**Assignment 1**

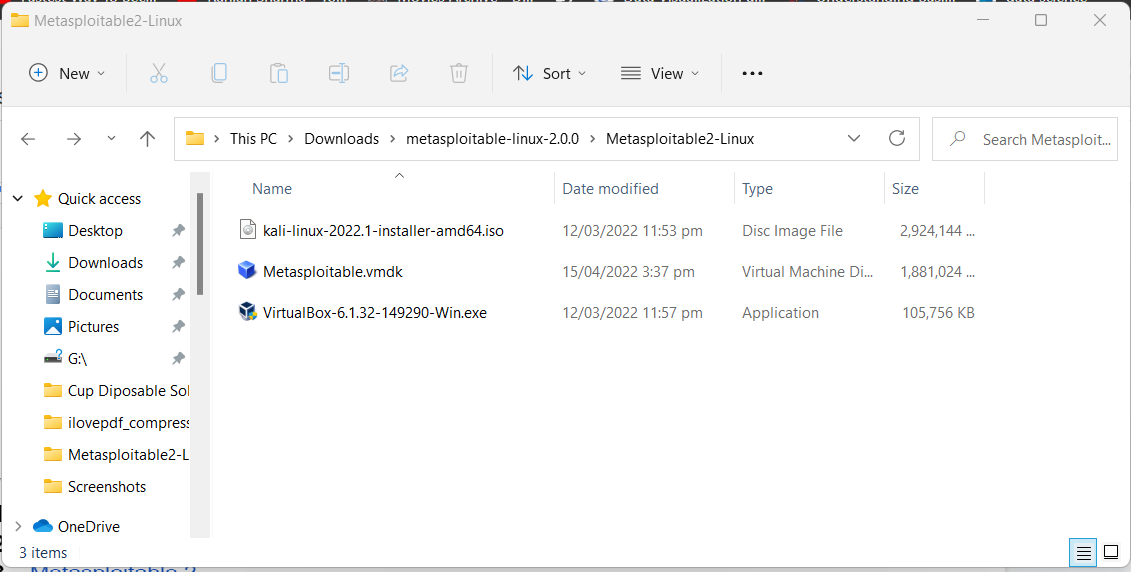
Muhammad Waleed

22-11081

**Step 1:**

Download the following things: **(Screenshot 1.1)**

1. [Oracle VM Virtual Box.](https://www.oracle.com/pk/database/technologies/oracle-database-software-downloads.html)
2. [Kali Linux iso image file.](https://www.kali.org/docs/introduction/download-official-kali-linux-images/)
3. [Metasploitable 2](https://sourceforge.net/projects/metasploitable/files/Metasploitable2/).

