

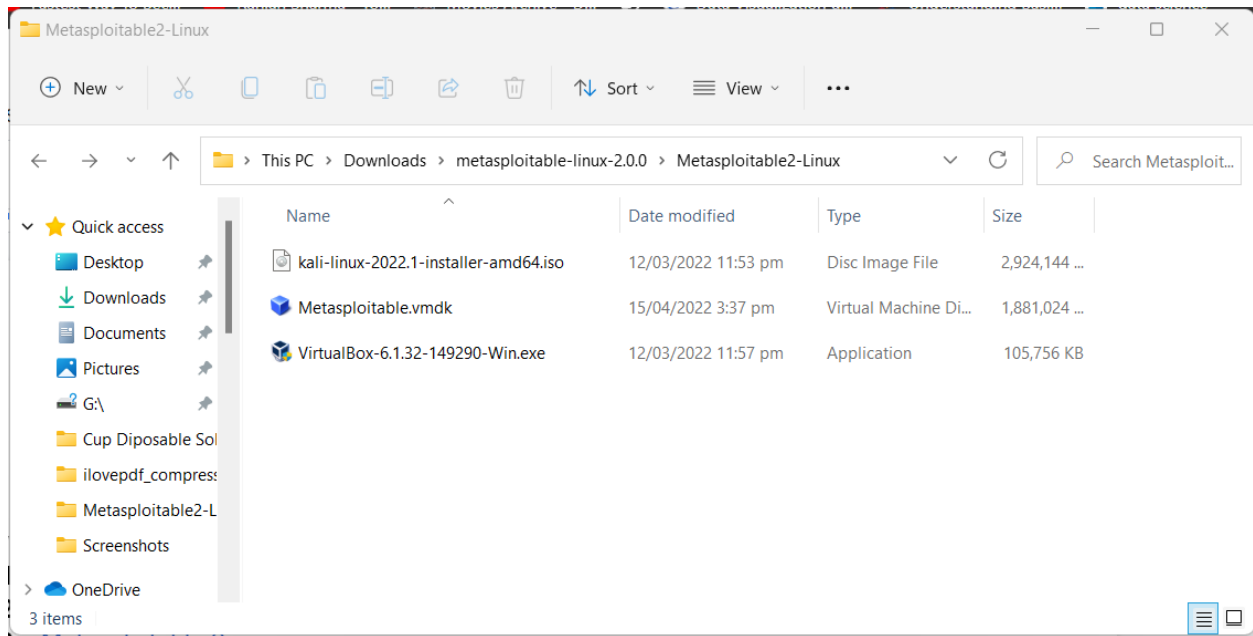
Assignment 1

Muhammad Waleed
22-11081

Step 1:

Download the following things: ([Screenshot 1.1](#))

1. [Oracle VM Virtual Box.](#)
2. [Kali Linux iso image file.](#)
3. [Metasploitable 2.](#)

