16. Evading Firewall, IDS, Honeypot

Practical 1: Working with Windows Firewall

1. In Microsoft Windows OS, Go to Control Panel ==> Windows Firewall.

2. Click on “Turn Windows Firewall on or off”.

3. Check the boxes that says “Turn on firewall” for Private Network Settings and Public Network Settings.

4. To add some manual rules, click on Advanced Settings.

Practical 2: Working with Linux Firewall (UFW)

1. To install ufw on Kali Linux enter the following command in terminal:

```
apt-get install ufw gufw
```

2. Once it is installed, you can find “Firewall Configuration” in All Applications list. If you click on that, you can get the graphical interface of it.

3. To do it from console, enter the following command:

```
sudo ufw enable
```

Note: ufw comes pre-installed with Ubuntu OS. You can follow 3rd step to enable it.

Practical 3: Using Snort IDS in Kali Linux

1. Install snort by entering following command:

```
apt-get install snort
```

2. To edit a configuration file, enter following command:

```
leafpad /etc/snort/snort.conf
```

3. In the file find a line like: ipvar HOME_NET <any>
In place of <any> enter your system’s IP Address and save the file and close.

4. In terminal, enter command in following syntax:

```
snort -i <device> -q -A console -c /etc/snort/snort.conf
```

For example:

```
snort -i eth0 -q -A console -c /etc/snort/snort.conf
```

Practical 4: Using valhala honeypot in Windows

1. Double click on the honeypot icon of valhala to start.

2. Click on Server Config.

3. Provide desired configuration for few servers which we want to.

4. Click on monitoring button to start. Valhala will get minimised.

5. From attacker system perform NMAP port scan to check if ports got open.

6. Now all the activities will get logged in valhala.

Practical 5: Using honeybot in Windows

1. Install the honeybot application from the installer.

2. Start it by double clicking on HoneyBot icon.

3. You can provide configuration by going to options.

4. Click on start button to start monitoring.

5. Now go to attacker system and perform NMAP port scan. You can see so many ports/services open.

6. All activities on them gets logged in honeybot.