

CEH Module 9: Social Engineering

Assignment - 05

(Marepalli Rakesh)

Given 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

Given Lab Objectives:

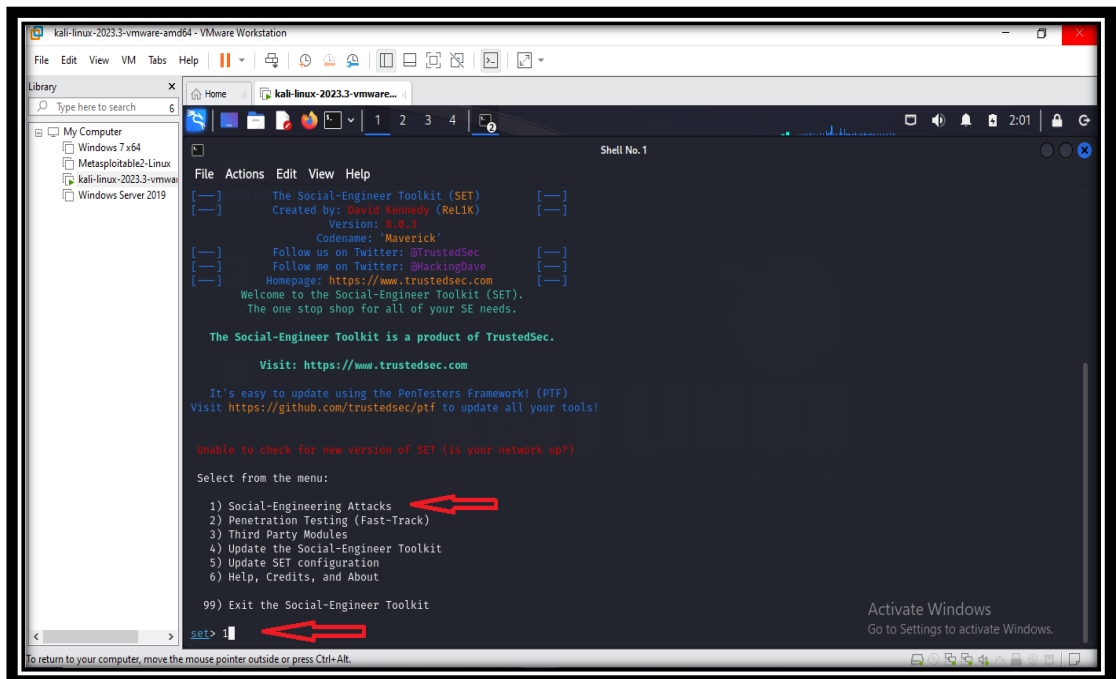
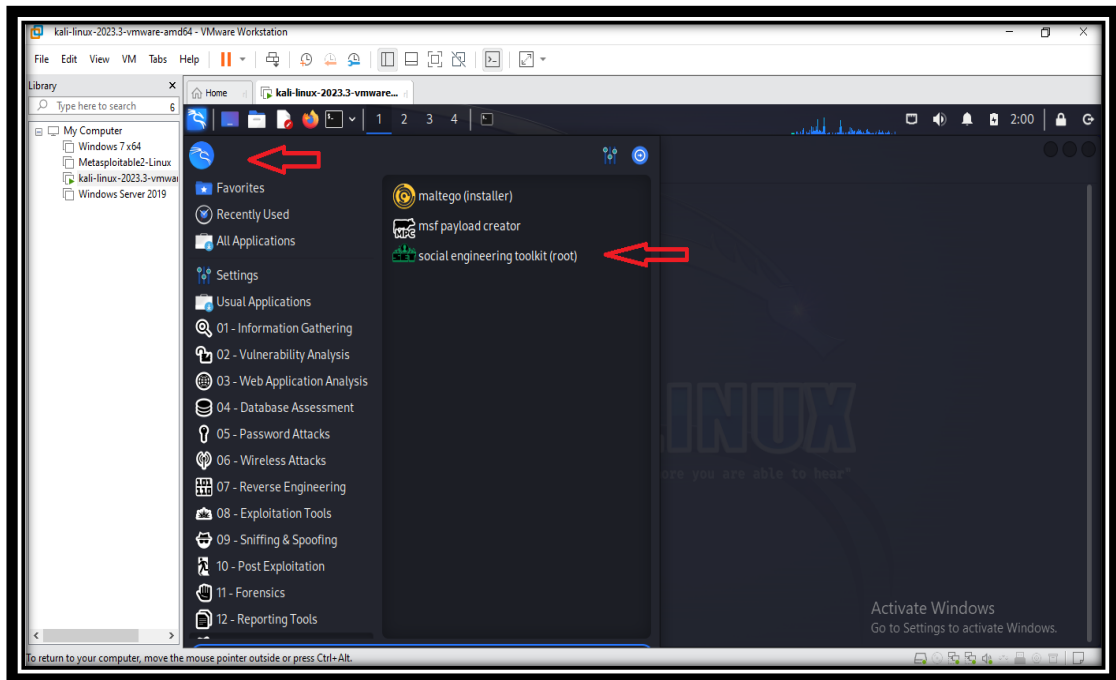
- Sniff users' credentials using the Social-Engineer Toolkit (SET)
- Perform phishing using Shell Phish