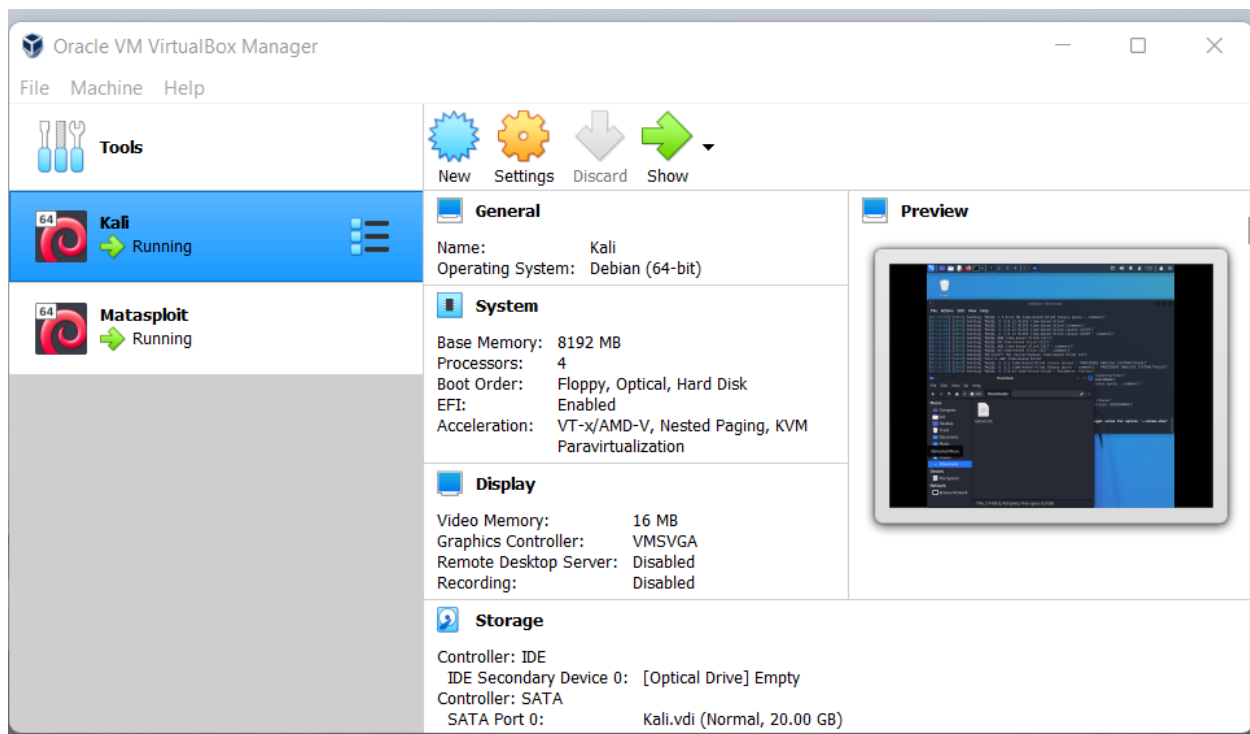


Applications (SS 1.1)

Step 2:

Follow the given steps in order: ([SS 2.1](#))

1. Install Oracle VM Virtual Box
2. Install the Kali Linux via VM Virtual Box.
3. Install Metasploitable 2 via VM Virtual Box



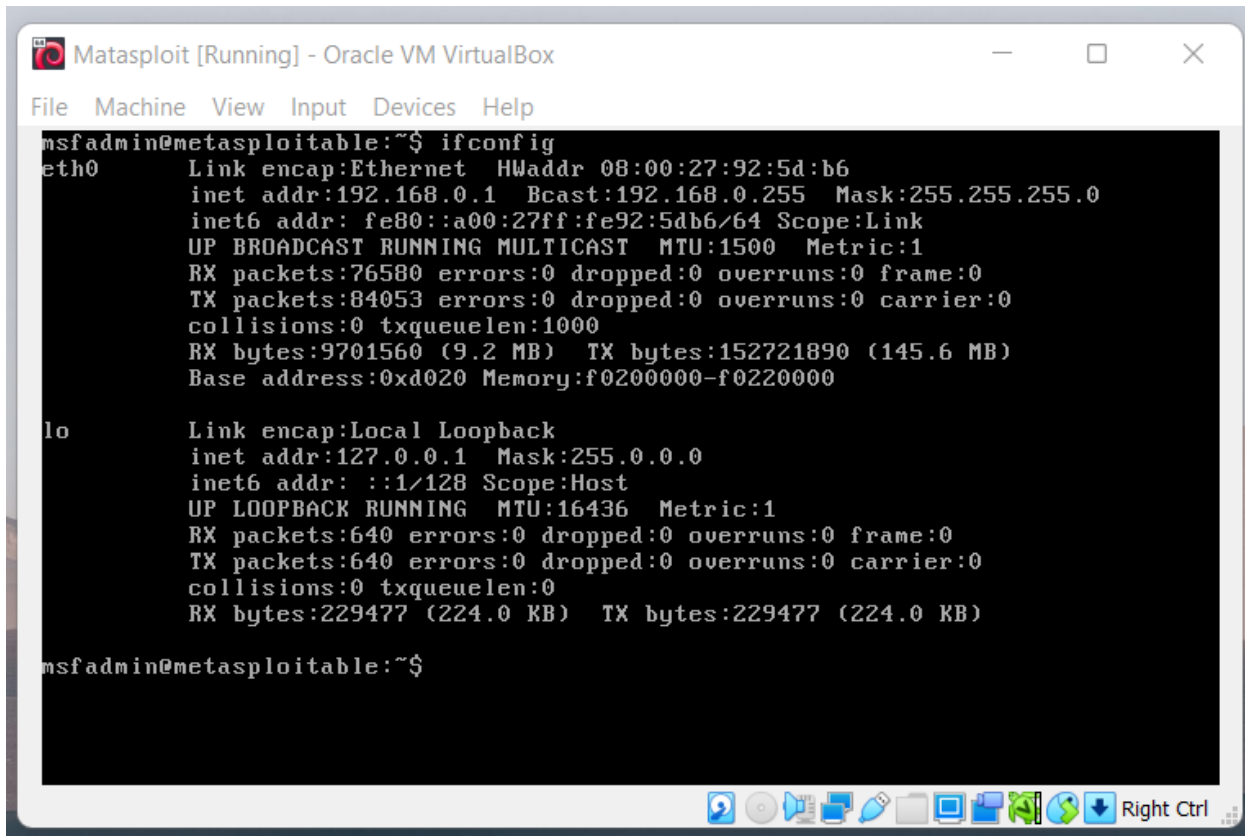
Virtual Machine Oracle (SS 2.1)