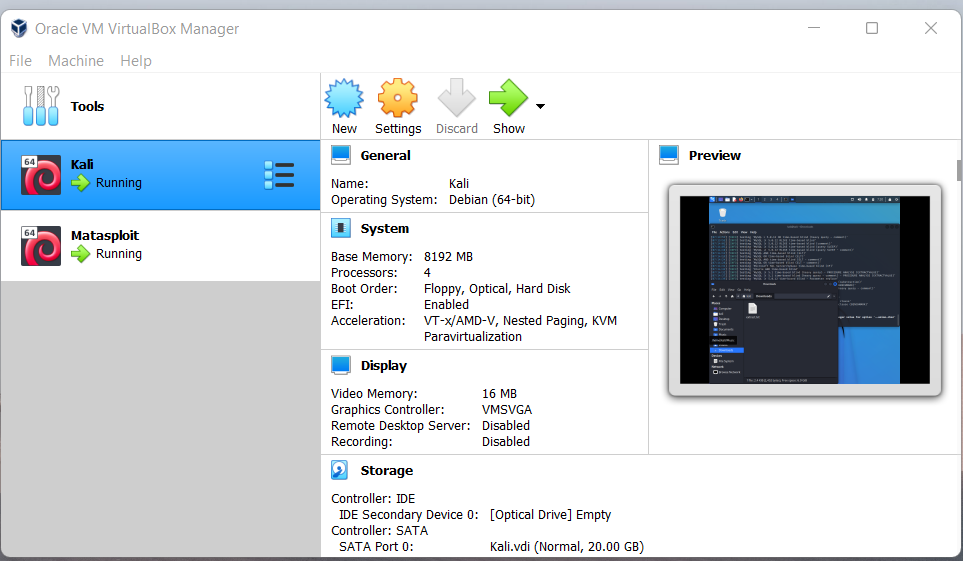


**Applications (SS 1.1)**

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

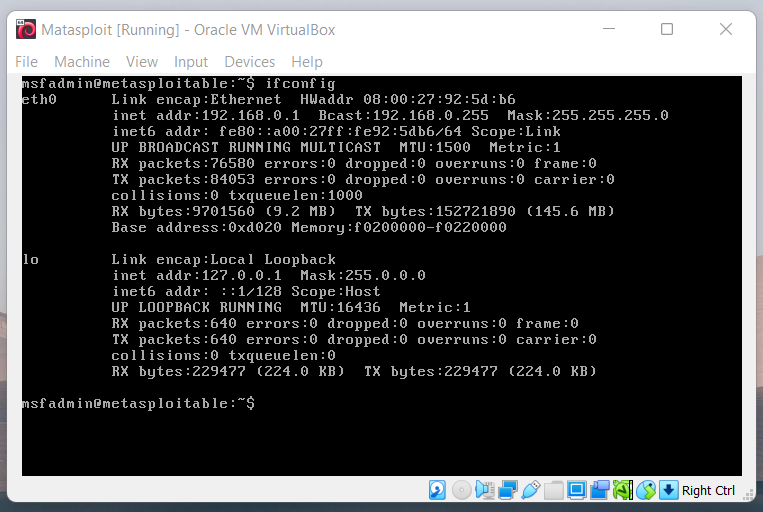
**Step 3:**

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”**

1. Type ifconfig to check the ip.



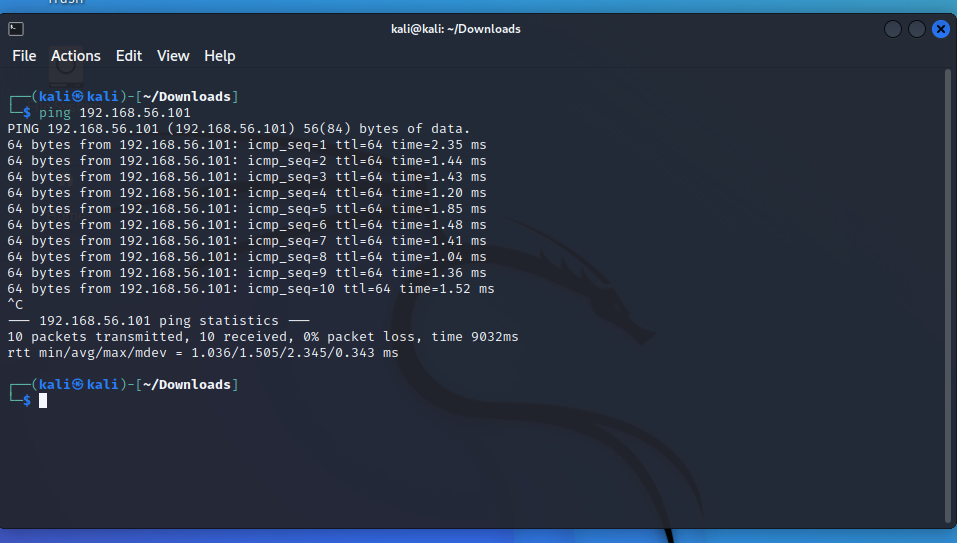
**Step 4:**

Run the Kali Linux and perform the following tasks:

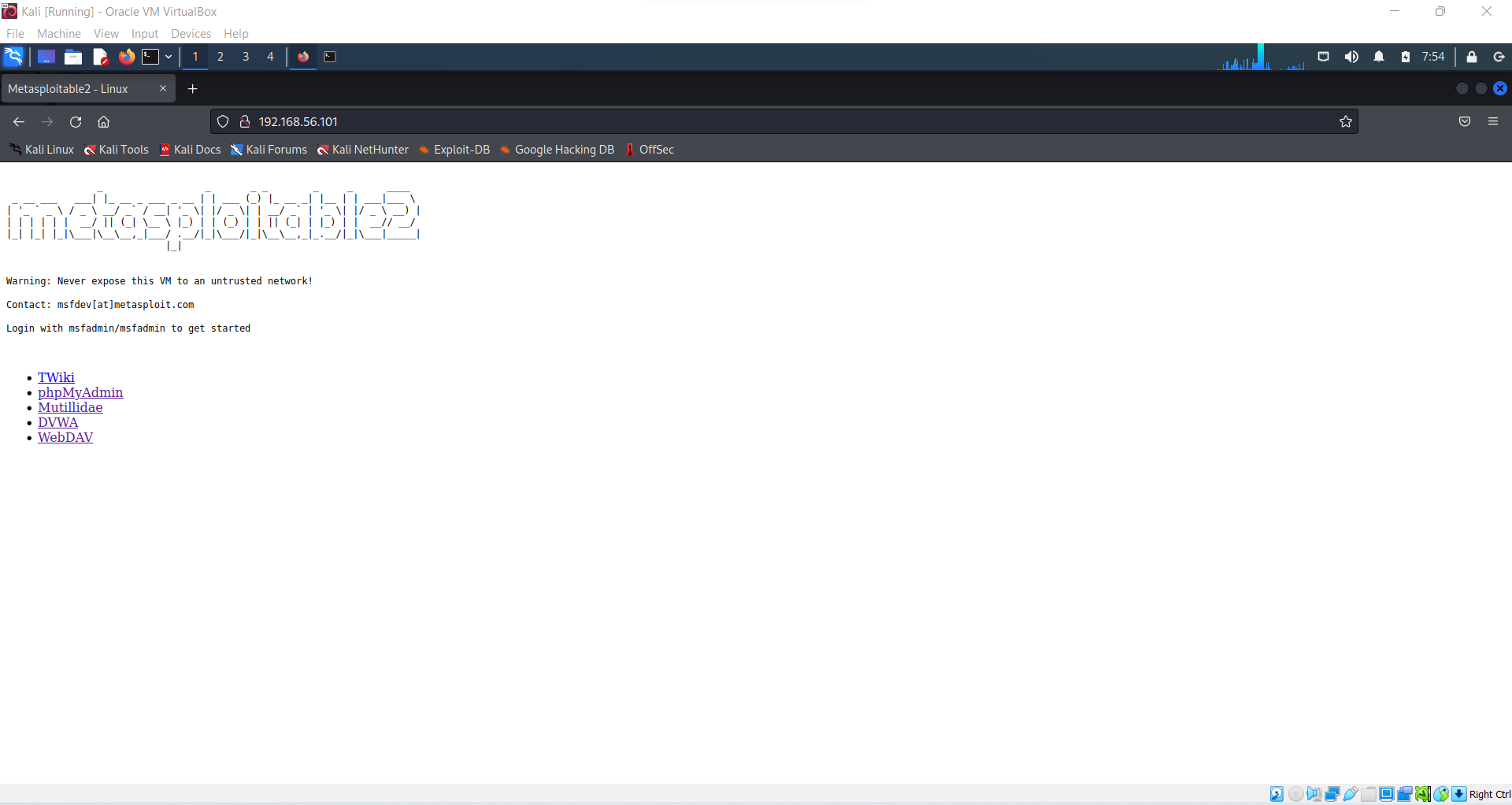
1. Ping the Metasploit in order to check if there is communication between Kali Linux and Metasploit or not. **(SS 4.1)**

