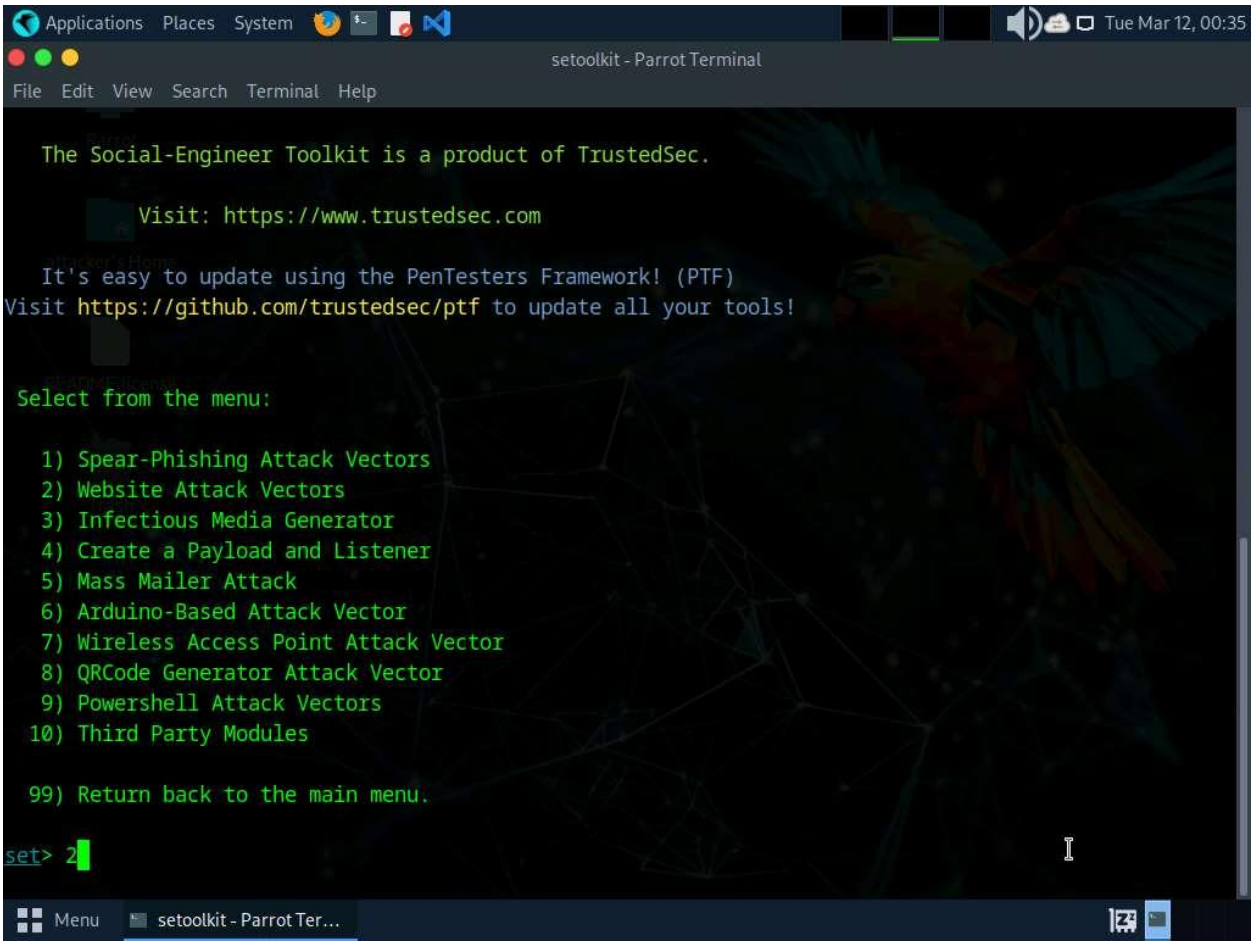
If a **Do you agree to the terms of service [y/n]** question appears, enter **y** and press **Enter**.



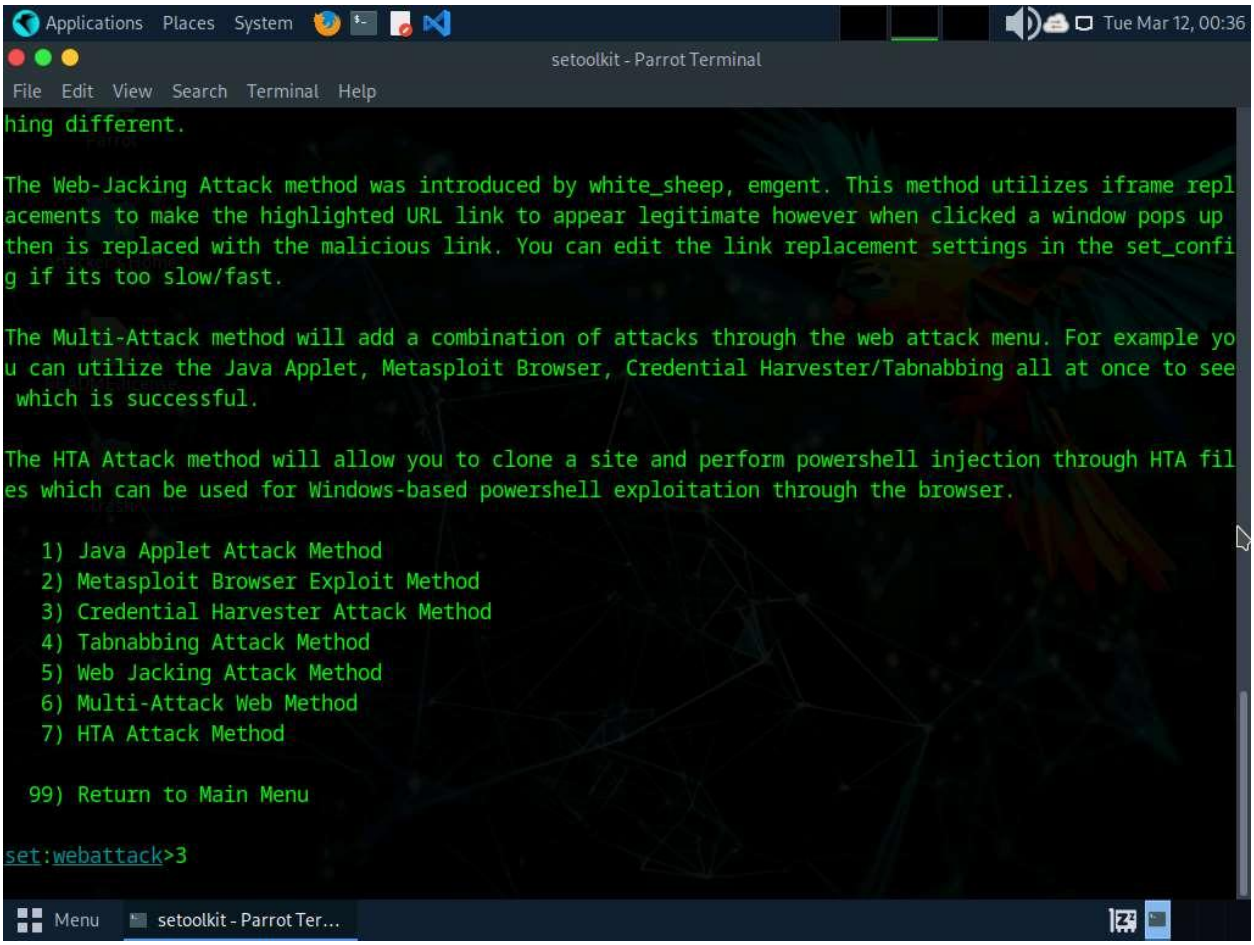
4. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **Social-Engineering Attacks**.



