**FUTURE INTERNS CS TASK 2**

**SOCIAL ENGINEERING & PHISHING SIMULATION**

**INTRODUCTION**

This report presents the findings of a Social Engineering and Phishing Simulation.

The assessment deploying of a Fake Login Site and Capturing the credentials of users using SET.

Task: Simulate phishing attacks to test employee awareness and improve security training programs.

Tools: SET (Social Engineering Toolkit).

Environment: Kali Linux (in VirtualBox)

Apache2 Web Server : Local IP Used: 10.x.x.xx

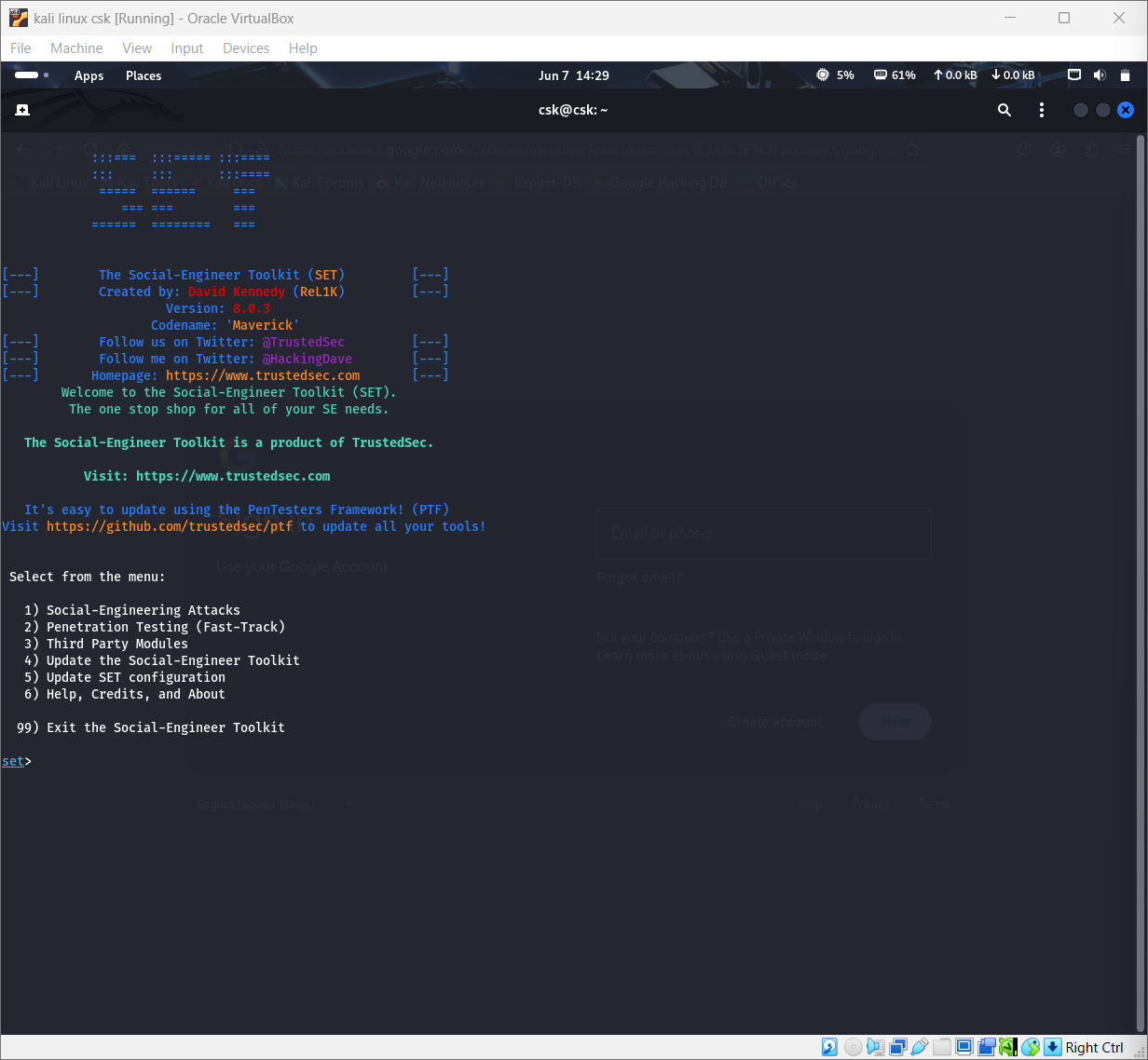
**STEP BY STEP GUIDE**

**STEP 1 : Launch SET Toolkit**

Navigate to terminal

Execute “ sudo setoolkit “

Enter yes and hit enter .