Objective: 01

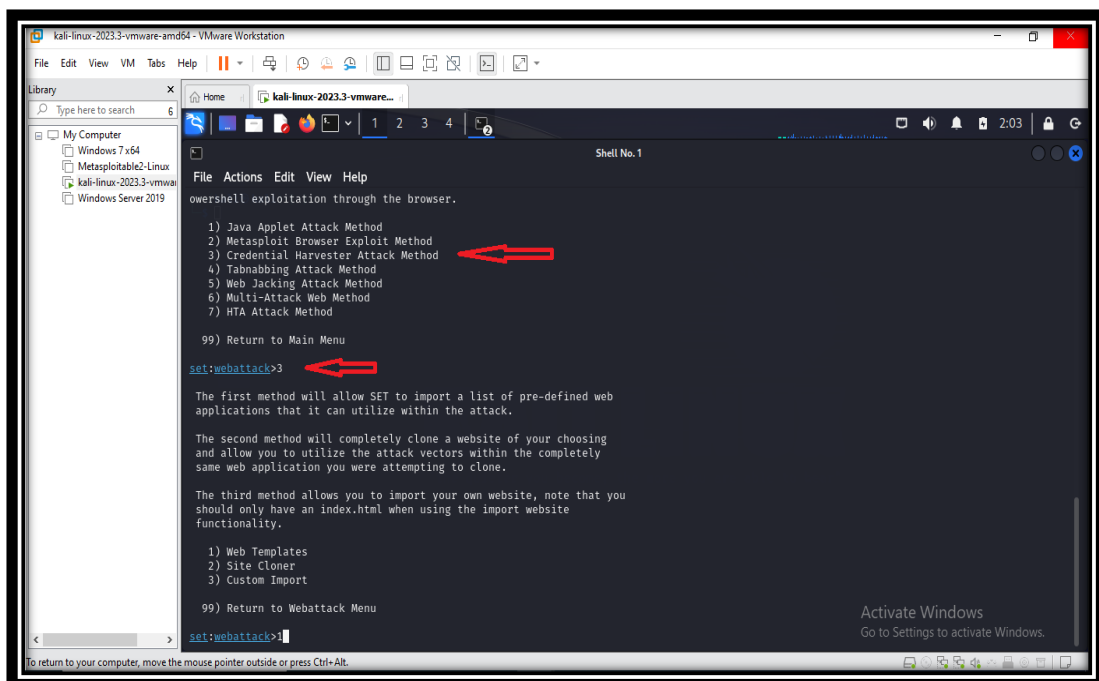
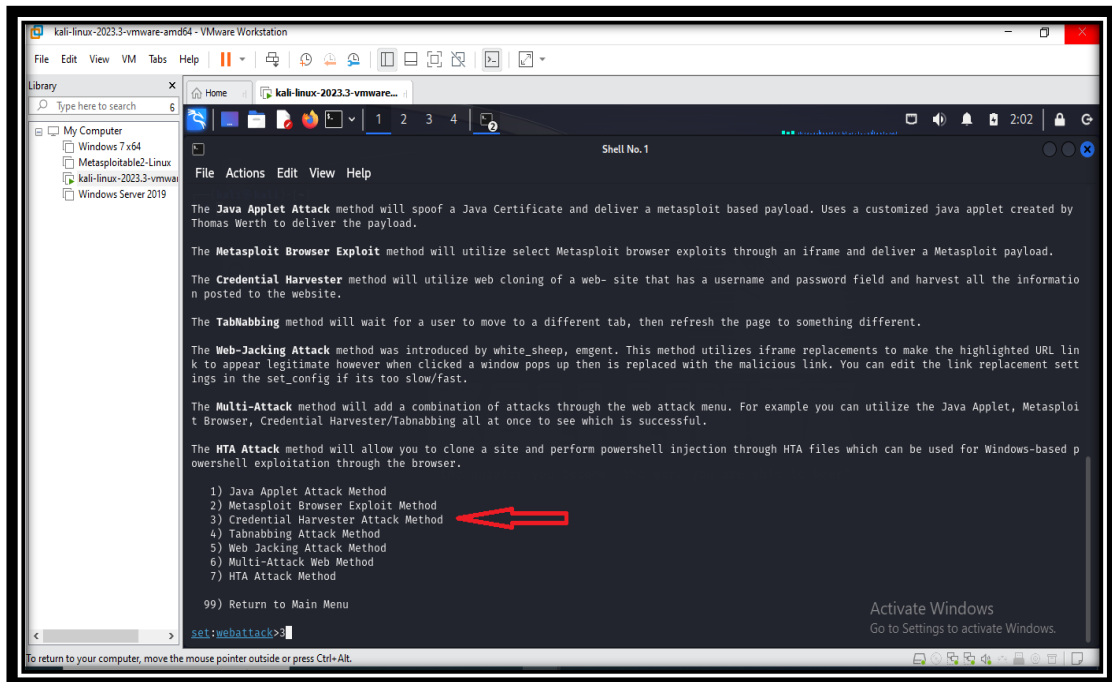
Sniff users' credentials using the Social-Engineer Toolkit (SET)

- In the ever-evolving realm of cybersecurity, maintaining a keen watch for digital threats is paramount. While technology has been at the forefront of our defences, understanding the human aspect of security is equally vital. This lab assignment dives into the realm of social engineering, a psychological tactic, to examine and counteract its potential risks. Specifically, we'll explore the Social-Engineer Toolkit (SET) and its application in simulating scenarios where credentials might be compromised.
- The primary goal of this lab objective is to gain insights into the Social-Engineer Toolkit (SET) and its role in simulating and comprehending how cybercriminals can exploit human vulnerabilities to gain access to sensitive credentials. SET is a versatile framework built to automate a range of attacks, with a particular focus on manipulation and social engineering.

