■■ SET Credential Harvester Manual (2025 Updated Edition)

1. Introduction

Tool: Social Engineering Toolkit (SET)
Attack Vector: Credential Harvester (phishing via cloned login pages)
Update Focus: Apache integration, new menu items, Tabnabbing, Web Jacking, Mass Mailer improvements.
Use Case:
- Red Team → Demonstrate phishing techniques in training labs.
- Blue Team → Learn indicators of phishing for defense.

2. Starting SET

Command:
sudo setoolkit

Menu Navigation:
1 → Social-Engineering Attacks
2 → Website Attack Vectors
3 → Credential Harvester Attack Method
2 → Site Cloner

Note: If Apache is disabled, edit /etc/setoolkit/set.config and set APACHE_SERVER=ON.

Input	Description
IP Address	Attacker machine IP (lab only)
URL to clone	Target login page (e.g., test site)
Output Location	/var/www/html/ (Apache default directory)
Apache Config	Enable in /etc/setoolkit/set.config (APACHE_SERVER=ON)

3. Setup

Updated input and configuration for 2025 release.

4. File Locations

Path	Purpose
/var/www/html/	Cloned site files
/var/www/html/harvester.txt	Logs captured credentials (simulation only)
/etc/apache2/sites-enabled/	Apache configs
/etc/setoolkit/set.config	Main SET configuration file

Common directories used by SET for cloned sites and harvested credentials.

5. Example Workflow

sudo setoolkit
→ Social Engineering Attacks
→ Website Attack Vectors
→ Credential Harvester
→ Site Cloner

Enter IP (Kali VM IP) + target login URL (test site only).

SET clones the site into /var/www/html/ and captures credentials.
If Apache is not active, enable and restart service.

Example target (for lab use): http://testphp.vulnweb.com/login.php

Indicator	Defense Measure
Suspicious shortened URL	Block via email filters
No HTTPS / fake certs	Warn users; enforce TLS inspection
Odd IP in link	Educate users; DNS filtering
Login page looks 'off'	Awareness training & phishing simulations
Unexpected POST traffic	Monitor logs; trigger SIEM alerts
Mass phishing emails	Email gateways + phishing detection AI

6. New Attack Vectors

- Tabnabbing → replaces background tab with malicious login page.
- Web Jacking → overlays legitimate site with a fake login form.
- Multi-Attack Mode → run several attack vectors at once for simulation.
- Credential Harvester remains core module but enhanced with better logging.

7. Mass Mailer Improvements

- Supports Gmail and custom SMTP providers.
- Options for sender name, subject, attachments, HTML/plain text.
- Improved reliability and reduced chance of failure.
- Useful for simulating spear-phishing campaigns (lab use).

8. Blue Team Notes

Updated defenses against modern SET phishing techniques.

9. Defensive Best Practices

- Enforce MFA → stops stolen credentials from being useful.
- Awareness Training → teach recognition of cloned sites & fake emails.
- TLS/HTTPS validation → warn if fake/self-signed certs.
- DNS and email filtering → block shortened/malicious links.

- SIEM/Log monitoring → detect abnormal login patterns or POST traffic.

10. Ethical Use Policy

- For controlled labs and authorized pentests only.
- Never use against real accounts or unauthorized systems.
- Purpose: Educate, train, and secure systems against phishing.