# Module 09: Social Engineering - Practical Guide

This guide focuses on the specialized tools and hands-on laboratory sessions required to master the "Human Hacking" phase of the CEH v13 curriculum.

## 1. Comprehensive Social Engineering Toolset

### The Frameworks

* **Social Engineering Toolkit (SET):** The industry standard. It is a Python-driven framework that automates almost every social engineering attack, from website cloning to SMS spoofing.
* **Gophish:** A powerful, open-source phishing platform designed for businesses and penetration testers to run simulated phishing campaigns and track user clicks/submissions.

### Website Cloning & Impersonation

* **HTTrack:** While used for reconnaissance, it is vital for Social Engineering to "clone" a target website accurately so it can be hosted on an attacker's server as a phishing portal.
* **Wifiphisher:** Used to mount automated phishing attacks against Wi-Fi networks. It forces users to disconnect from their real AP and connect to a "rogue" one that serves a social engineering page (e.g., "Firmware Update Required - Enter Password").

### OSINT for Target Profiling

* **Sherlock:** Used to find a target's presence across hundreds of social media platforms, allowing for a more convincing "pretext" during an attack.
* **theHarvester:** Essential for gathering the email addresses of employees within a specific company to build a spear-phishing list.

## 2. Hands-On Lab Sessions

### Lab 1: Credential Harvester Attack (SET)

**Goal:** Create a pixel-perfect clone of a login page to steal usernames and passwords.

1. **Open SET:** In Parrot OS terminal, type sudo setoolkit.
2. **Navigate:** Choose 1) Social-Engineering Attacks -> 2) Website Attack Vectors -> 3) Credential Harvester Attack Method.
3. **Clone:** Choose 2) Site Cloner.
4. **IP Configuration:** SET will ask for your "IP for the POST back". This is your Parrot OS local IP.
5. **Target URL:** Enter the URL you want to clone (e.g., http://testphp.vulnweb.com/login.php).
6. **Test:** Open the browser on a victim machine and visit your Parrot OS IP.
7. **Result:** When the victim "logs in," their credentials will appear in cleartext in your terminal.

### Lab 2: Malicious QR Code Generator (SET)

**Goal:** Create a QR code that redirects a victim to a malicious URL when scanned.

1. **Open SET:** Run sudo setoolkit.
2. **Navigate:** Choose 1) Social-Engineering Attacks.
3. **Generate:** Choose 9) QRCode Generator Attack Vector.
4. **URL:** Enter the URL you want the QR code to point to (e.g., your credential harvester IP).
5. **Location:** SET will generate a .png file in your /root/.set/reports/ directory.
6. **Use Case:** An attacker might print this and stick it over a legitimate "Scan for Menu" code at a restaurant.

### Lab 3: Spear-Phishing with Gophish

**Goal:** Set up a full-scale corporate phishing simulation.

1. **Configure Sending Profile:** Set up an SMTP relay (like a Gmail account or local Mailserver).
2. **Create Landing Page:** Import a site (like Microsoft 365) and check "Capture Submitted Data".
3. **Build Email Template:** Write a convincing email (e.g., "Urgent: Password Reset Required"). Include the {{.URL}} placeholder.
4. **Launch:** Add a list of targets and launch the campaign.
5. **Dashboard:** Watch the real-time graph to see who opened the email, who clicked the link, and who submitted their credentials.

### Lab 4: Social Media Recon with Sherlock

**Goal:** Profile an individual to choose the best social engineering "pretext."

1. **Run Command:** sherlock [Target\_Username]
2. **Analyze:** Identify which platforms the user is active on (e.g., Twitter, GitHub, Instagram).
3. **Scenario:** If you find they are an active developer on GitHub, you can send a spear-phishing email pretending to be from GitHub Support regarding a "Security breach in your repository."

### Lab 5: Wireless Social Engineering (Wifiphisher)

**Goal:** Trick a user into giving up their Wi-Fi password.

1. **Run Tool:** sudo wifiphisher.
2. **Select Target:** Choose a target AP to "deauthenticate" users from.
3. **Choose Scenario:** Select the "Network Manager Connect" or "Firmware Upgrade" scenario.
4. **The Attack:** The tool creates a "Twin" AP. When the user connects, they see a screen saying their router needs an update and they must enter their WPA password.

## 3. CEH Practical Tips

* **SET Port:** SET usually runs on port 80. Ensure Apache (sudo systemctl stop apache2) is stopped before starting the Website Attack Vector.
* **Pretexting:** The "Pretext" is the made-up story an attacker uses. For the exam, remember that the most successful pretexts use **Authority** or **Urgency**.
* **Phishing vs. Pharming:** \* **Phishing** uses an email to lead you to a fake site.
  + **Pharming** redirects you to the fake site automatically by poisoning your DNS/Host file (no email required).