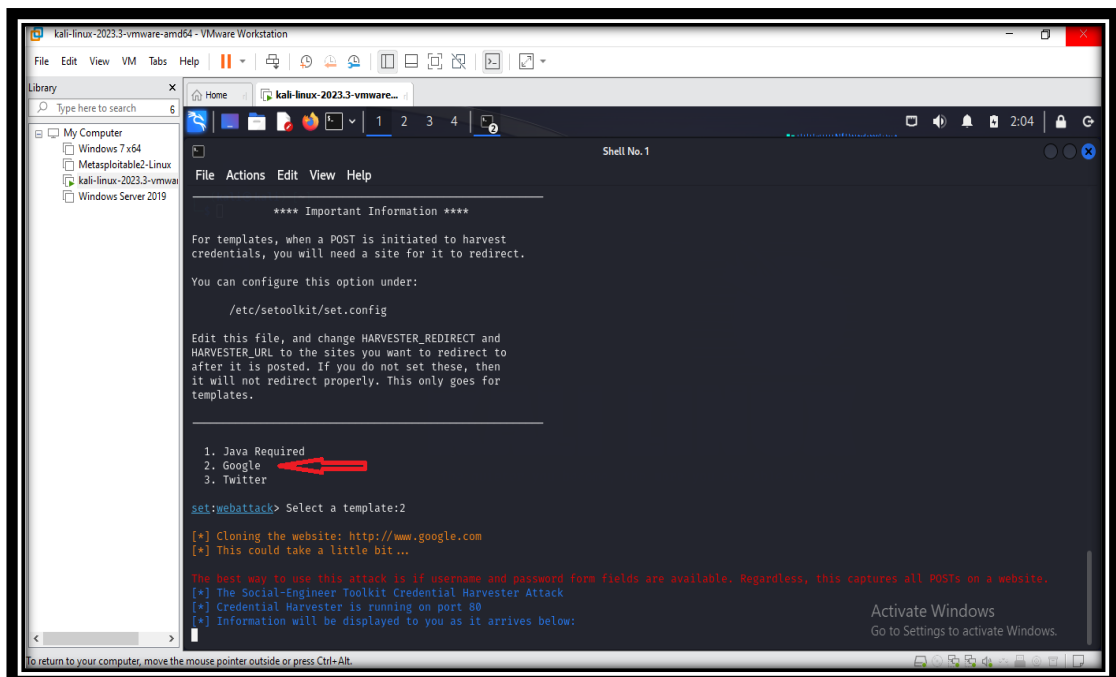
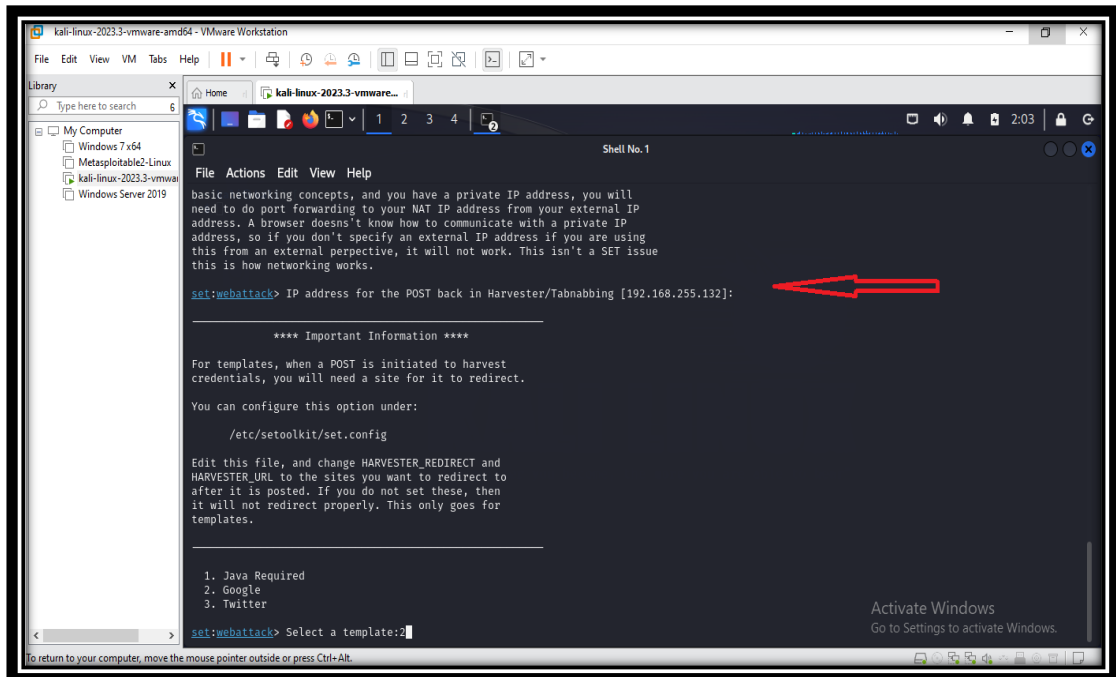
- To start, I opened my VMware and launched a Kali Linux VM. Within the Kali Linux applications, I discovered the "Social Engineering" option, which led me to the Social Engineering Toolkit (SET). After launching the tool, I encountered several options. I selected option one, which pertained to social engineering attacks.



- Upon selecting this option, I was presented with more choices. I chose option 2, signifying the "Website Attack Vector." Continuing down this path, I encountered additional options and selected option 3, specifying the "Credentials Harvest Attack Method." After this, I chose option 1, "Web templates," from the available choices.