Note: (For Both Kali and Metasploit) Go to Settings → Network → Adapter 1 and set Attached to Host-only Adapter so both Kali and Metasploit will run on the same ip net so that they can communicate with each other.

Step 3:

Run the Metasploit 2 and perform the following tasks:

1. Login via default username and password i.e msfadmin
2. Change the ip with the following command.
Command: sudo ifconfig eth0 "your ip" netmask "your mask"
3. Type ifconfig to check the ip.



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:92:5d:b6
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe92:5db6/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:76580 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84053 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9701560 (9.2 MB)  TX bytes:152721890 (145.6 MB)
          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:640 errors:0 dropped:0 overruns:0 frame:0
          TX packets:640 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:229477 (224.0 KB)  TX bytes:229477 (224.0 KB)

msfadmin@metasploitable:~$
```

Step 4:

Run the Kali Linux and perform the following tasks:

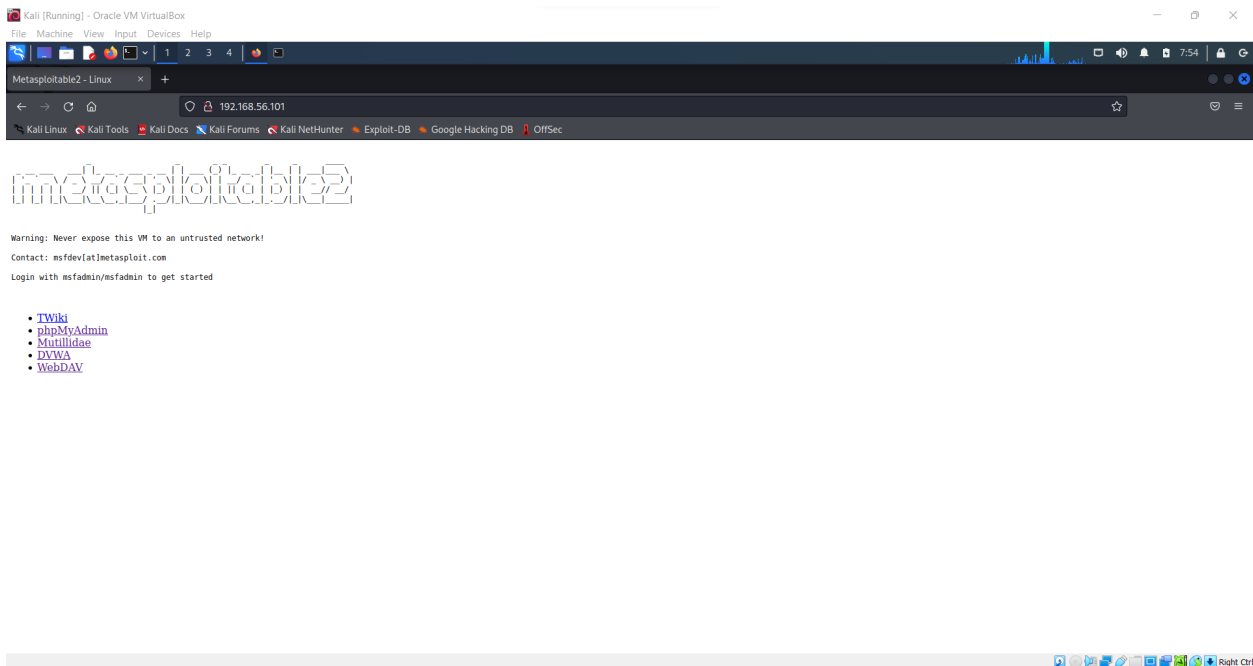
1. Ping the Metasploit in order to check if there is communication between Kali Linux and Metasploit or not. [\(SS 4.1\)](#)
Command: ping "Metasploit ip"
2. Open the browser and type the Metasploit's ip. [\(SS 4.2\)](#)
3. After seeing Metasploit on the browser go to Mutillidae → OWASP → A1 - Injection → SQLi - Extract Data → User Info.
4. This will redirect you to the login page. [\(SS 4.3\)](#)
5. Before Login, run BurpSuite.
6. In BurpSuite, go to the proxy section and after that go to your user login page again and login with a random name and password.
7. When you click, get account details, BurpSuite will automatically start to capture HTTP requests and will show you. [\(SS 4.4\)](#)
8. After getting an HTTP request, save the result in any folder for later use.

