# Experiment-9: Bruteforce Attack using Burpsuite

**Aim:**

To create a bruteforce attack on DVWA to retrieve the username and password

**Tools Required:**

Damn Vulnerable Web Application (DVWA)

**Procedure:**

1.Open kali -> burpsuite -> proxy
(Run meta and type the meta ip address in kali firefox browser and click on dvwa)
2. Open dvwa -> bruteforce and enter random username and password
(keep the security low)
3. Now open a new tab in firefox and type **about:config** and click on **accept the risk and continue**
4. In the opened browser search bar , type **hijack** and give true for the all service which were disabled
5. Now keep the intercept on in burp suite and click on login in dvwa (request will be captured in bs)
6. Click on **action -> send to intruder** and disable the intercept
7. In Burp suite go to **intruder** and before making any changes click on **clear $** (which will clear all the $ signs)
8. Now select the username which was given as input and click on **Add $.** Do the same for the password also.(do this in a sequential manner)
9. In **Attack type** choose **Cluster Bomb (As we are going to brute force in more than one parameter (username and password)**
10. Now go to **Payloads** tab ( Payload set : 1 or 2 , 1->username , 2->password)
11. Keep the payload set as **1** and the Payload type as **Simple Kit**

12. Add any no.of usernames including the given username and click on **Add** button
13. Keep the payload set as **2** and the Payload type as **Simple Kit**
14. Add any no.of passwords including the given password and click on **Add** button
15. Now go to **Settings** tab and clear all history of errors in **grep match** field.
16. Go to dvwa -> view source (on the bottom of the page) . Select the error message which will be like “Username and Password Incorrect” and copy it.
17. Now in Burp suite paste the selected message where we cleared the history and click on **Add**
18. Now click on  **Start attack** and click ok.

# Experiment-10:Remote File Upload Vulnerability

**Aim:**

To upload a file in DVWA and checking the upload vulnerability

**Tools Required:**

Damn Vulnerable Web Application (DVWA)

**Procedure:**

1.Boot Kali VM and go to firefox.

2.Download a high resolution image from the internet and save it locally.

3.Open a new tab in browser and go to Steganography online(Github pages)

4.Import the downloaded image.

5.Get a vulnerable code from github and paste it in the message field in Steganography webpage and click on encode.

6.Save the last image in the page locally.

7.Now open DVWA in Kali and keep the security low.

8.Goto Upload -> browse and select the downloaded vulnerable image and click on upload.

# Experiment-11: Phishing Attack – using Kali Linux “setoolkit”

### Definition:

Phishing attack using kali Linux is a form of a cyber attack that typically relies onemail or other electronic communication methods such as text messages and phone calls. It is one of the most popular techniques of social engineering. Where hackers pose as a trustworthy organization or entity and trick users into revealing sensitive and confidential information.

### Aim:

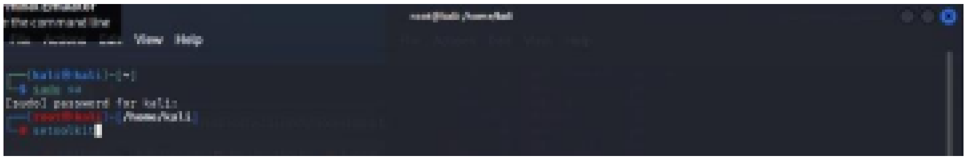
We will create a phishing page using Social Engineering Toolkit which is a preinstalled functionality in Kali Linux OS. The phishing link can be sent to any user on the same Local Area Network as you and the data that they enter on the fraudulent page will be stored in a file on the attacker’s machine.

### Prerequisites:

Social Engineering Toolkit or SET for short is the standard for social engineering testing among security professionals and even beginners must have a basic idea about using the tool. Basically, it implements a computer-based social engineering attack.