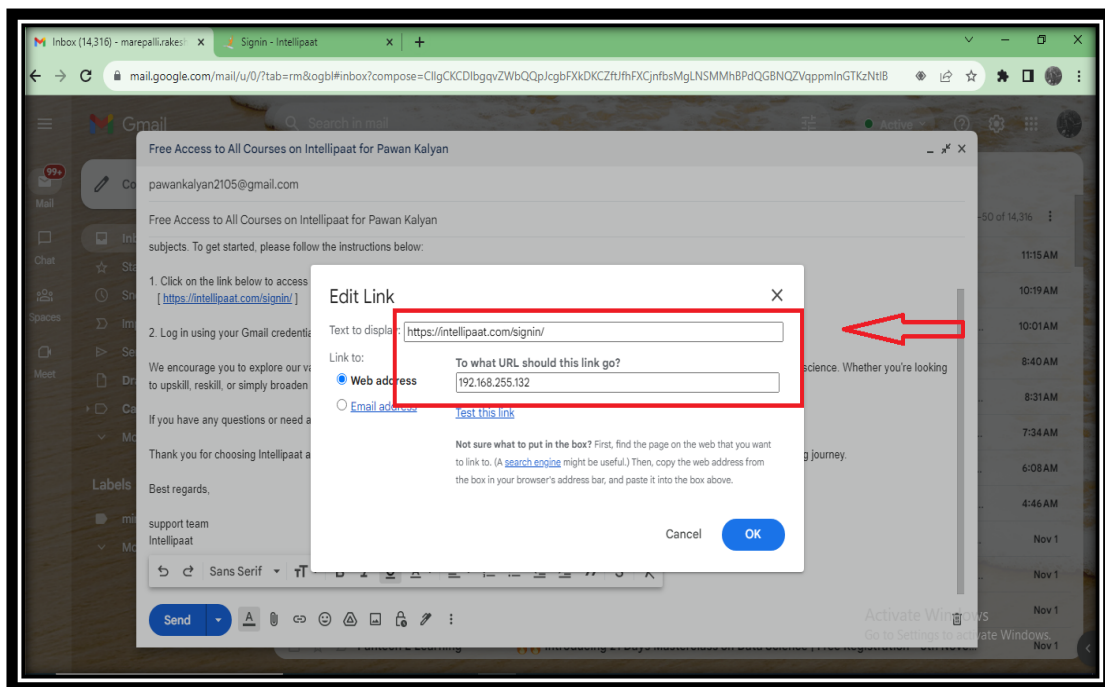
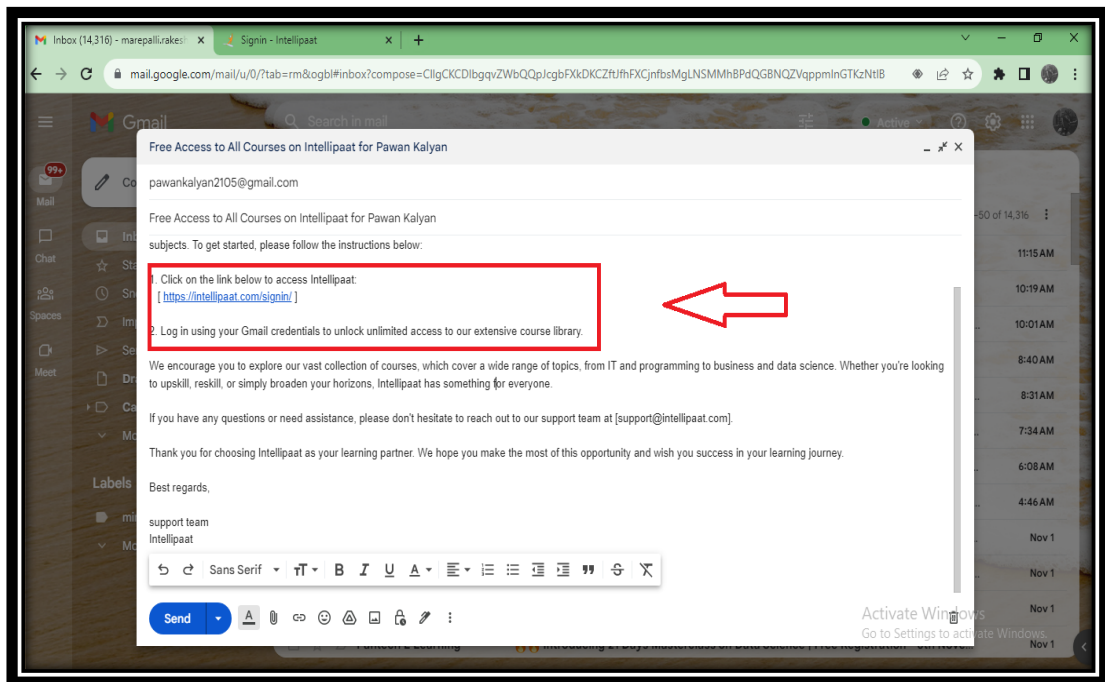


