TRAINING DAY 24 REPORT:

Phishing :

- ## Introduction to Phishing

Phishing is a type of **social engineering attack** where attackers trick users into revealing sensitive data such as:

- Passwords

- Credit card numbers

- OTPs

- Personal Identifiable Information (PII)

How it works:

- Attackers send a **fake email/message/website** that looks genuine.

- It urges the victim to click a link or enter details.

- That data is captured and misused by the attacker.

Types of Phishing:

1. Email Phishing – Fake emails with malicious links.

2. Spear Phishing – Targeted attacks on specific individuals or companies.

3. Smishing – Phishing through SMS.

4. Vishing – Phishing via voice calls.

5. Angler Phishing – Fake social media accounts or messages.

Purpose:

- Identity theft

- Credential stealing

- Bank fraud

- Spying or gaining unauthorized access

- ## Part 1: Creating a Phishing Page

This section generally explains how to:

- Clone a legitimate website (e.g., Facebook, Instagram).

- Use tools like `HTTrack`, `Blackeye`, or `SocialFish` to mirror the login page.

- Modify the cloned page to send login info to the attacker's server.

Key Components:

`index.html`: Cloned login page.

`login.php`: Captures the credentials and stores them (often in a `.txt` file).

`credentials.txt`: Stores the stolen data.

Legal Note: Always perform phishing labs in **ethical environments**, not for illegal use.

- ## Part 2: Hosting the Phishing Page

This step includes:

- Hosting the cloned page **locally** (on your computer) using tools like:

  - `PHP Server` (`php -S 127.0.0.1:8080`)
  - `Apache` (via XAMPP or LAMP)

- Once hosted locally, the attacker must expose it to the internet using tunneling services like **Ngrok**.

Objective:

- Let anyone over the internet access your fake page.

- ## Part 3: Collecting Credentials & Tracking

This final part focuses on:

- Setting up the `login.php` script to collect:

  - Username
  - Password
  - IP address
  - Device info (optional)

- Using `tail` or `cat` to read live stolen credentials.

- Optional: Email alerts when someone falls for the trap.

Ethical Training Tip: Combine with **IP tracking tools** (like Hound) to collect geolocation/IP-based details from the target.

- # Installation of Ngrok

Ngrok is a tunneling tool that creates **public URLs** for your local server (like your phishing page).

Purpose:

- Makes your local page accessible from anywhere on the internet.

Installation Steps:

1. Go to https://ngrok.com and sign up.

2. Download ngrok binary (`ngrok.exe` for Windows, or Linux version).

3. Use terminal commands:

   - `ngrok authtoken <your-token>`
   - `ngrok http 8080` (assuming your phishing page runs on port 8080)

Result:

- You get a **public link** like: `https://a1b2c3.ngrok.io`

- Share this with the target (in social engineering attack)

- # Phishing Tools – Blackeye, ShellPhish, SEToolkit

➢ ## Blackeye:

- Bash-based script for generating phishing pages.

- Supports cloning of over 30 websites (Facebook, Instagram, Netflix, etc.)

- Easy to use with terminal.

Command:

```
bash blackeye.sh
```

- **ShellPhish:**

  - Another open-source phishing tool.

  - Offers automated website cloning + ngrok hosting.

  - Better GUI in terminal.

  Command:

  ```
  bash shellphish.sh
  ```

- **SEToolkit (Social Engineering Toolkit):**

  - A powerful Python-based tool used by penetration testers.

  - Offers:

    - Credential harvester
    - Fake login pages
    - Malicious payload creation
    - Email phishing, SMS spoofing

  - Often used in **Kali Linux**.

  Command:

  ```
  sudo setoolkit
  ```