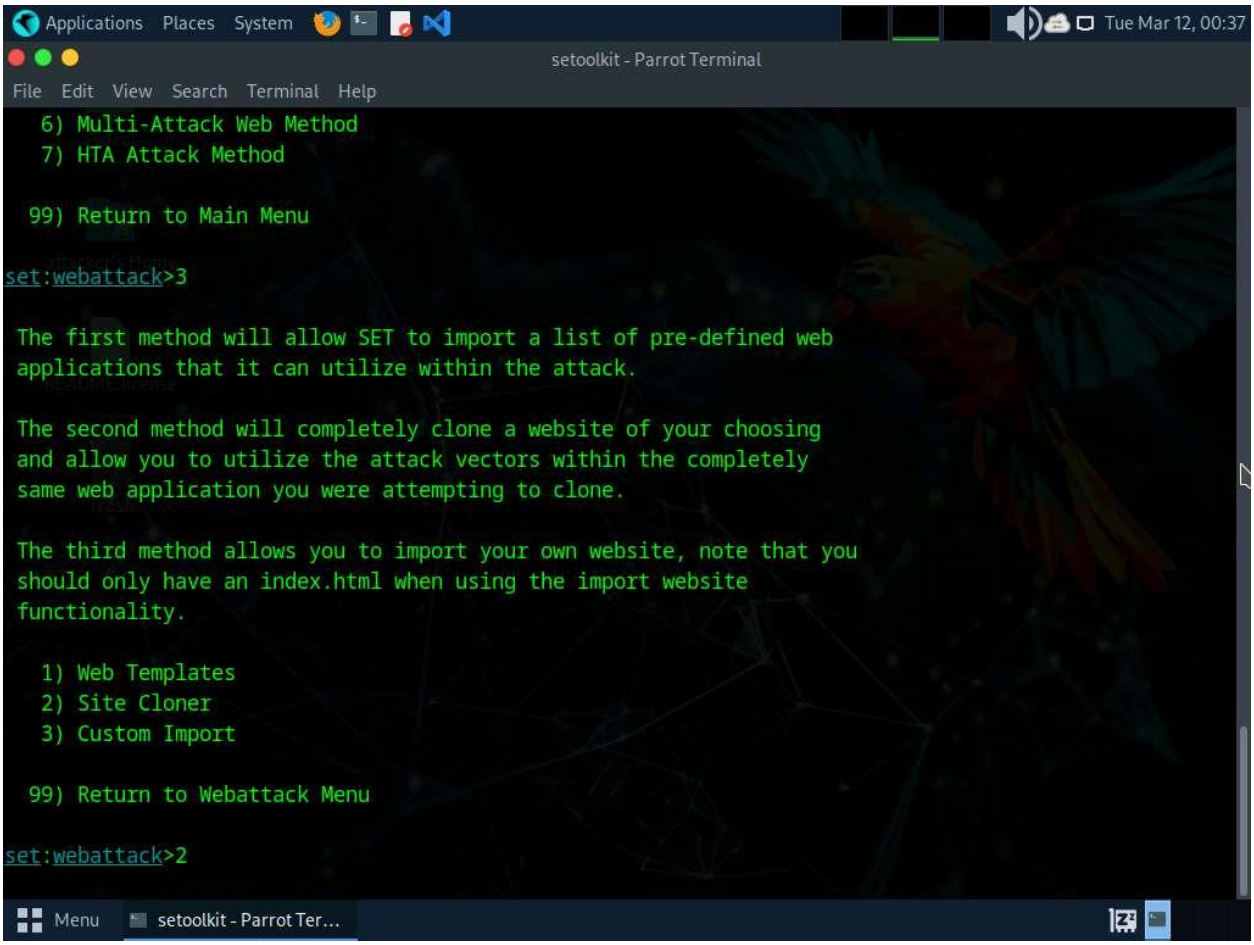
5. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors**.



6. A list of options in **Website Attack Vectors** appears; type **3** and press **Enter** to choose **Credential Harvester Attack Method**.