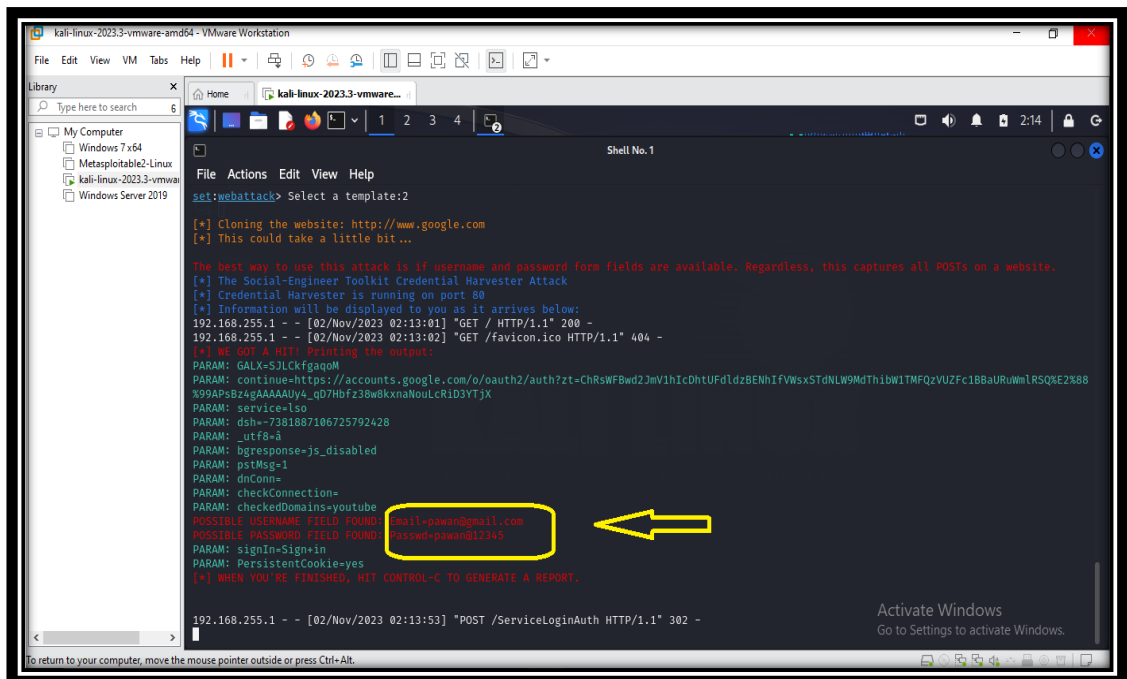
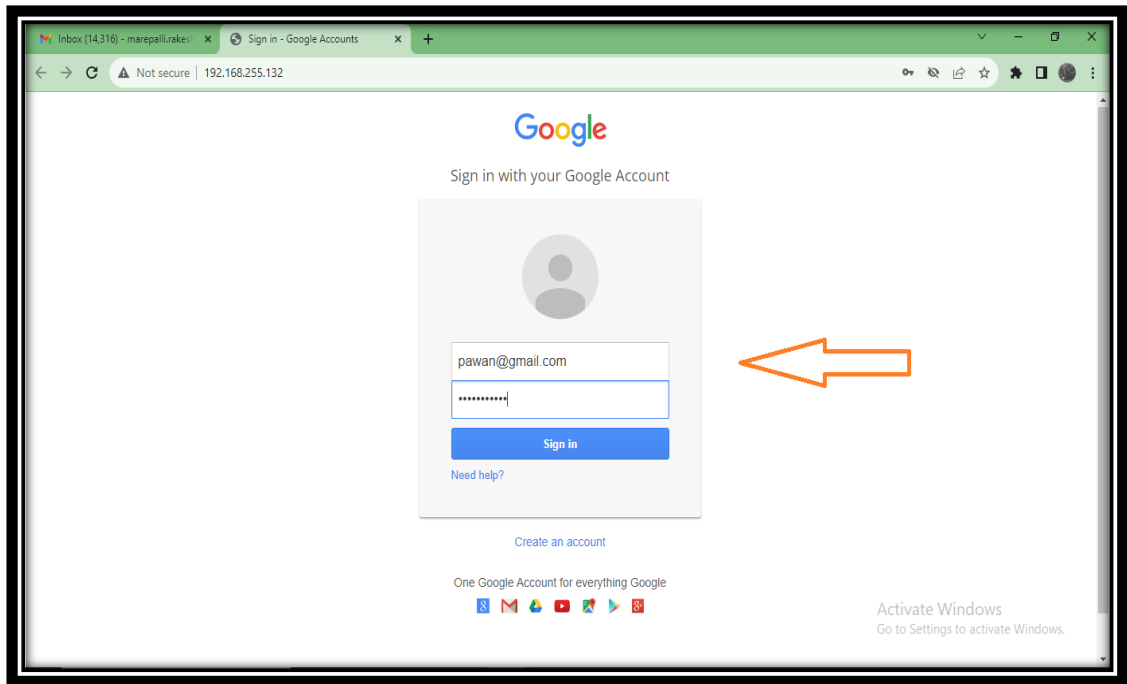
- Next, I obtained my IP address from the generated results and entered it as part of the process. Further down the line, I opted for "Google" from the available options by entering '2.' This set up the tool for credential sniffing.



- Subsequently, I crafted a phishing email and sent it to my victim. In this email, I included a malicious link generated using the SET tool. To camouflage this link, I used a legitimate link as a cover. When the victim clicked the link and entered their

credentials through the malicious link, the SET tool effectively sniffed and captured the victim's credentials, displaying them on my terminal.



