FORMAN CHRISTIAN COLLEGE

(A CHARTERED UNIVERSITY)

Spring 2021

COMP421: Information Security

Assignment #1

Name: Ossama Bin Raza

Student ID: 22-10162

Setting up the environment:

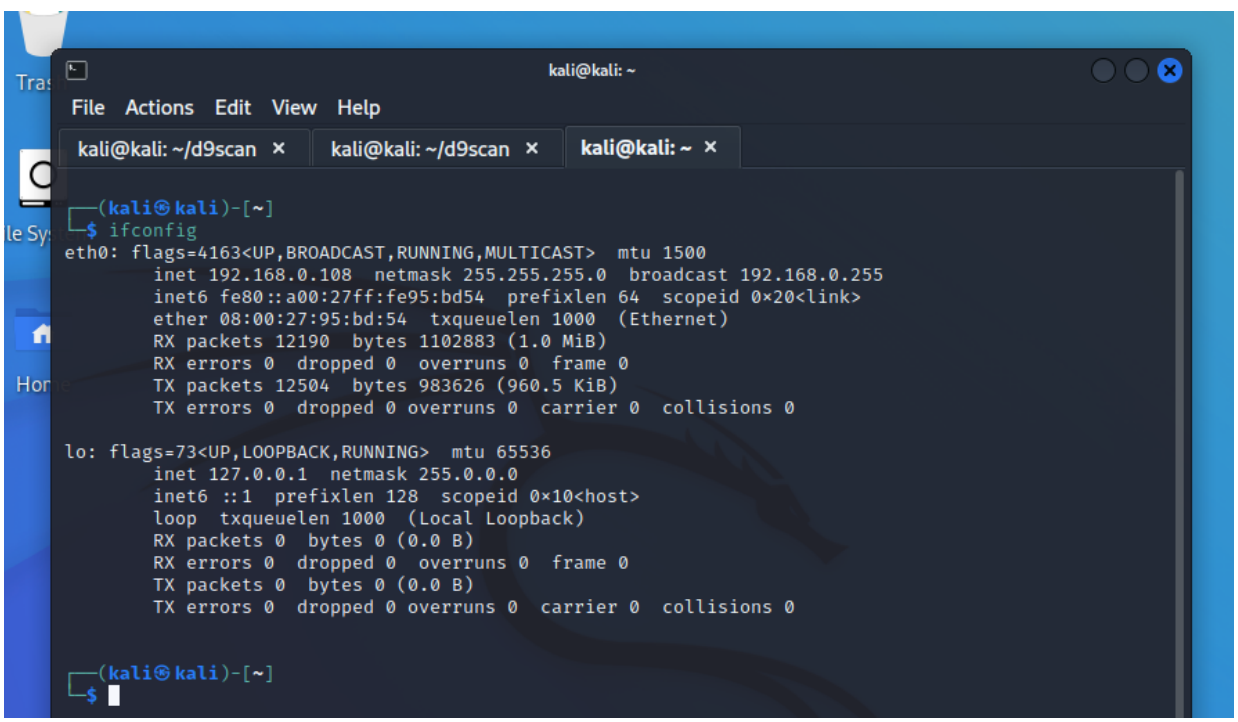
Use ‘ifconfig’ command in metasploitable2 to check if an IP address is assigned.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:24:0f:e6
          inet addr:192.168.0.106  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe24:fe6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:103 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10454 (10.2 KB)  TX bytes:13003 (12.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:360 errors:0 dropped:0 overruns:0 frame:0
          TX packets:360 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:152989 (149.4 KB)  TX bytes:152989 (149.4 KB)