**Command: ping “Metasploit ip”**

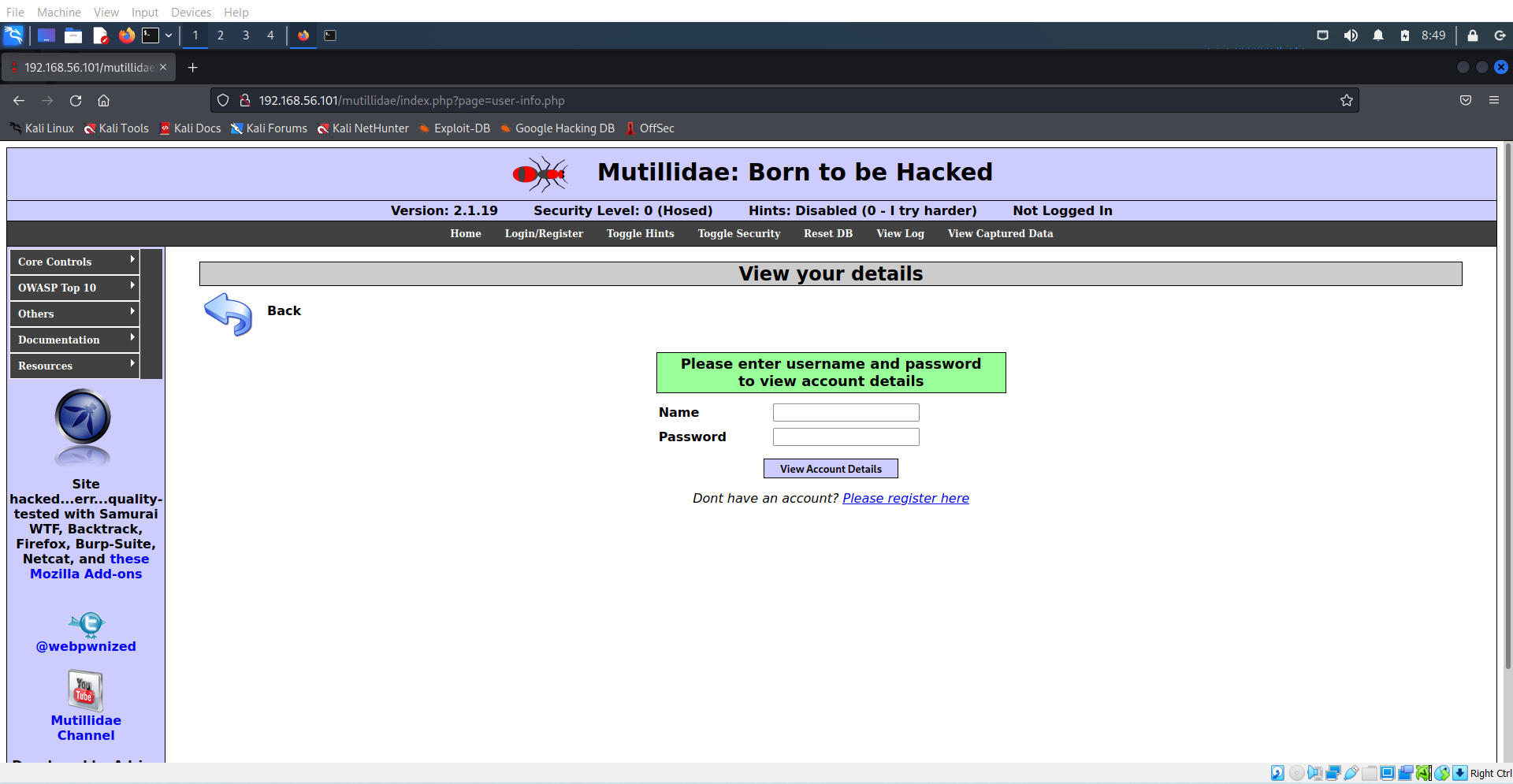
1. Open the browser and type the Metasploit’s ip. **(SS 4.2)**
2. After seeing Metasploit on the browser go to Mutillidae → OWASP → A1 - Injection → SQLi - Extract Data → User Info.
3. This will redirect you to the login page. **(SS 4.3)**
4. Before Login, run BurpSuite.
5. In BurpSuite, go to the proxy section and after that go to your user login page again and login with a random name and password.
6. When you click, get account details, BurpSuite will automatically start to capture HTTP requests and will show you. **(SS 4.4)**
7. After getting an HTTP request, save the result in any folder for later use.