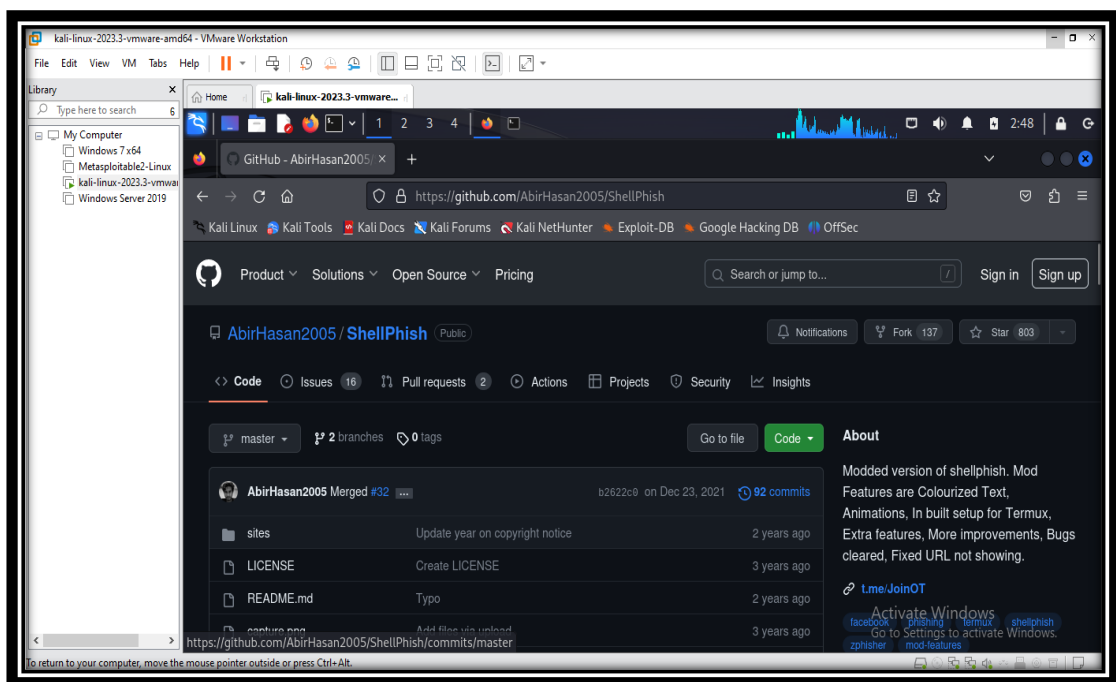


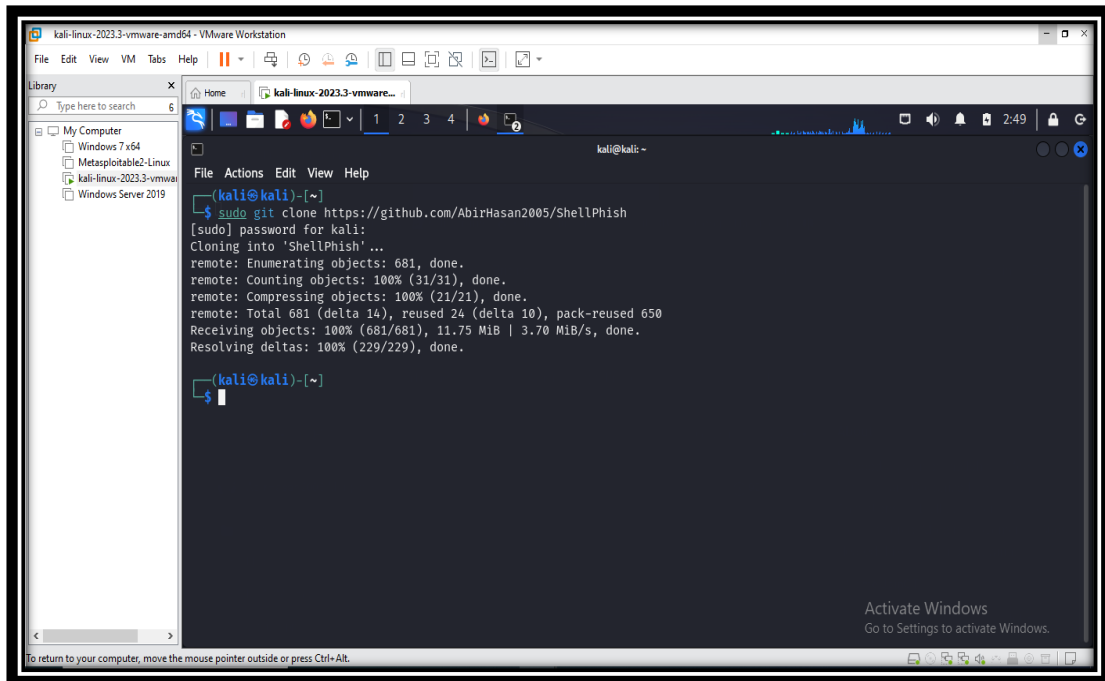
- This assignment illustrated the potential risks associated with social engineering attacks and how tools like SET can be used to exploit these vulnerabilities.

Objective: 02

Perform phishing using Shell Phish

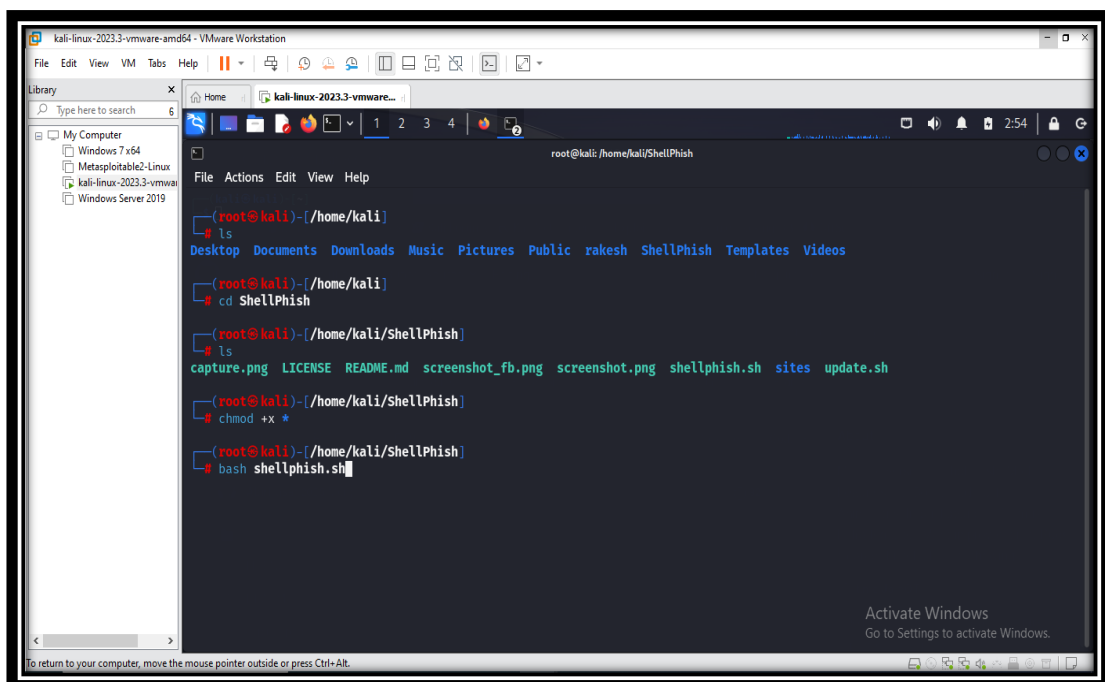
- The primary objective of this assignment is to delve into the world of phishing attacks, specifically utilizing the Shell Phish tool. Phishing is a deceptive cyberattack method aimed at duping individuals into revealing sensitive information, including usernames, passwords, and personal data, by masquerading as a trusted entity. Shell Phish is a versatile tool that empowers users to craft convincing phishing pages and gain a hands-on understanding of the strategies employed by cybercriminals.
- In this assignment, I began by launching my VMware and deploying a Kali Linux VM. Within the Kali Linux terminal, I cloned the shell Phish tool from GitHub using the 'git clone' command. Once the tool was cloned, I navigated to the shell Phish directory and executed 'bash shellphish.sh' to initiate the tool.