7. Type **2** and press **Enter** to choose **Site Cloner** from the menu.

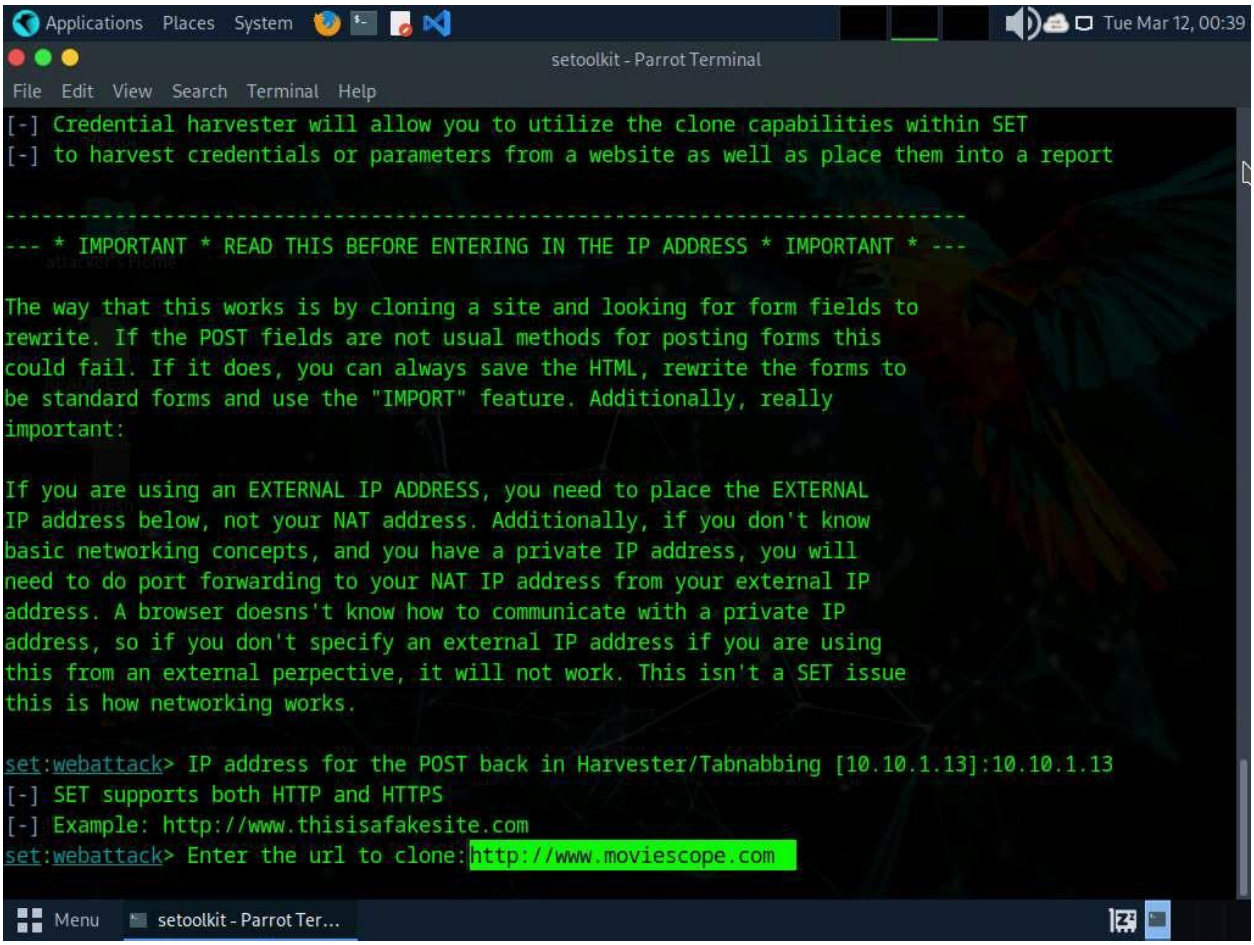


8. Type the IP address of the local machine (**10.10.1.13**) in the prompt for "**IP address for the POST back in Harvester/Tabnabbing**" and press **Enter**.

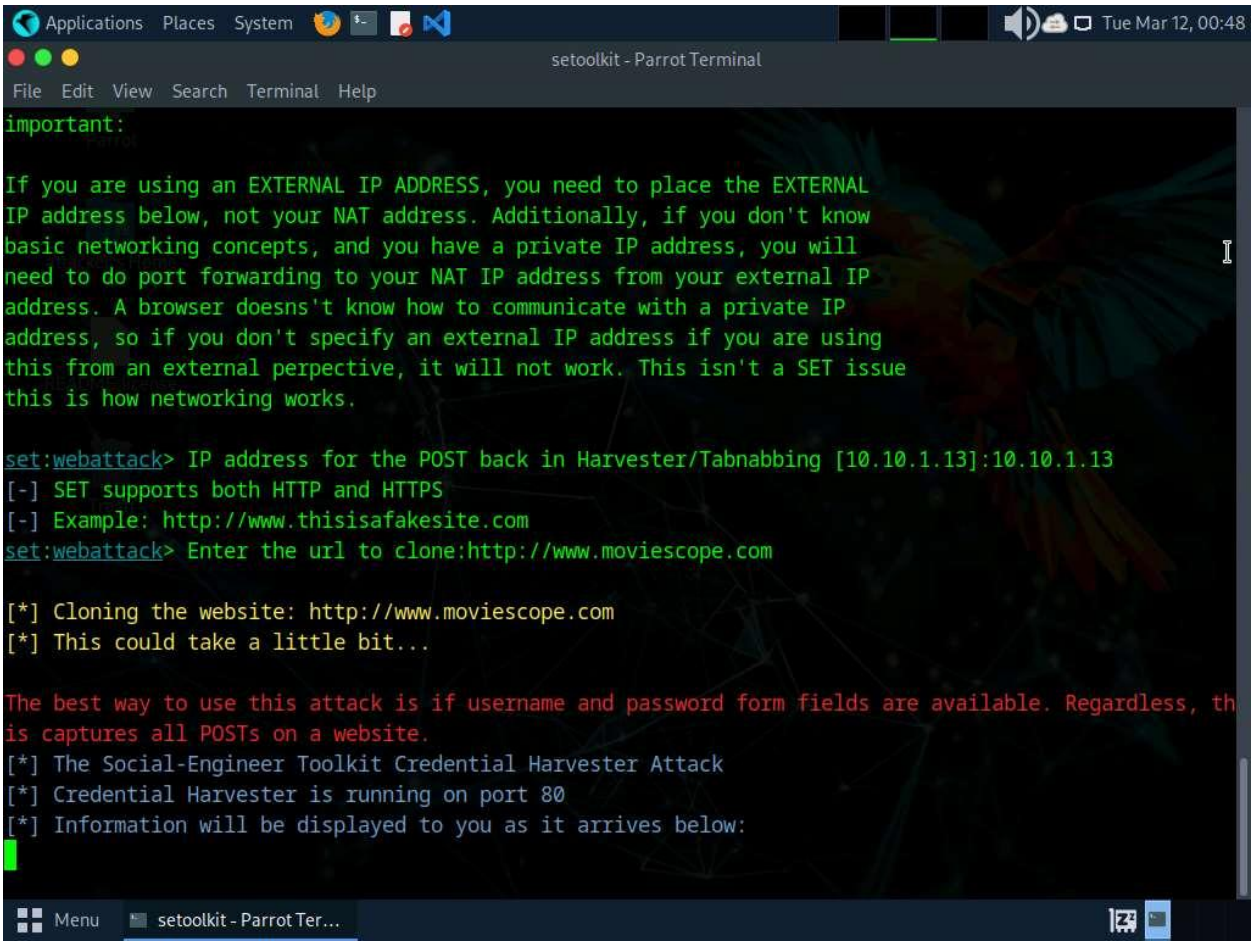
In this case, we are targeting the **Parrot Security** machine (IP address: **10.10.1.13**).