# STEP 2: NAVIGATE TO CREDENTIAL HARVESTER

In the SET menu:

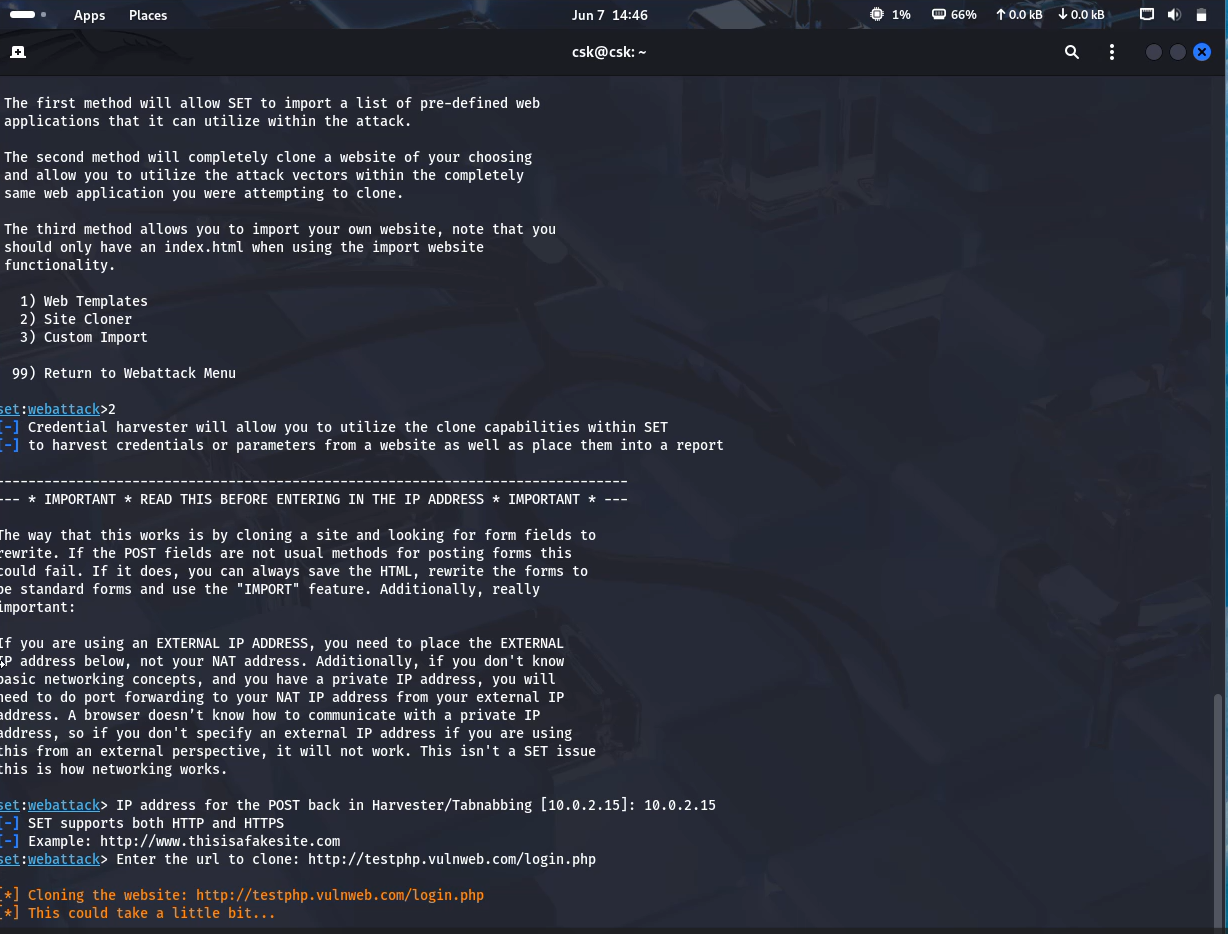
Choose 1) Social-Engineering Attacks  
 Choose 2) Website Attack Vectors  
 Choose 3) Credential Harvester Attack Method  
 Choose 2) Site Cloner