The screenshot shows a Kali Linux terminal window within a VMware Workstation. The terminal is at the user 'kali' prompt. The user has run the command `sudo git clone https://github.com/AbirHasan2005/ShellPhish`. The output shows the repository being cloned into 'ShellPhish'. The terminal output is as follows:

```
(kali@kali)-[~]
$ sudo git clone https://github.com/AbirHasan2005/ShellPhish
[sudo] password for kali:
Cloning into 'ShellPhish'...
remote: Enumerating objects: 681, done.
remote: Counting objects: 100% (31/31), done.
remote: Compressing objects: 100% (21/21), done.
remote: Total 681 (delta 14), reused 24 (delta 10), pack-reused 650
Receiving objects: 100% (681/681), 11.75 MiB | 3.70 MiB/s, done.
Resolving deltas: 100% (229/229), done.
(kali@kali)-[~]
$
```



The screenshot shows the same Kali Linux terminal window, now at the root prompt. The user has navigated to the cloned repository and listed the files. The terminal output is as follows:

```
(root@kali)-[/home/kali]
$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  rakesh  ShellPhish  Templates  Videos

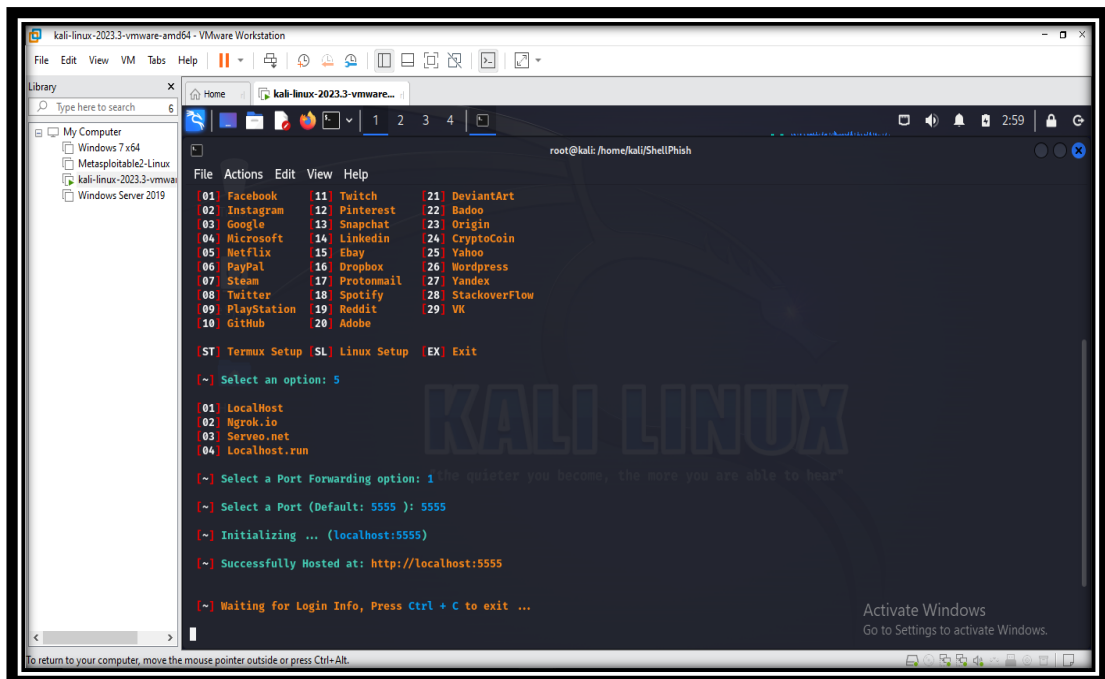
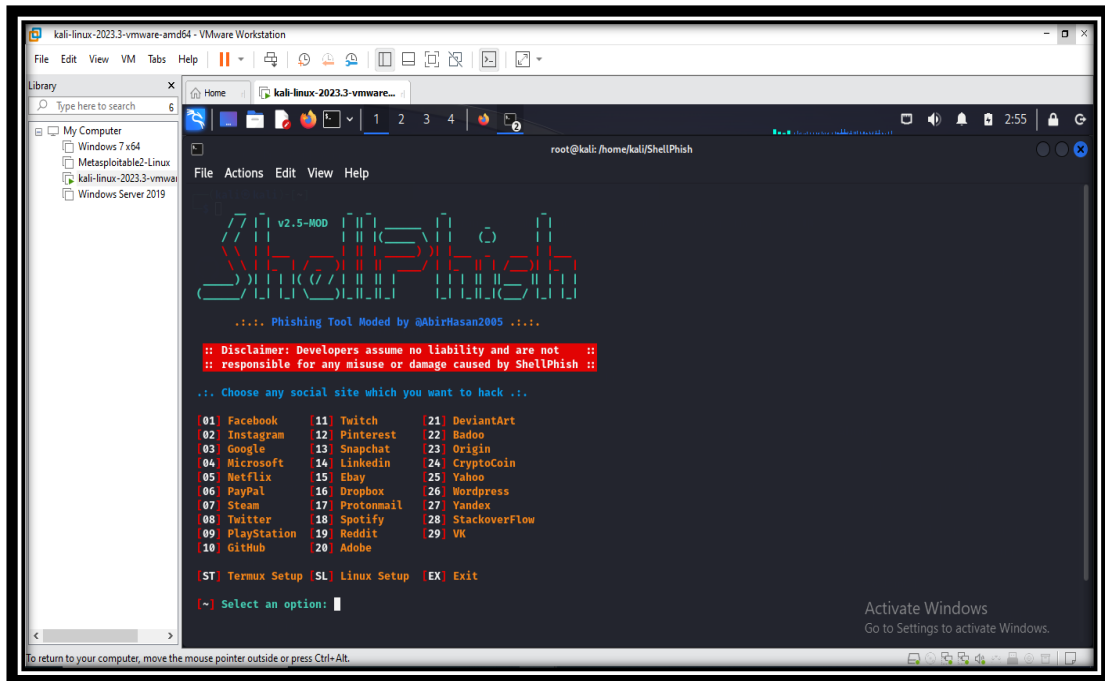
(root@kali)-[/home/kali]
$ cd ShellPhish

(root@kali)-[/home/kali/ShellPhish]
$ ls
capture.png  LICENSE  README.md  screenshot_fb.png  screenshot.png  shellphish.sh  sites  update.sh