9. 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 task, we will clone the URL **http://www.moviescope.com**.

You can clone any URL of your choice.



10. If a message appears that reads **Press {return} if you understand what we're saying here**, press **Enter**.
11. After cloning is completed, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.



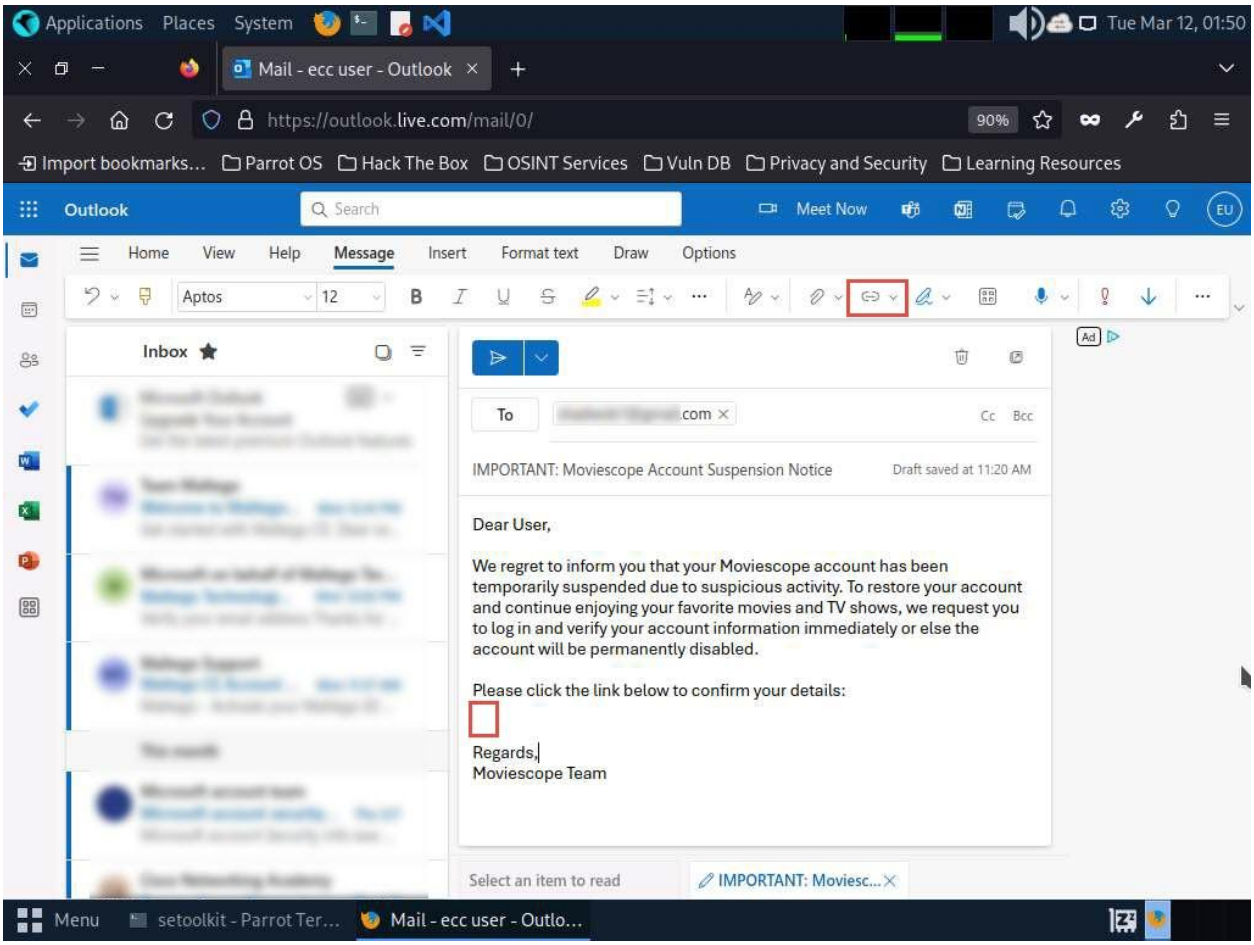
12. Having successfully cloned a website, you must now send the IP address of your **Parrot Security** machine to a victim and try to trick him/her into clicking on the link.
13. Click **Firefox** icon from the top-section of the **Desktop** to launch a web browser window and open your email account (in this example, we are using **Mozilla Firefox** and **Outlook**, respectively). Log in, and compose an email.

You can log in to any email account of your choice.