**STEP 3: ENTER HOSTING INFORMATION**

Enter the IP address to use for the POST back in Harvester/Tabnabbing: 10.x.x.xx

Enter the URL to clone: <http://testphp.vulnweb.com/login.php>

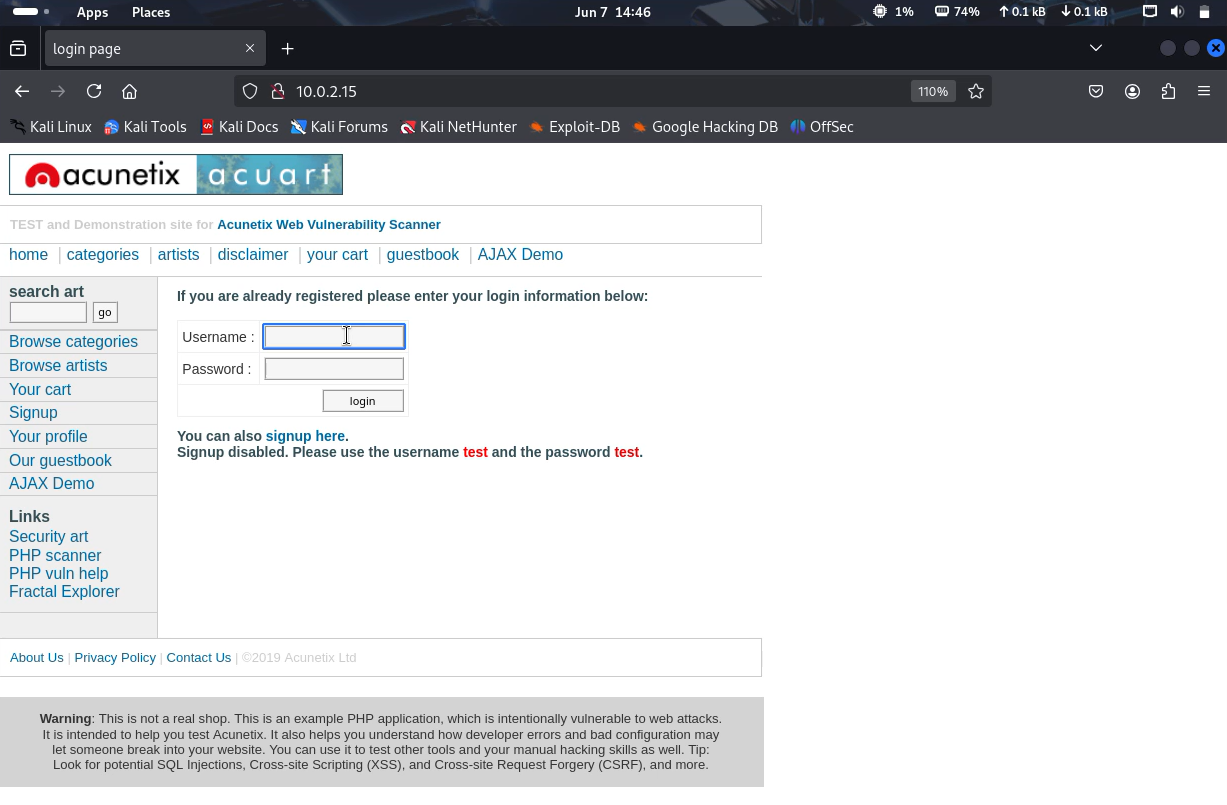


**STEP 4: HOSTING CLONED PAGE**

SET automatically places the cloned phishing page into /var/www/html and starts hosting it.

Navigate to firefox browser . Enter <http://10.x.x.xx> (hosting ip address)

The cloned page appears



This page is seen for employees. Enter the credentials . here we have used test and test for testing purposes.