msfadmin@metasploitable:~$
clear     ifconfig  ipconfig
msfadmin@metasploitable:~$
```

The same ‘ifconfig’ command is used in Kali Linux terminal to check if an IP address is assigned.

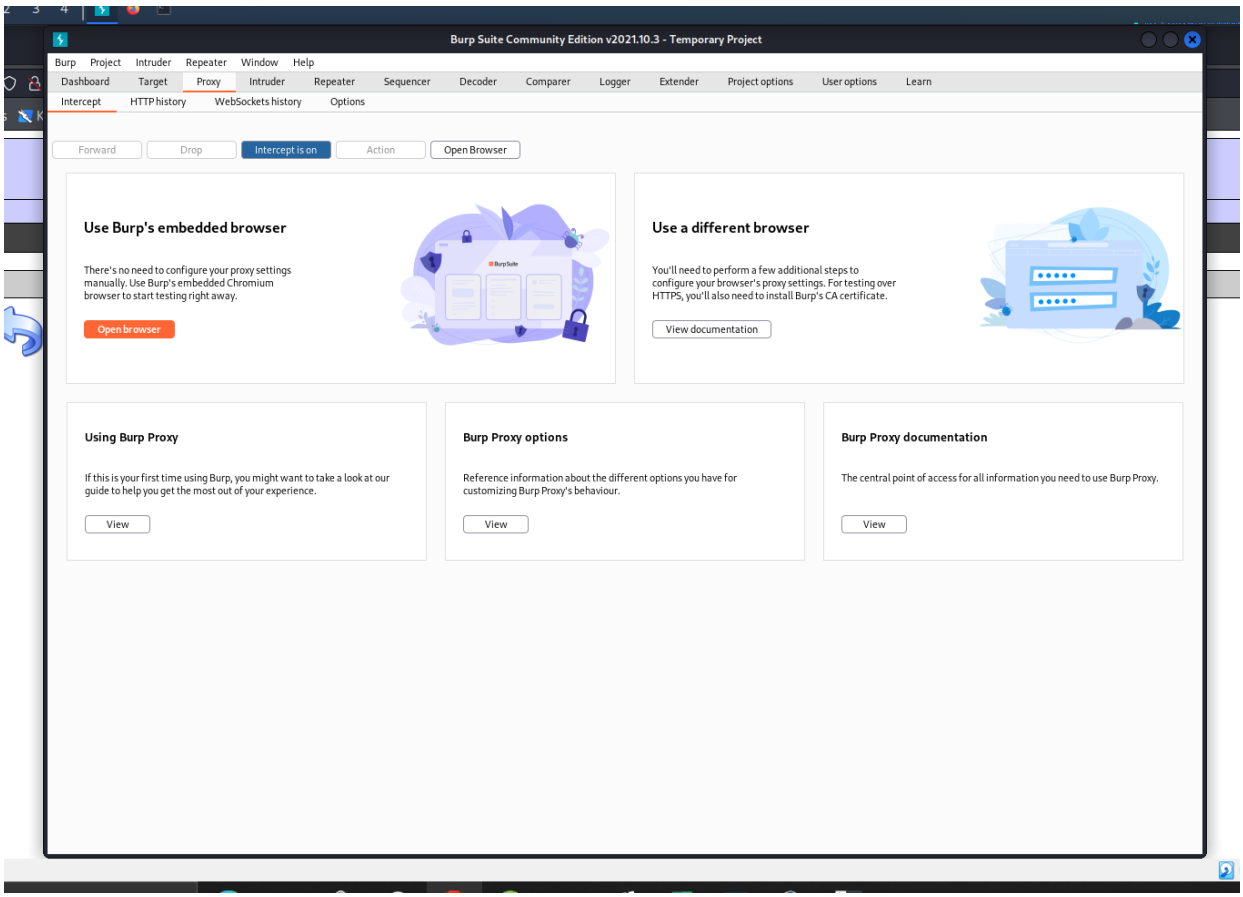


Steps to perform the attack:

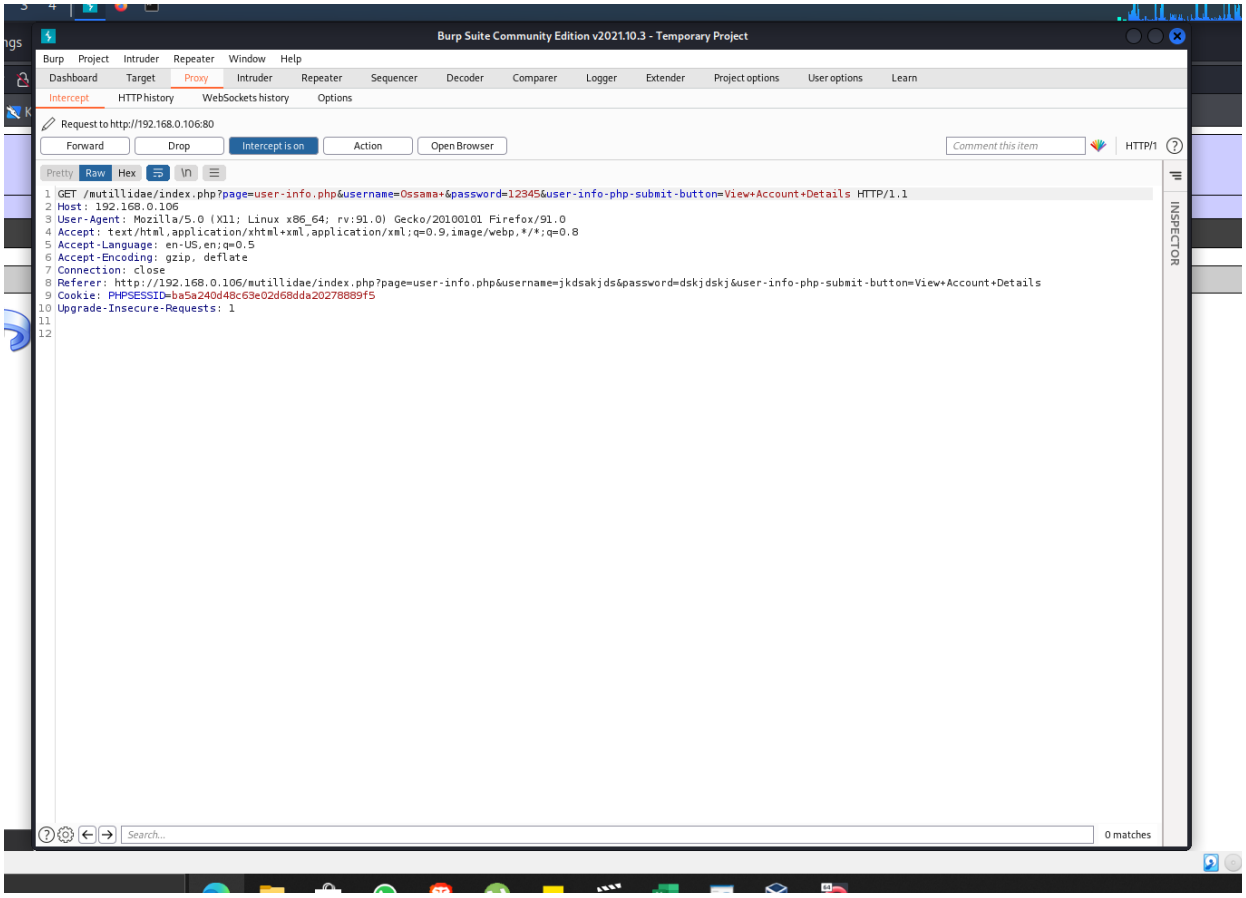
Notice that both the machines are assigned different IP addresses with the same subnet mask.

Use a web browser and enter the IP address of the Metasploitable2 machine. Select the 'mutillidae' link to get redirected to the Mutilldae page. From there the dummy page is selected where the user enters their login credentials.

Start up BurpSuite and turn on the intercept feature.



Set up the proxy setting in the browser. Use dummy data to login to the website. These dummy credentials are captured by the BurpSuite software as shown.



Save the extracted data. In this case the extracted data is save onto the desktop and is named ‘extract’.

Now use the sqlmap software through terminal to detect and exploit database vulnerabilities from the extracted data

The ‘cd Desktop’ command is used to change the target directory to ‘Desktop’

Then the ‘sqmap -r extract.txt --dbs’ command is used where extract.txt is the file name.

Different entry points are shown on the terminal along with the available databases. Select in any one of the database and use the command ‘sqmap -r extract.txt -D mysql –tables’ (mysql is the name of one of the available databases)

The tables will now be displayed and the command ‘sqmap -r extract.txt -D mysql -T credit_cards –dump’ is used to view the data contained in the table and the information is dumped to be viewed later.

The output of the sql attack is saved in the ‘sql injection dump’ file.