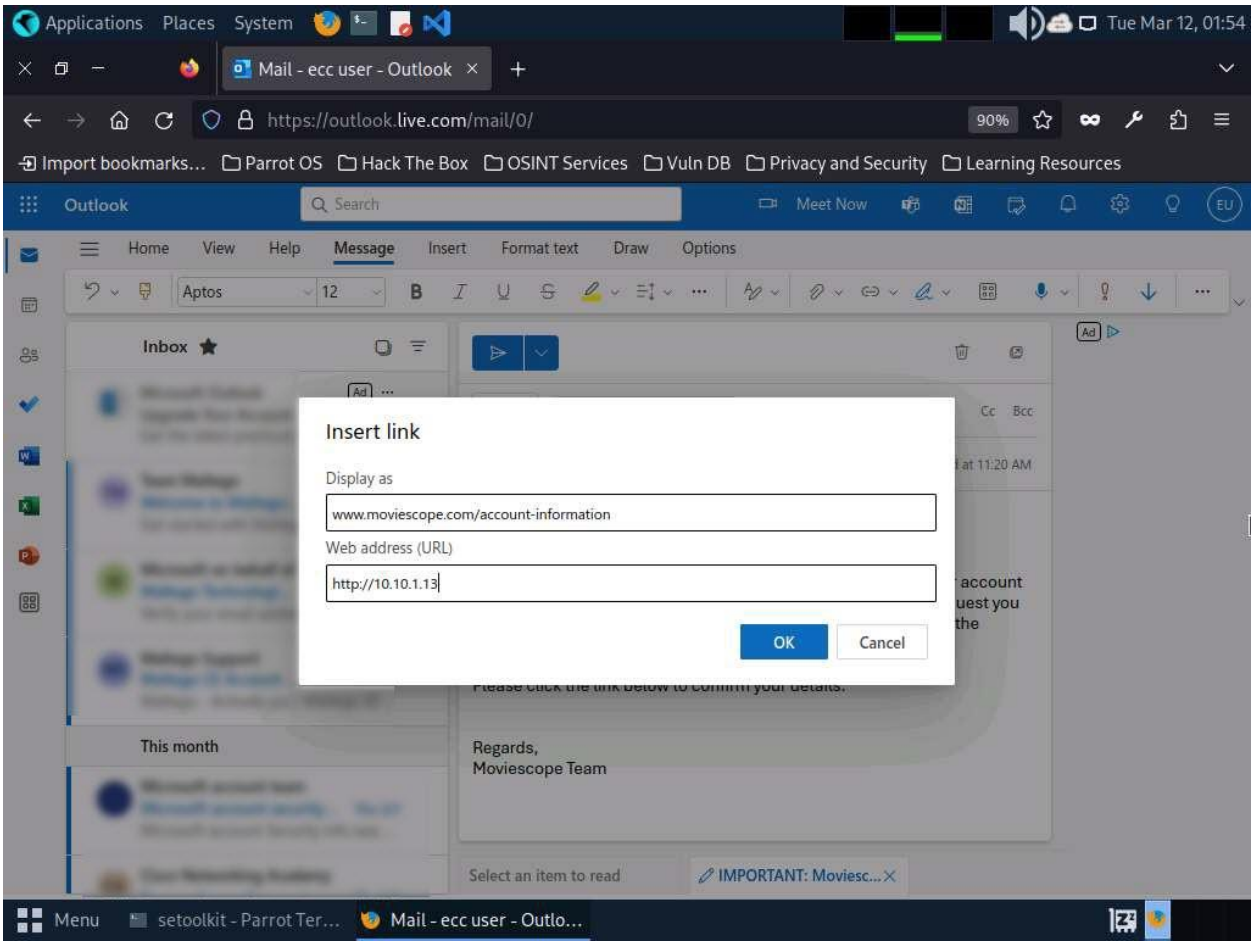
14. After logging into your email account, click the **New Mail** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

A good way to conceal a malicious link in a message is to insert text that looks like a legitimate MovieScope URL (in this case), but that actually links to your malicious cloned MovieScope page.

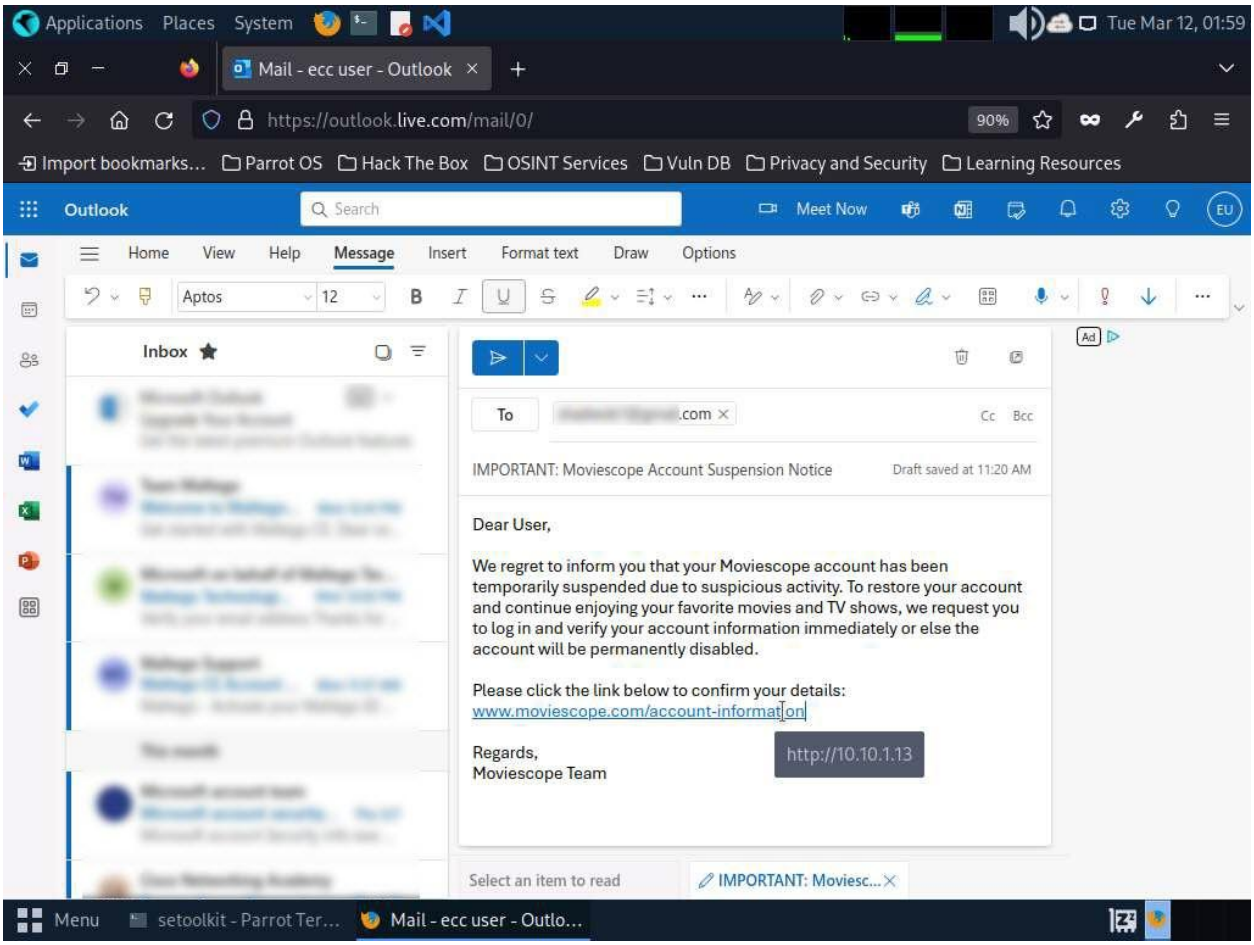
15. Position the cursor just above Regards to place the fake URL, then click the **Insert link** icon.