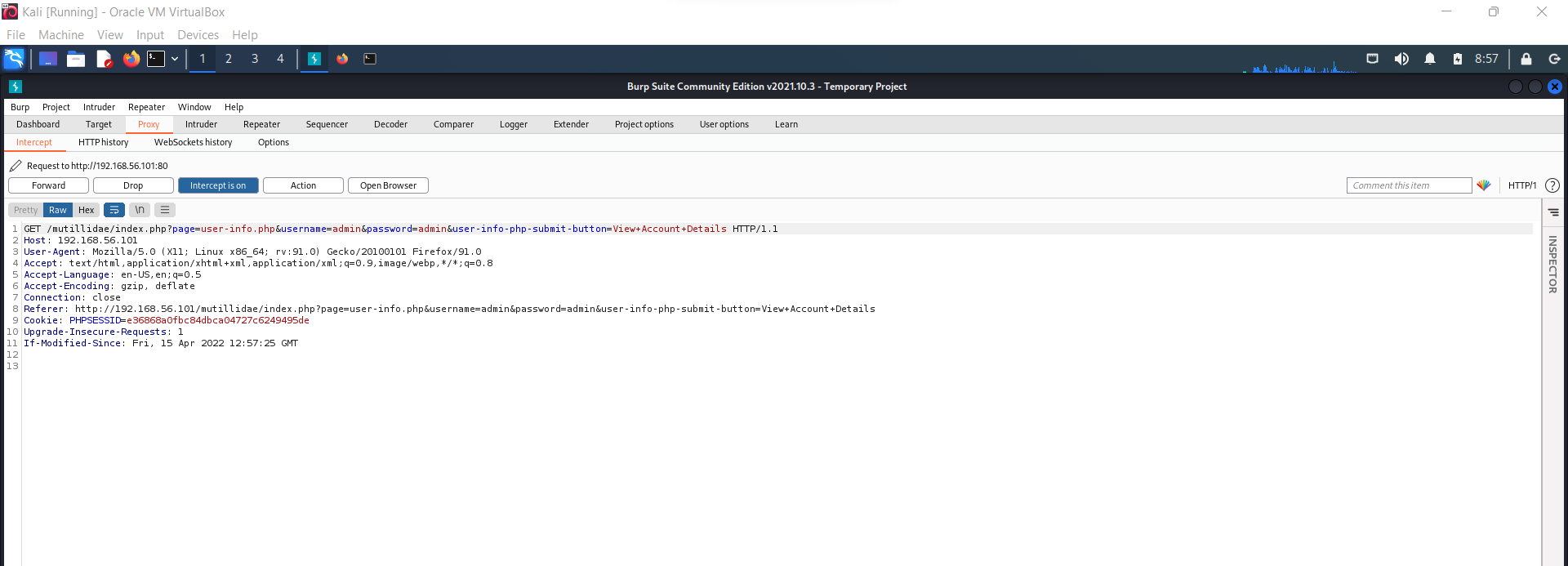
**Ping - (SS 4.1)**



**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

1. This will show you all the details of the database including its tables.
2. In order to fetch tables type the following command. **(SS 5.2)**