### Procedure:

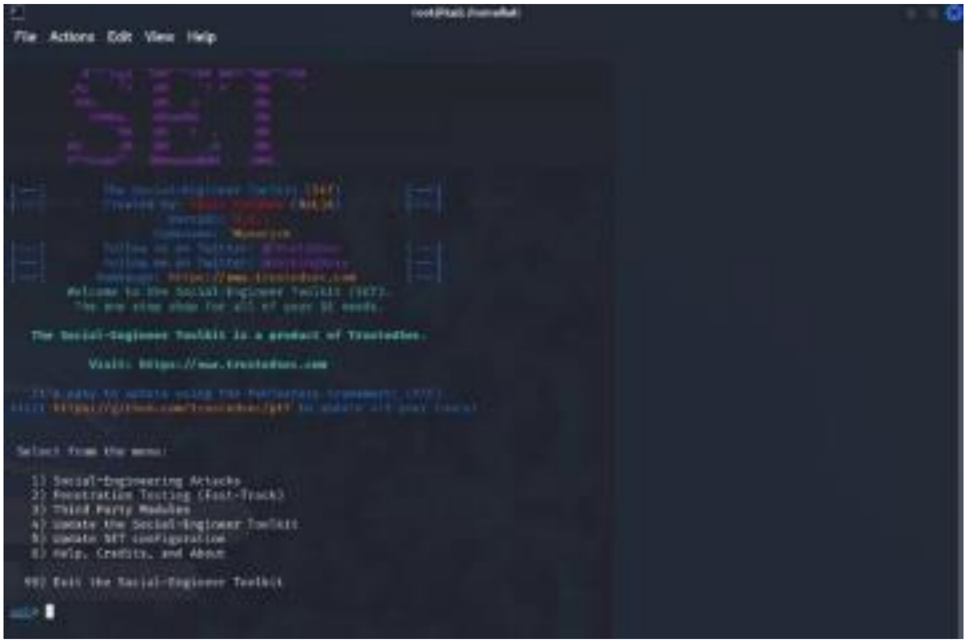
- Open the terminal window in Kali and make sure you have root access as ‘setoolkit’ needs you to have root access
- Type ‘setoolkit’ in the command line



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# setoolkit
```

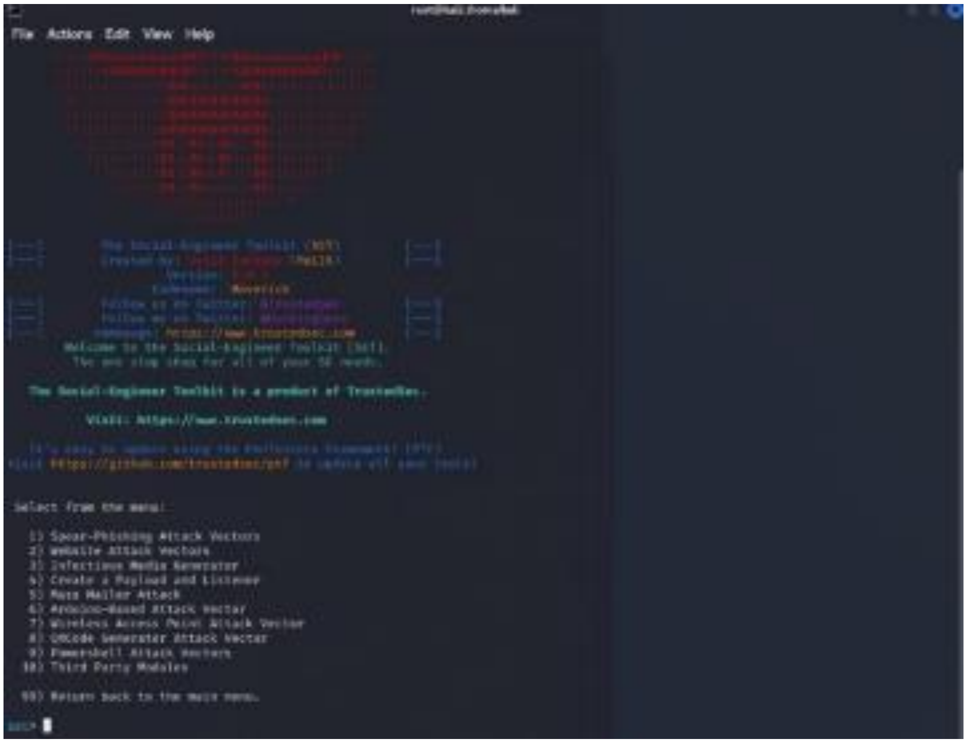
You will be warned that this tool is to be used only with company authorization or for educational purposes only and that the terms of service will be violated if you use it for malicious purposes.

- Type y to agree to the conditions and use the tool
- A menu shows up next. Enter 1 as the choice as in this demo we attempt to demonstrate a social engineering attack.



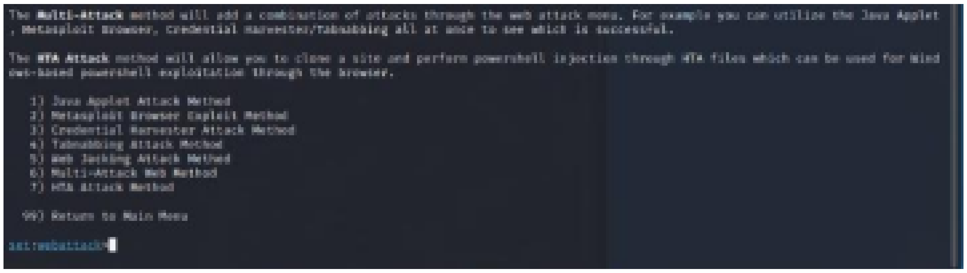
```
[---]        The Social-Engineer Toolkit (SET)        [---]
[---]        Created by: David Kennedy (ReL1K)        [---]
                  Version: [illegible]
                Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec        [---]
[---]        Follow me on Twitter: @HackingDave       [---]
[---]       Homepage: https://www.trustedsec.com      [---]
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