16. 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.moviescope.com/account-information** and the actual address of our cloned MovieScope site is **http://10.10.1.13**.



17. The fake URL should appear in the message body.
18. 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 verified, send the email to the intended user.



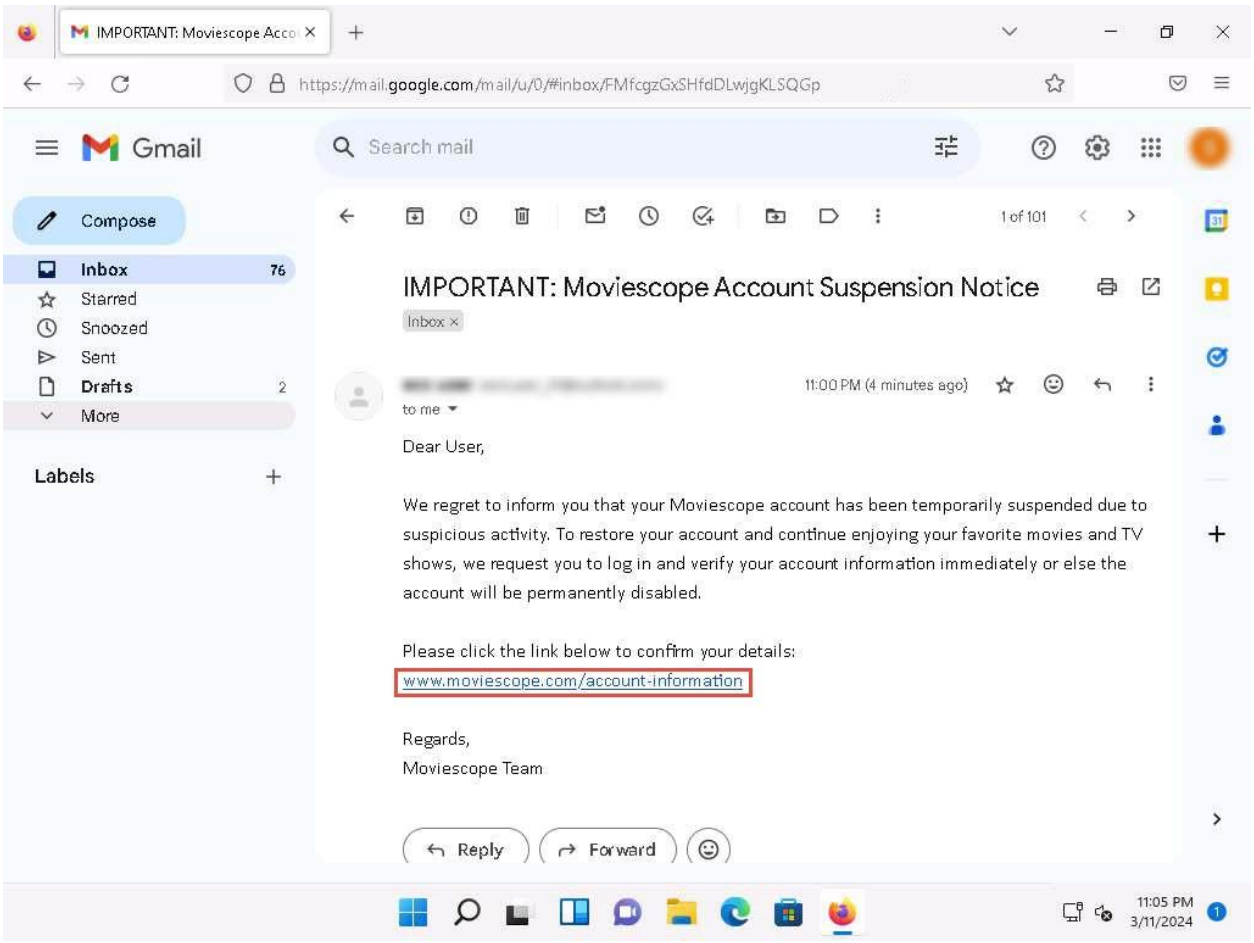
19. Click Windows 11 to switch to the **Windows 11** machine and login using **Admin**/**Pa$$w0rd**.

Alternatively, you can also click **Pa$$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane.