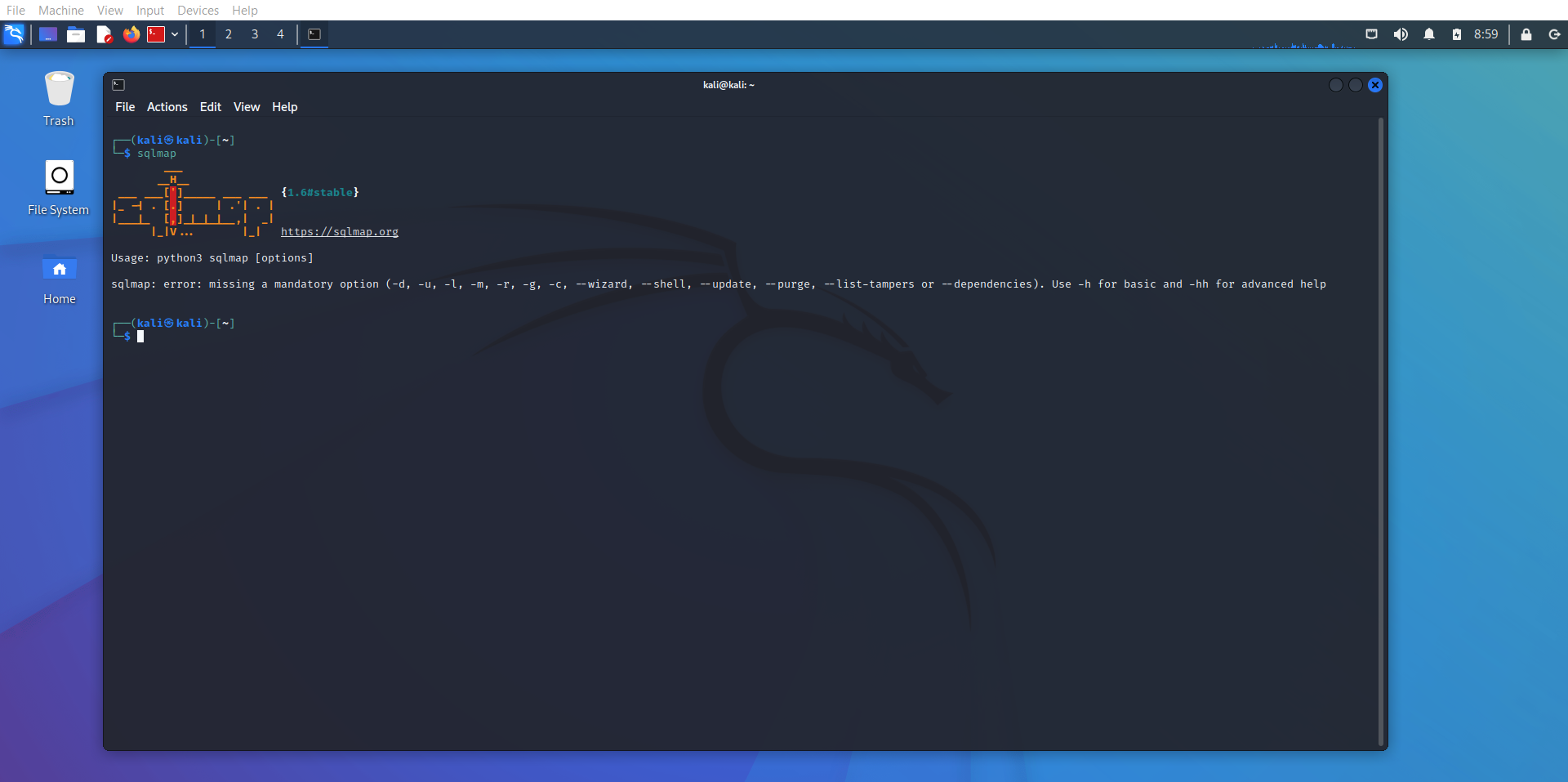
**Command: sqlmap -r “your save file location” -D “table name” –tables**