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

  99) Exit the Social-Engineer Toolkit

set>
```

Under Social Engineering, there are various computer-based attacks and SET explains each in one line before asking for a choice.



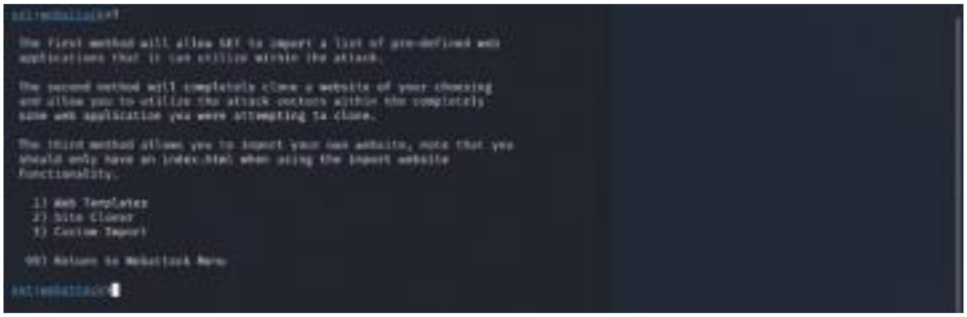
```
[---]        The Social-Engineer Toolkit (SET)        [---]
[---]        Created by: David Kennedy (ReL1K)        [---]
                  Version: [illegible]
                Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec        [---]
[---]        Follow me on Twitter: @HackingDave       [---]
[---]       Homepage: https://www.trustedsec.com      [---]
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set>
```

- Now under social engineering among other we choose Website Vector Attacks.



```
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet
, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Wind
ows-based powershell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>
```

- Select the ‘Credential Harvester Attack Method’ as out aim is to obtain user credentials by creating a bogus page that will have certain form fields.Now we have a choice to either craft a malicious web page on our own or we can use the setoolkit to just clone an existing trustworthy site (in our case linkedin ).



```
set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>
```

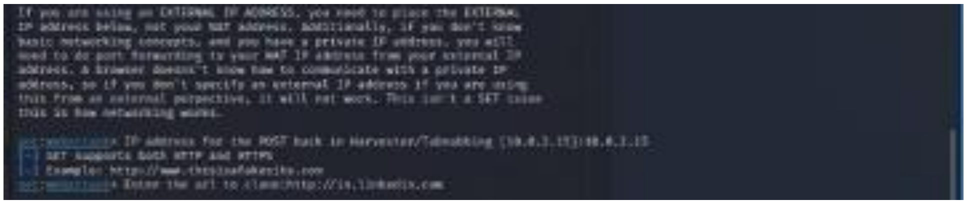
- Select ‘Site Cloner’

- Now we have to get the ipaddress of our local machine, SET will ask us to provide an IP where the credential captured will be stored.

- Paste the IP address of our local machine.

- Since we chose to clone a website we have to provide the URL to be clonned. In this example it will be http://in.linkedin.com (note: avoid ‘https’ instead use ‘http’ ).

- Social Engineering toolkit now clones the URL provided and runs it on the local server.



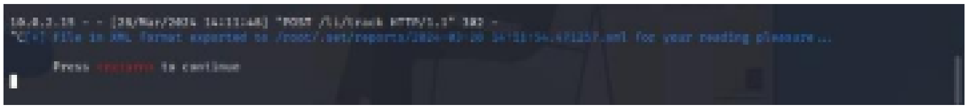
```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://in.linkedin.com
```

The setup for a phishing attack is complete, you have cloned Facebook and hosted it on the server.

- Now Go to browser and type http://"your Ip" (eg: http://10.0.2.15) which will open our bogus cloned page.

If an unsuspecting user fills in their details and clicks on 'Log In', the fake page takes them to the actual linkedin login page. Usually, people tend to pass it off as a  glitch on the browser or an error in their typing.

- Once we finish the attack we can come back to the terminal and stop the attack  by clicking Ctrl+c and then 'enter'.
- Once finished the setoolkit will store all the information gathered from the attack at '/root/.set/reports' location as .xml file
- We can use *cat* command to view the contents through terminal.