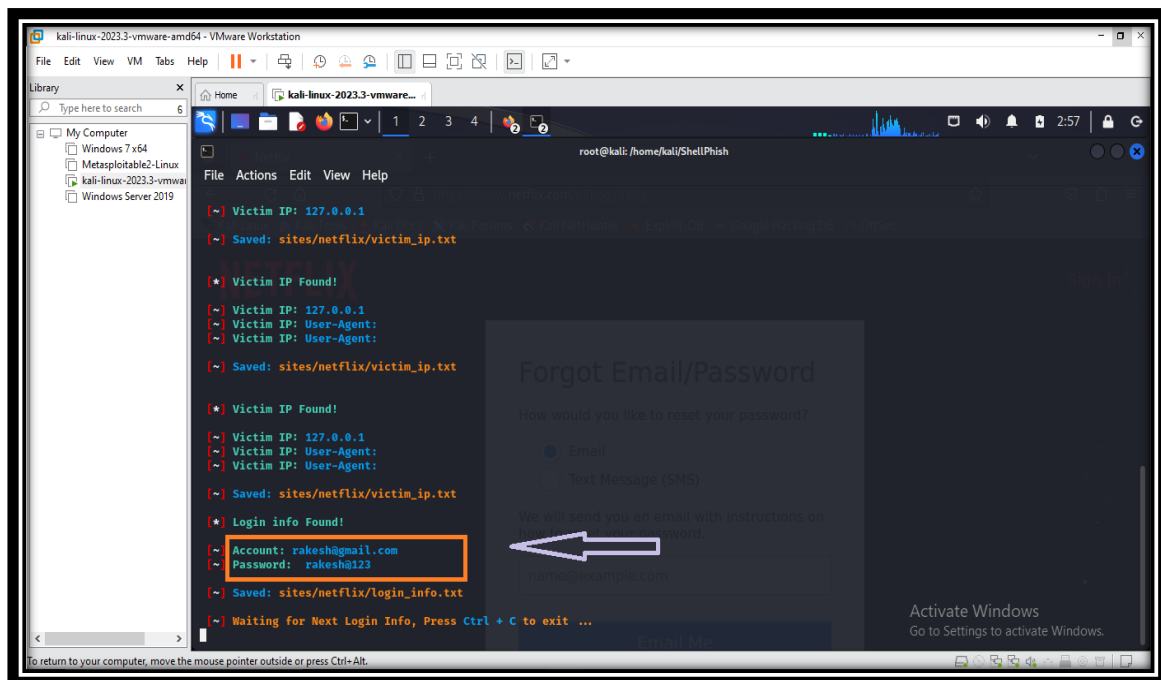
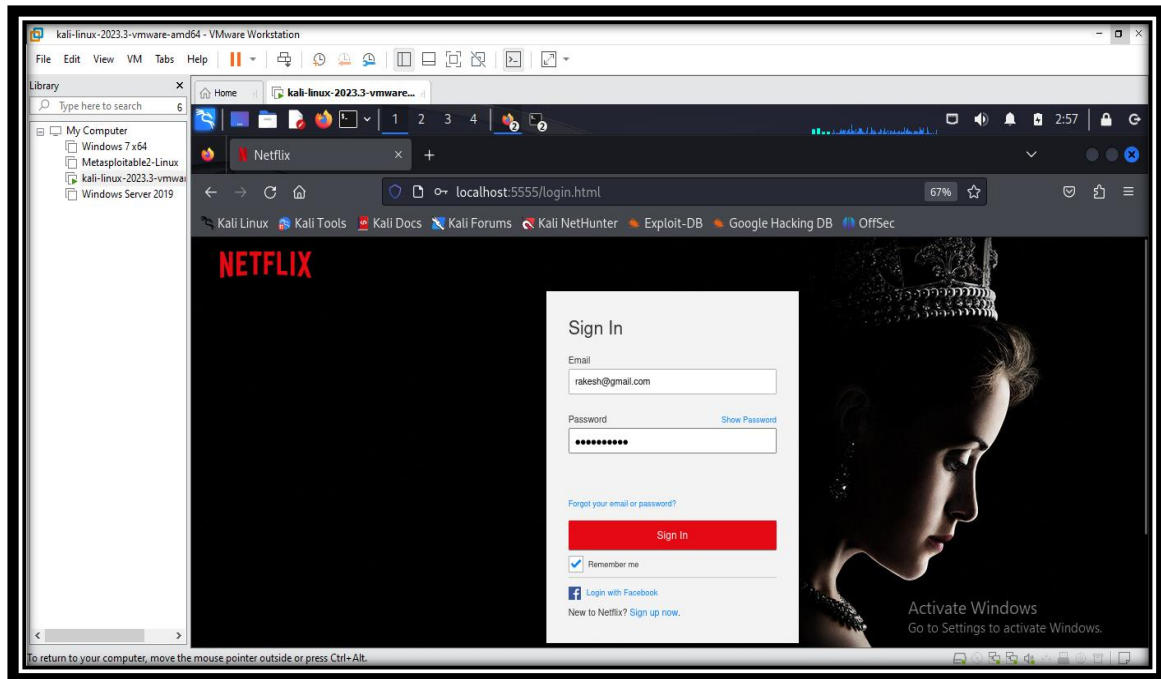
(root@kali)-[/home/kali/ShellPhish]
$ chmod +x *

(root@kali)-[/home/kali/ShellPhish]
$ bash shellphish.sh
```

- Upon launching shell Phish, I encountered a wide array of social sites, approximately 20 in total, suitable for phishing. From this selection, I chose Netflix, denoted as option 5. Subsequently, I was presented with additional options, and I opted for "localhost" (option 1). I specified my desired default port number.



- Executing the tool resulted in the generation of a phishing link. This link, concealed within a legitimate facade, could be employed to lure victims into providing their credentials. Just as in a previous assignment, I composed a phishing email, incorporating this link while maintaining a legitimate appearance. When a victim opened the email and entered their valid credentials, the shell Phish tool intercepted and displayed these credentials on my screen.



- This assignment is an immersive exploration of phishing tactics using the shell Phish tool, offering first-hand experience and insights into the mechanics of phishing attacks and reinforcing the importance of cybersecurity awareness.

Submitted By
Marepalli Rakesh
(Marepalli.rakesh@gmail.com)