If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

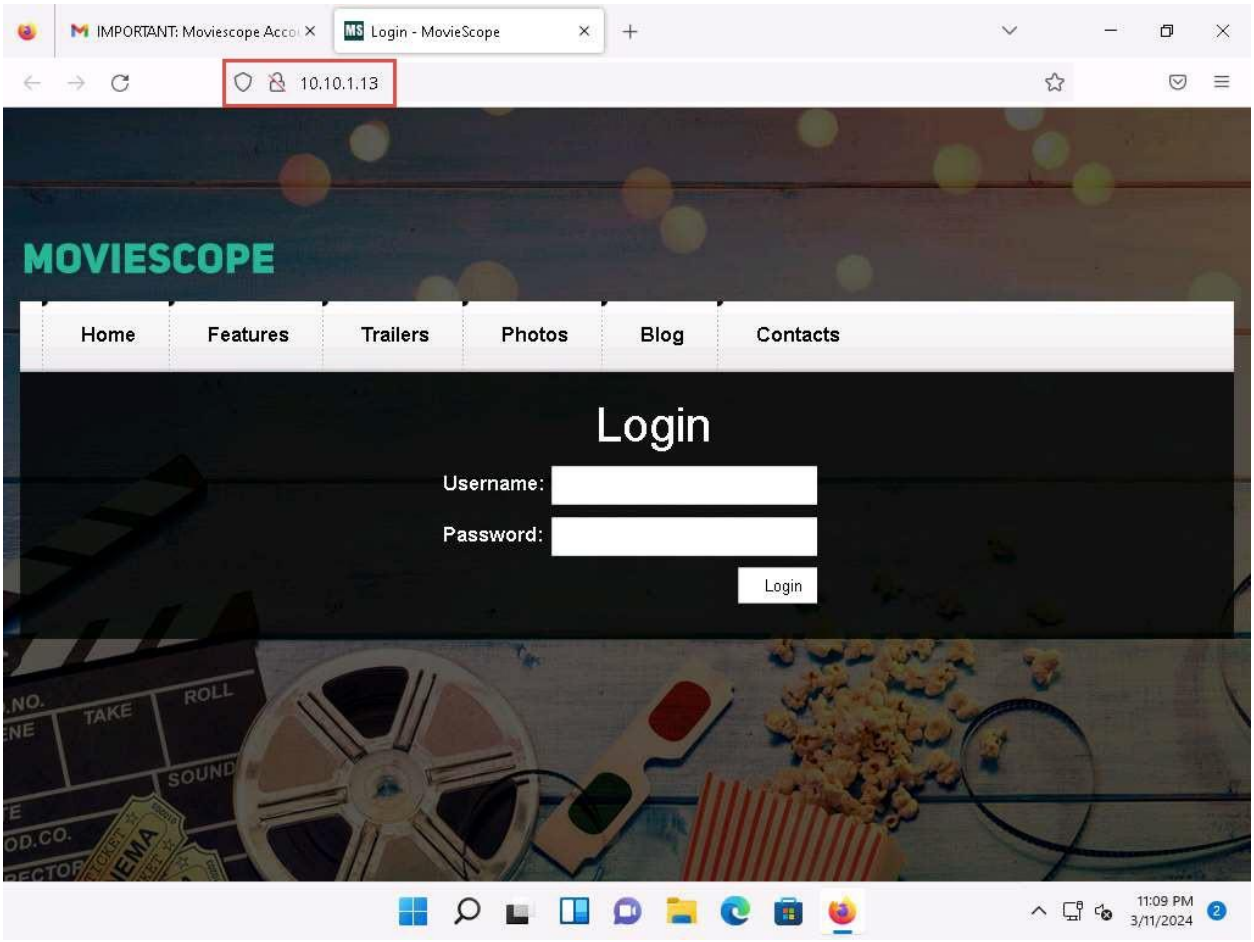
Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

20. Open any web browser (here, we are using **Mozilla Firefox**), 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.