```
kali@kali: ~/Downloads
File Actions Edit View Help

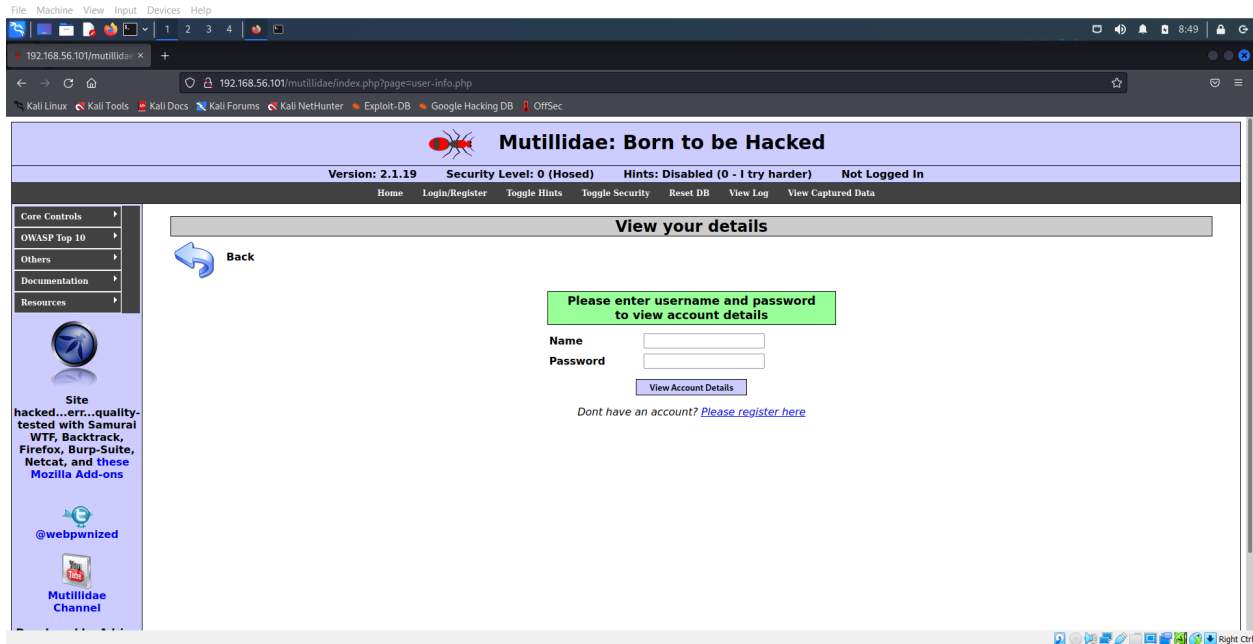
(kali@kali)-[~/Downloads]
$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=2.35 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=1.44 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=1.43 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=1.20 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=1.85 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=1.48 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=1.41 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=1.04 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=1.36 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=64 time=1.52 ms
^C
— 192.168.56.101 ping statistics —
10 packets transmitted, 10 received, 0% packet loss, time 9032ms
rtt min/avg/max/mdev = 1.036/1.505/2.345/0.343 ms

