

# FUTURE\_CS\_02

## SOCIAL ENGINEERING & PHISHING SIMULATION

### TASK

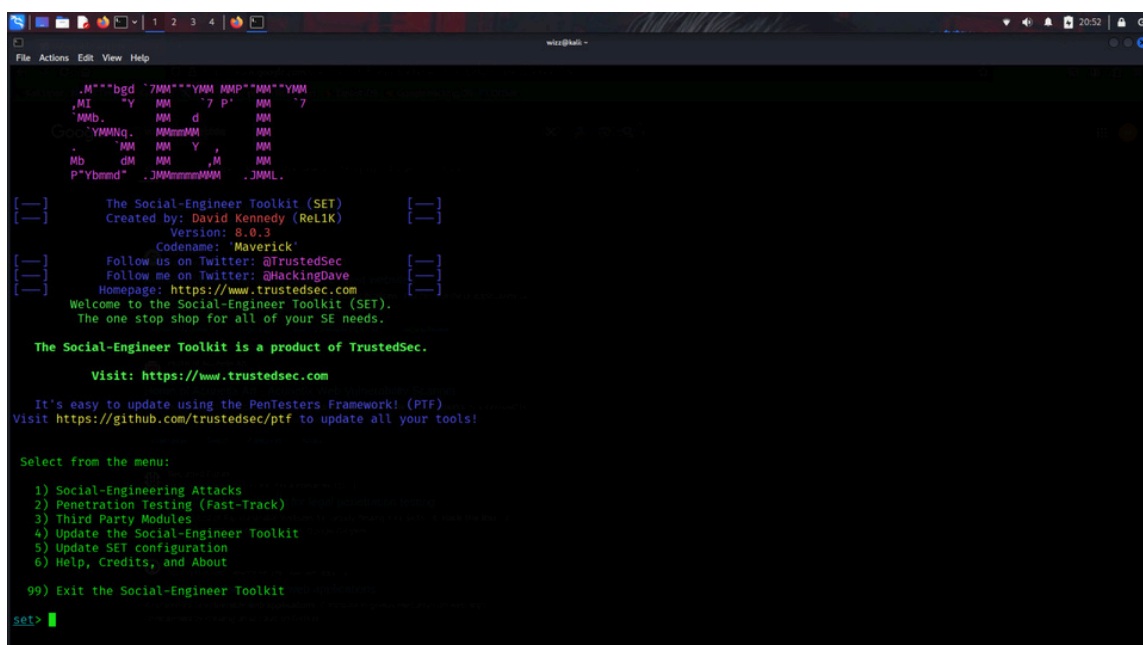
- Simulate phishing attacks to test employee awareness and improve security training programs.
- Skills Gained: Social engineering, email security, security awareness training.
- Tools: Gophish, SET (Social Engineering Toolkit).
- Deliverable: A phishing campaign report analyzing success rates and recommendations for training employees.

### TOOL USED

- SOCIAL ENGINEERING TOOL(SET)

### METHODOLOGY

- SET was used to clone a legitimate login page (Vuln Web).
- A phishing webpage was hosted on the attacker's machine using the SET credential harvester method.
- A target was asked to interact with the page to simulate real-world phishing exposure.
- Credentials submitted by the user were captured in the terminal session.



```
File Actions Edit View Help
.M""bqd `7MA""YMM MMP"MA""YMM
.MI "y MM "7 p" MA "7
.MMB. MM d MM
YMMNg. MMmmMM MM
MM MM Y MM
Mb dM MM ,M MM
P"Ybmd" .JMMmmmmMM .JMMML.

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 8.0.3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] 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> █
```

```
wizz@kali ~
File Actions Edit View Help
[~] 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.

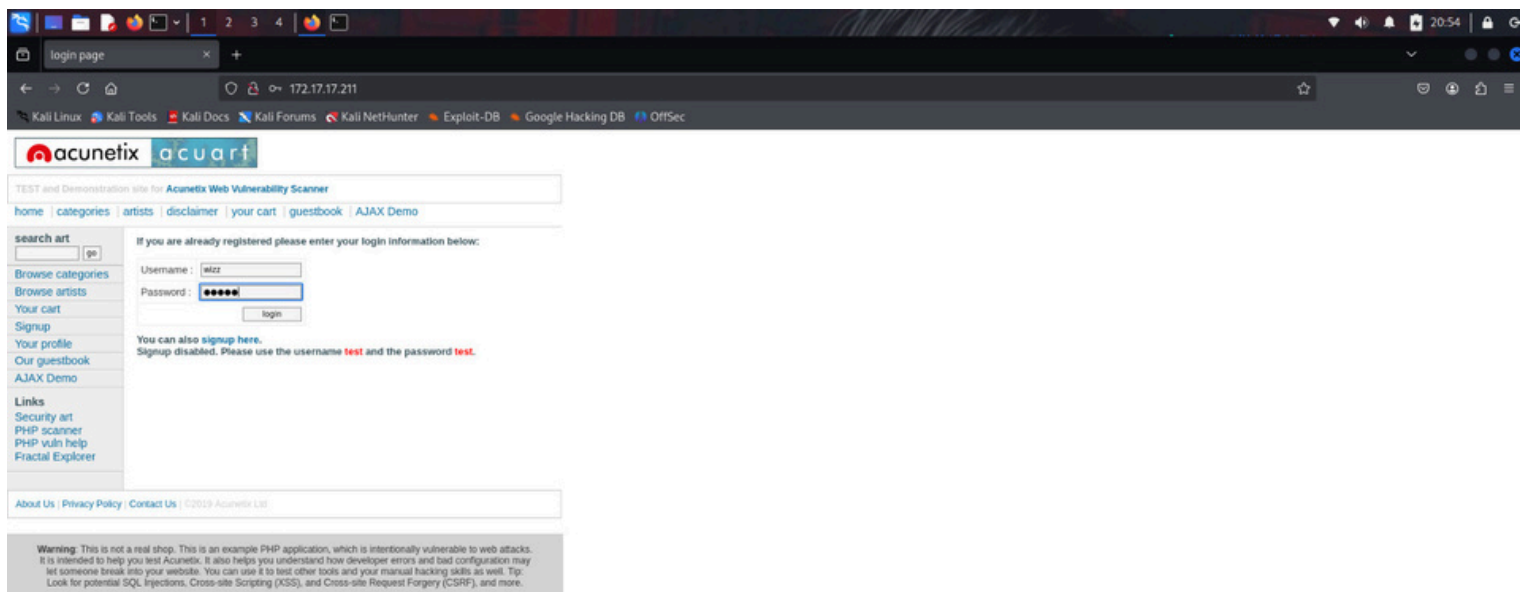
set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.17.17.211]: 172.17.17.211
[~] SET supports both HTTP and HTTPS
[~] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this 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:
172.17.17.211 - - [30/May/2025 20:53:51] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uname=wizz
POSSIBLE PASSWORD FIELD FOUND: pass=12344
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

## OBSERVATION

- The cloned page appeared visually identical to the original.
- Entering credentials redirected to an error page to avoid suspicion.
- Credentials entered were logged and visible in the terminal.
- This demonstrated how attackers exploit human behavior more than technical flaws.



## **RECOMMENDATIONS**

- Conduct regular phishing awareness training.
- Simulate phishing attacks as part of internal security assessments.
- Use email filters, DNS security, and warning banners for external emails.

## **CONCLUSION**

The task successfully demonstrated how phishing can harvest user credentials and why awareness is a critical part of cybersecurity.