# Social-Engineer Toolkit (SET) - Practical Lab Cheat Sheet

⚠ Important: Use SET only inside an isolated virtual lab environment. This guide is for educational purposes and CEH practice only.

## 1. Start SET

Command to launch:

sudo setoolkit

This opens the interactive menu with options like:

1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration

## 2. Credential Harvester (Phishing Page)

Steps to perform in a lab environment:

1) Choose: 1 → Social-Engineering Attacks

2) Choose: 2 → Website Attack Vectors

3) Choose: 3 → Credential Harvester Attack Method

4) Choose: 1 → Web Templates OR 2 → Site Cloner

5) Enter your attacker IP and target site URL (dummy/test site).

6) SET hosts the cloned site. Victim visits http://<attacker-ip> and enters test credentials.

7) Credentials are displayed in SET console.

## 3. Malicious Payload (Test Only)

1) Main Menu: 1 → Social-Engineering Attacks

2) Choose: 4 → Create a Payload and Listener

3) Select payload type (e.g., windows/meterpreter/reverse\_tcp).

4) Enter your IP and port.

5) SET creates payload file for testing inside victim VM.

6) Place payload manually on victim VM (no internet use).

## 4. Spear-Phishing Email Attack

1) Main Menu: 1 → Social-Engineering Attacks

2) Choose: 5 → Mass Mailer Attack

3) Select: E-Mail Attack Single or Mass Email Attack

4) Use a test SMTP server and send to a test email account on victim VM.

5) Optionally attach payload or a phishing link.

## 5. Lab Safety & Logging

- Run Wireshark on both VMs to observe traffic.

- Review logs in SET directory:

cat ~/.set/logs/<file>

## 6. Quick Command / Menu Reference

|  |  |
| --- | --- |
| Command / Menu Option | Purpose |
| sudo setoolkit | Launch SET |
| 1 → 2 → 3 | Website → Credential Harvester |
| 1 → 4 | Create payload + listener |
| 1 → 5 | Mass Mailer Attack |
| Ctrl+C | Stop listener / attack |
| cat ~/.set/logs/<file> | View saved results |