(kali@kali)-[~/Downloads]
$
```

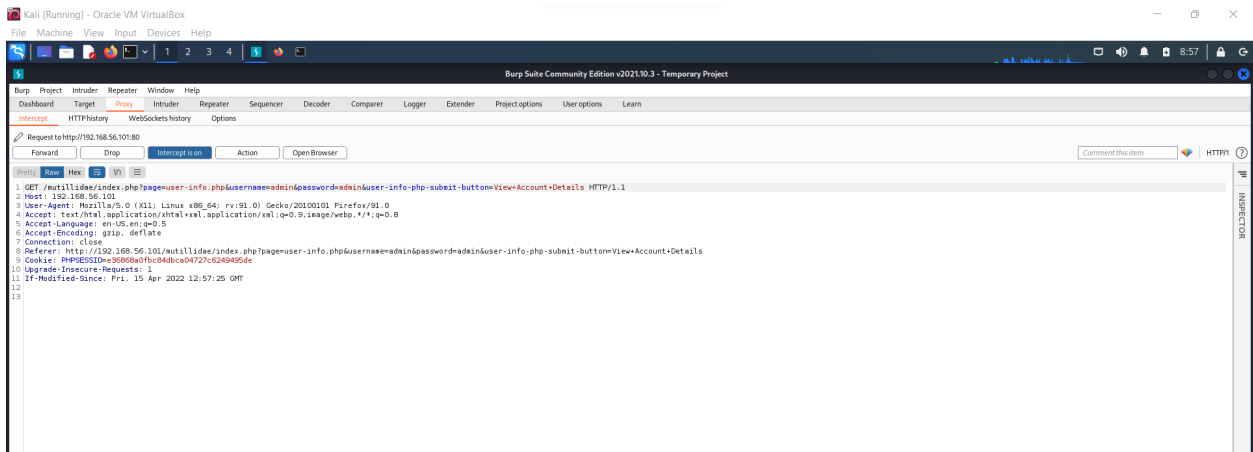
Ping - (SS 4.1)



Metasploitable 2 - (SS 4.2)



Metasploitable 2 - (SS 4.3)



BurpSuite - (SS 4.4)

Step 5:

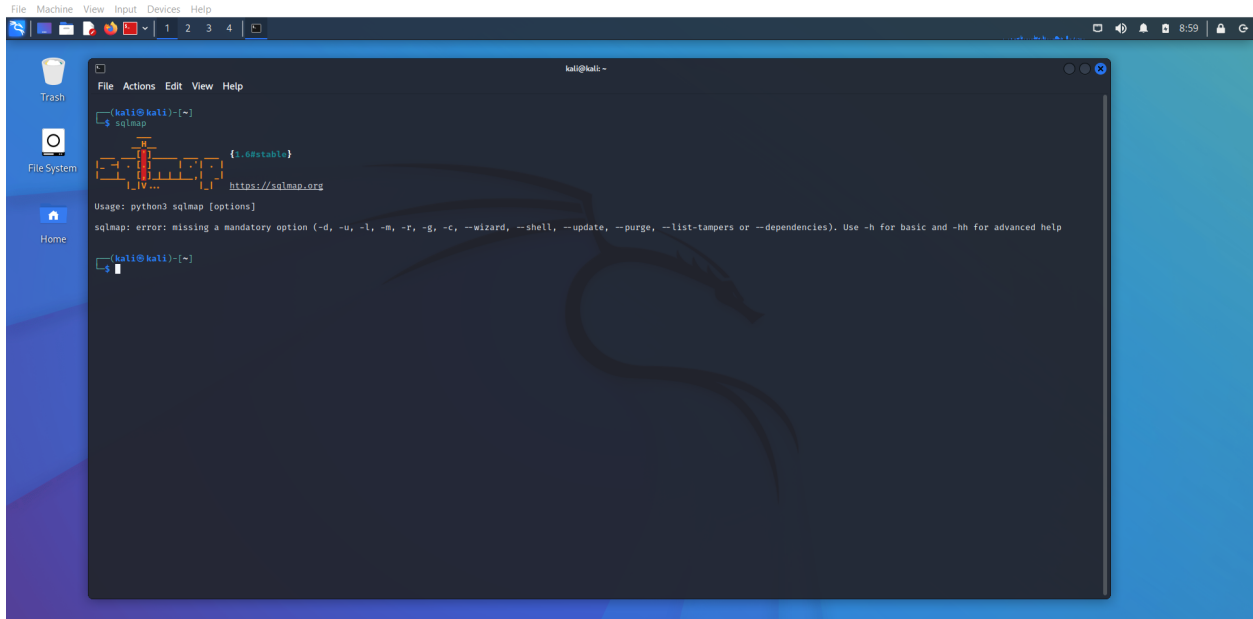
After saving the request perform the following operations:

1. Open the terminal and type sqlmap and press enter. (SS 5.1)
2. Sqlmap can be used to perform different types of sql attacks.
3. Type the command to fetch the details
Command: sqlmap -r "your save file location" -dbs
