# **Internship Report 2: SOCIAL ENGINEERING & PHISHING** **SIMULATION**

**1. Introduction**

This task involved conducting a Social Engineering attack to test employee awareness and improve security training programs.

To evaluate its resilience against unauthorized access and other vulnerabilities.

The goal was to identify weak points and recommend security improvements.

**2. Tools Used: SET (Social Engineering Toolkit)**

**What is SET?**

The Social-Engineer Toolkit (SET) is a collection of tools designed for penetration testing and ethical hacking, specifically focusing on social engineering attacks. It is pre-installed in Kali Linux and allows security professionals to simulate real-world attacks to assess vulnerabilities.

**Purpose of Using SET**

The primary goal of using SET is to educate individuals and organizations about the risks associated with social engineering and phishing attacks. By demonstrating how these attacks work, users can better recognize and defend against them.

**3. Methodology**

Process to setup and run the SET Toolkit for Phishing and Social Engineering

Open Github and Install from the link --

A screenshot of a computer

Description automatically generated

In Kali terminal , install it with git clone and paste the link

As the tool kit installed

Type the command “setoolkit”

A screenshot of a computer

Description automatically generated

It must be run as root, so we used “sudo setoolkit”

A screenshot of a computer

Description automatically generated

**Selecting the attack type**

To phish for the victim’s login credentials, we select option 1 for a social engineering attacks.

A black square with white text

Description automatically generated with medium confidence

We select the option 2 ‘Website Attack Vectors’

A black rectangle with white text

Description automatically generated

We choose the option 3 for ‘Credential Harvester Attack Method’

Which will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

A screen shot of a computer

Description automatically generated

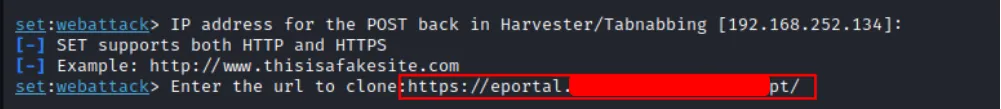
At this point we can either craft a malicious web login page or clone an existing one. We cloned a Legitimate website to make our attack look very realistic. So we select option 2

A screenshot of a computer

Description automatically generated

We press [Enter] to use our default local IP address, since we are hosting everything locally on our machine.

Then we enter the URL of the site which we want to clone. We are cloning <https://eportal.school.edu.xx/accpt/>



The setup for our phishing attack is complete, we cloned the school student portal login page, which now looks exactly like the real one.

A screenshot of a computer

Description automatically generated

Everything is Ready Now , just open the browser and paste the IP of our device as it is linked with the cloned website

A screenshot of a computer

Description automatically generated

At this point, all we need to do is trick the victim to access our IP address. So we use <https://www.shorturl.at/> to convert the IP into URL and send the victim newly created URL with email.

**4.Phishing our Victim**

**Malicious Actor**

We crafted a malicious email and sent it to our victim.

A screenshot of a computer email

Description automatically generated

As soon as the victim clicks on the link, we could capture the credentials

A screenshot of a computer program

Description automatically generated

**5.Understanding**

The SET (Social Engineering Toolkit) used for various attack vectors can be harmful if used for tricking people into clicking unknown links or images, as this can lead to stolen personal information, financial loss, identity theft, or even unauthorized control over their devices—making it crucial for everyone to be cautious and verify any unexpected messages before interacting with them.

**BUT**

It can also be a valuable educational resource when utilized responsibly, as it helps individuals understand the risks associated with clicking unknown links or images. By raising awareness about these potential threats, users can learn to protect their personal information, safeguard their finances, and maintain control over their devices, ultimately fostering a more secure online environment for everyone.

**6.Conclusion**

**Awareness and Education**

The use of SET for phishing and social engineering demonstrations is intended for educational purposes. It is crucial to conduct these activities in controlled environments and with explicit permission to avoid legal repercussions.

**Understanding Risks**

By simulating these attacks, individuals and organizations can better understand the tactics used by cybercriminals and implement stronger security measures to protect against such threats.