```
10.0.2.15 - - [28/Mar/2024 14:11:46] "POST /li/track HTTP/1.1" 302 -
^C[*] File in XML format exported to /root/.set/reports/2024-03-28 14:11:54.471257.xml for your reading pleasure...

      Press <return> to continue
```

## Experiment-12: Self Signed certificate creation using raspberry pi

### Aim:

To create a self signed certificate in raspberry pi using openssl.

### Tools Required:

Raspberry pi kit.

### Procedure:

## Creating a Self-Signed Certificate:

1. **Install OpenSSL:**
   If OpenSSL is not already installed on your Raspberry Pi, you can install it using the following command:

```
sudo apt-get update
sudo apt-get install openssl
```

2. **Generate a Private Key:**
   Use OpenSSL to generate a private key. In this example, we'll generate a 2048-bit RSA private key:

   ```
   openssl genrsa -out private.key 2048
   ```

3. **Generate a Certificate Signing Request (CSR):**
   Use the private key to generate a CSR. This will prompt you to enter information about your organization and domain:

   ```
   openssl req -new -key private.key -out csr.pem
   ```

4. **Generate a Self-Signed Certificate:**
   Use the private key and CSR to generate a self-signed certificate:

   ```
   openssl x509 -req -days 365 -in csr.pem -signkey
   private.k ey -out certificate.crt
   ```

## Verifying the Certificate:

1. **View the Certificate Details:**
   You can view the details of the certificate using the following command:

   ```
   openssl x509 -in certificate.crt -text -noout
   ```

2. **Verify the Certificate Chain:**
   To verify the certificate chain, you can use OpenSSL's `verify` command:

   ```
   openssl verify -CAfile certificate.crt certificate.crt
   ```

   **This will** Output something like:

```
certificate.crt: OK
```

If the certificate is valid, it will display "OK".

### Using the Certificate:

You can now use the generated certificate (`certificate.crt`) and private key (`private.key`) in your applications that require SSL/TLS encryption, such as web servers, MQTT brokers, etc.

## Accessing Raspberry Pi’s terminal in Windows

If you want to access your Raspberry Pi's terminal from a Windows computer without downloading any additional software like PuTTY, you can use the built-in Windows command prompt or PowerShell along with the `ssh` command. Here's how you can do it:

### Steps:

1. **Get the IP Address of Your Raspberry Pi:**
   You'll need the IP address of your Raspberry Pi to connect to it via SSH. You can find this by running `ifconfig` in the terminal on the Raspberry Pi or by checking your router's DHCP client list.

2. **Open Command Prompt or PowerShell:**
   On your Windows computer, open Command Prompt or PowerShell. You can do this by searching for "cmd" or "PowerShell" in the Start menu.

3. **Connect to Raspberry Pi Using SSH:**

   In the command prompt or PowerShell, use the `ssh` command followed by the username and IP address of your Raspberry Pi. The default username is usually `pi` . Replace `username`with your actual username and `xxx.xxx.xxx.xxx`with the IP address of your Raspberry Pi.

   ```
   ssh username@xxx.xxx.xxx.xxx
   ```

   For example:

   ```
   ssh pi@192.168.1.100
   ```

4. **Enter Password:**

   After running the `ssh` command, you'll be prompted to enter the password for your Raspberry Pi. Enter the password and press Enter.

5. **Access the Terminal:**

   Once authenticated, you'll have access to the terminal of your Raspberry Pi directly from the Windows command prompt or PowerShell. You can now execute commands as if you were using the terminal directly on the Raspberry Pi.

## Notes:

Ensure that your Raspberry Pi and your Windows computer are connected to the same network, whether it's a mobile hotspot or a local Wi-Fi network.

Make sure SSH is enabled on your Raspberry Pi (you can enable it through the Raspberry Pi Configuration).

Ensure that your Raspberry Pi's IP address is reachable from your Windows computer.

This method uses the built-in SSH client available in recent versions of Windows. If you're using an older version of Windows that doesn't have this feature, you may need to use a third-party SSH client like PuTTY.