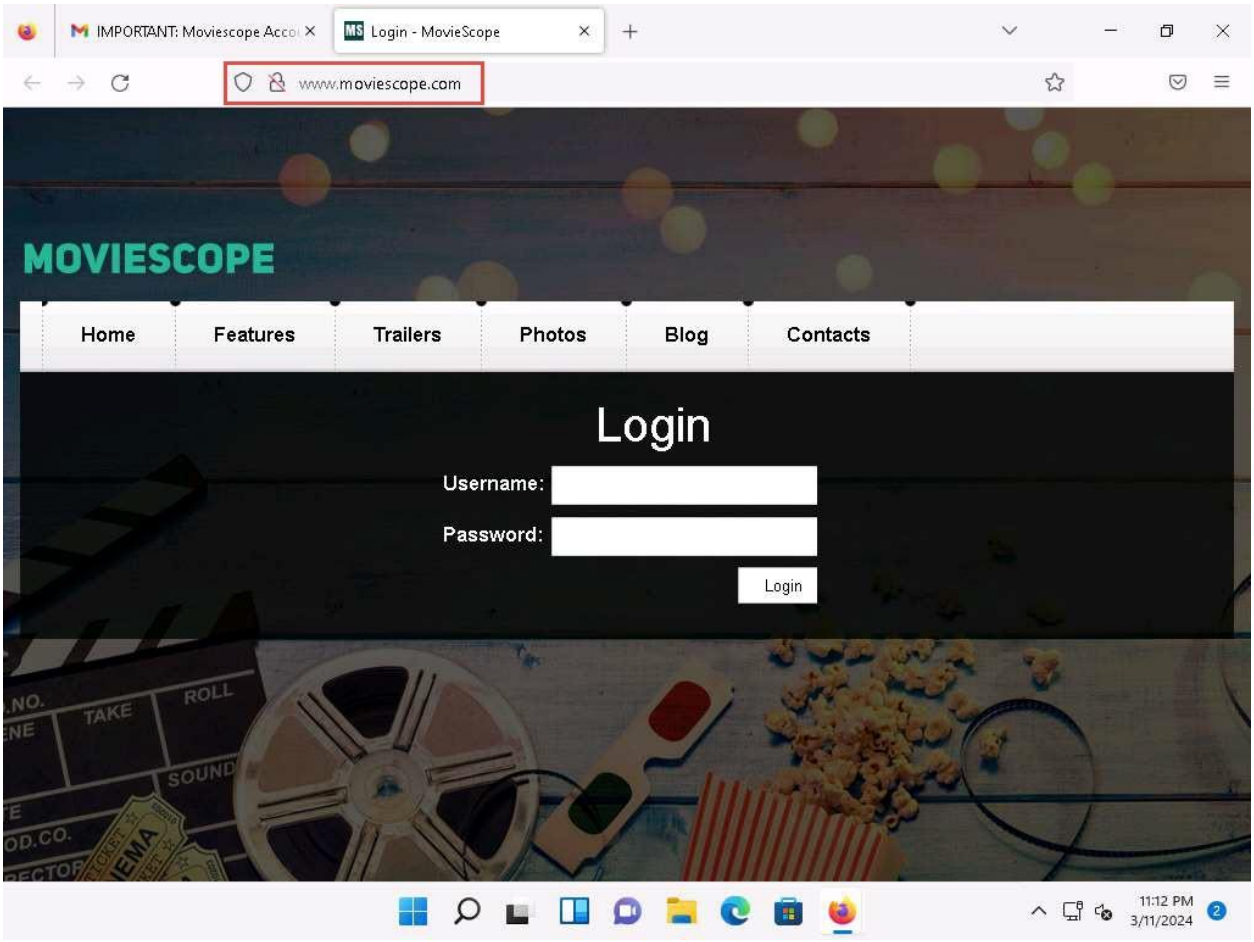


21. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of **www.moviescope.com**.

22. 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 **MovieScope** login page. Note the different URLs in the browser address bar for the cloned and real sites.



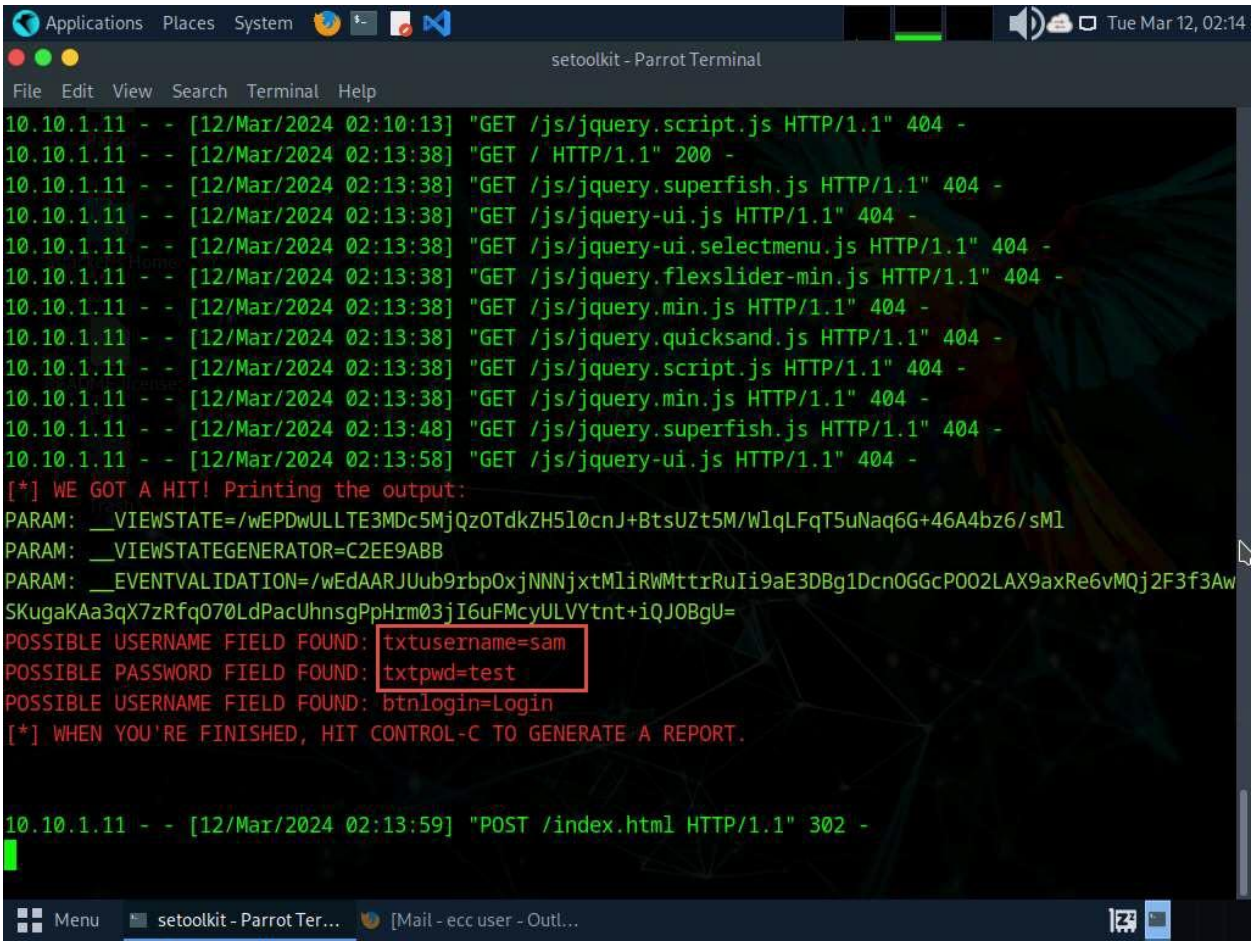
If save credentials notification appears, click **Don't Save**.



23. Now, click Parrot Security to switch back to the **Parrot Security** machine and switch to the **terminal** window.

24. As soon as the victim types in his/her **Username** and **Password** and clicks **Login**, **SET** extracts the typed credentials. These can now be used by the attacker to gain unauthorized access to the victim's account.

25. Scroll down to find **Username** and **Password** displayed in plain text, as shown in the screenshot.



26. This concludes the demonstration of phishing user credentials using the SET.
27. Close all open windows and document all the acquired information.