4. This will show you all the details of the database including its tables.
5. In order to fetch tables type the following command. (SS 5.2)
Command: sqlmap -r "your save file location" -D "table name" -tables
6. In order to fetch the details from the tables type the following command.

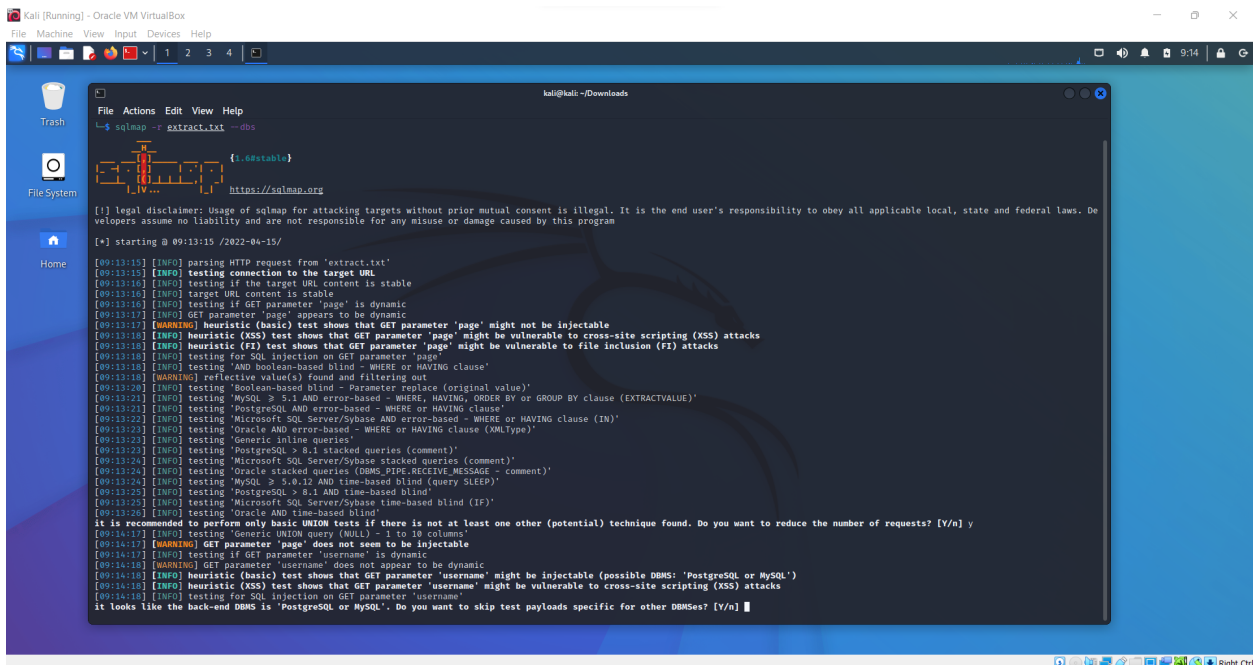
Command: sqlmap -r "file location" -D "table name" -T "table name" --dump

7. The below command will simply dump the data of the particular table.

Command: sqlmap -r "file location" --dump -D "database" -T "table"



Sqlmap (SS 5.1)



Sqlmap (SS 5.2)