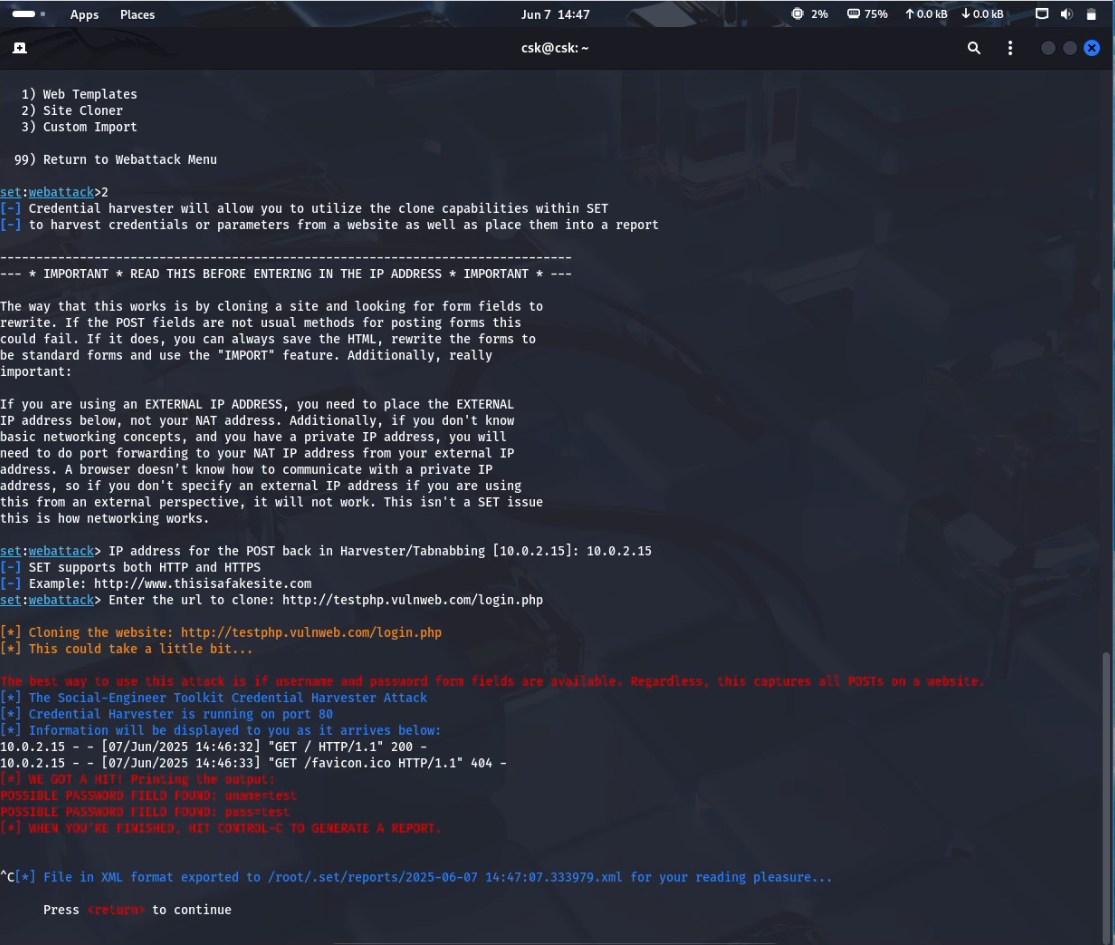
**STEP 5: CHECK FOR CAPTURED CREDENTIALS**

Navigate to terminal hosting SET

We can see the captured credentials .

Use following command to see the credentials stored in the computer :

cat /root/.set/reports/credentialharvester.txt



**RECOMMENDATIONS FOR TRAINING EMPLOYEES**

1. Launch Phishing Awareness Campaigns

Run regular phishing simulations (like this one) to test and improve employee response.

Include internal leaderboards (gamification) showing awareness growth.

2. Create an Email Security Checklist

Teach employees to check:

* Sender's email domain
* Spelling/grammar errors
* Hover over links before clicking
* Check for HTTPS and the correct domain
* Suspicious file attachments or login requests

3. Enforce Acceptable Use Policy (AUP)

* Make it clear that:
  + Login pages must never be accessed from suspicious emails
  + Passwords must not be shared or reused
  + Personal browsing on work machines should be avoided

4. Technical Safeguards

Even well-trained users may still fall victim. Add:

* Multi-Factor Authentication (MFA)
* Link analysis and sandboxing of attachments
* Email filters for known phishing signatures
* Block unknown IPs accessing internal services

5. Document Policy Violations

* Maintain logs of simulation results
* For employees repeatedly failing simulations, mandatory retraining should be enforced

6. Incorporate Phishing in Onboarding

* Introduce phishing awareness in the first week of employment
* Simulate an attack within the first month to benchmark baseline awareness

7. Provide Tools for Reporting

* Add “Report Phishing” button in email clients
* Provide a dedicated cybersecurity hotline or email
* Train employees to report, not ignore suspicious emails

**SUBMITTED BY :** MODEKURTI SRIHARSHA

**ROLE:** Cybersecurity Intern

**COMPANY :** Future Interns