1. In order to fetch the details from the tables type the following command.

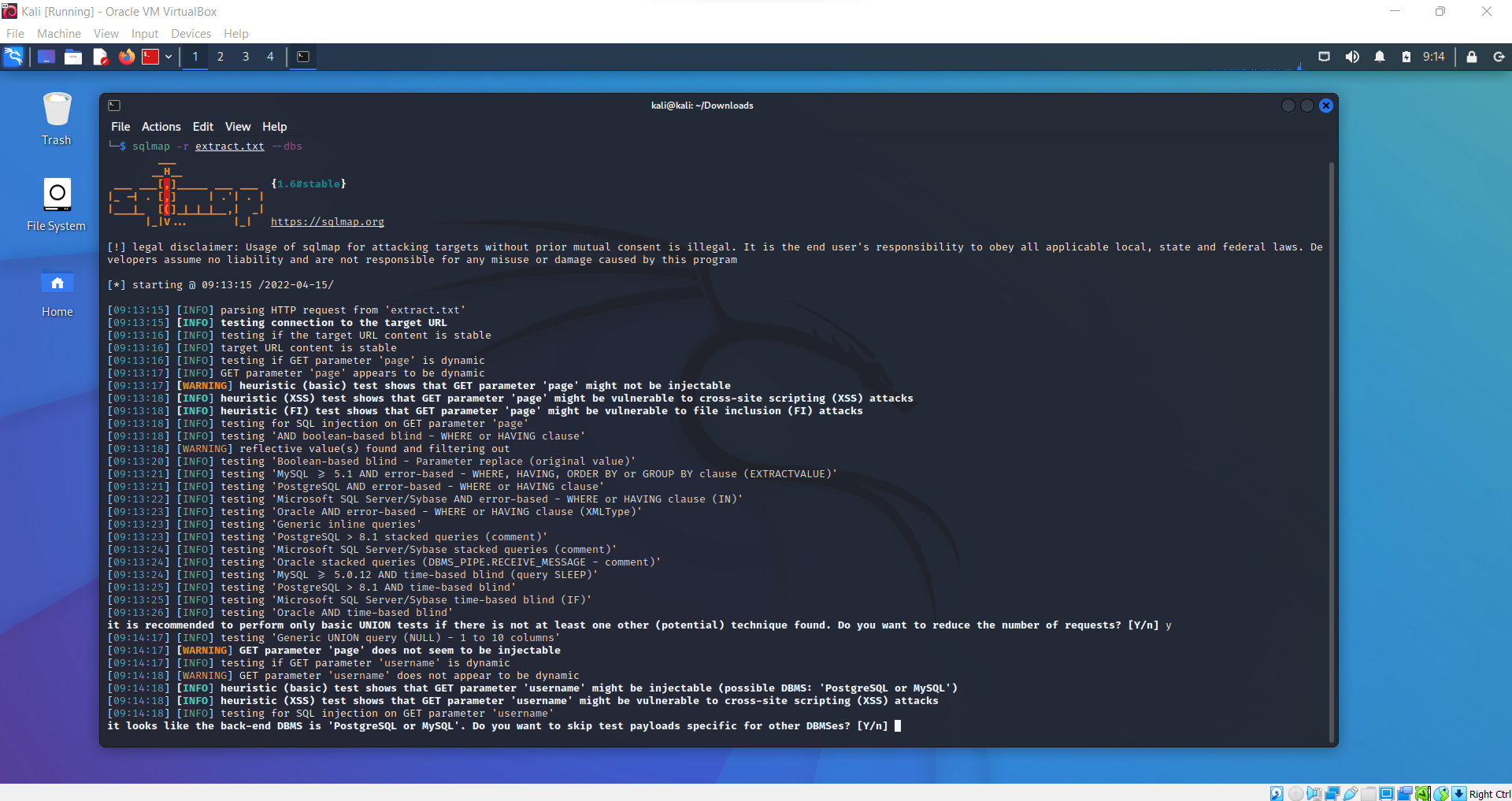
**Command: sqlmap -r “file location” -D “table name” –T “table name” –dump**

1. 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)**