

Spring 2021 COMP421: Information Security

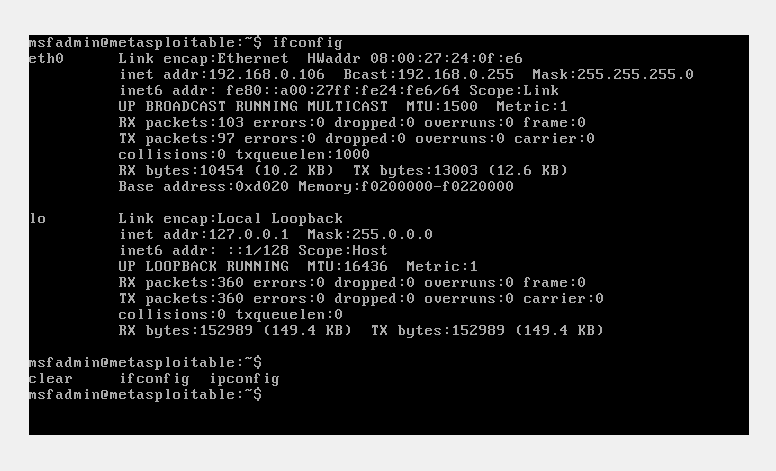
Assignment #1

**Name:** HUMZA WAQAR

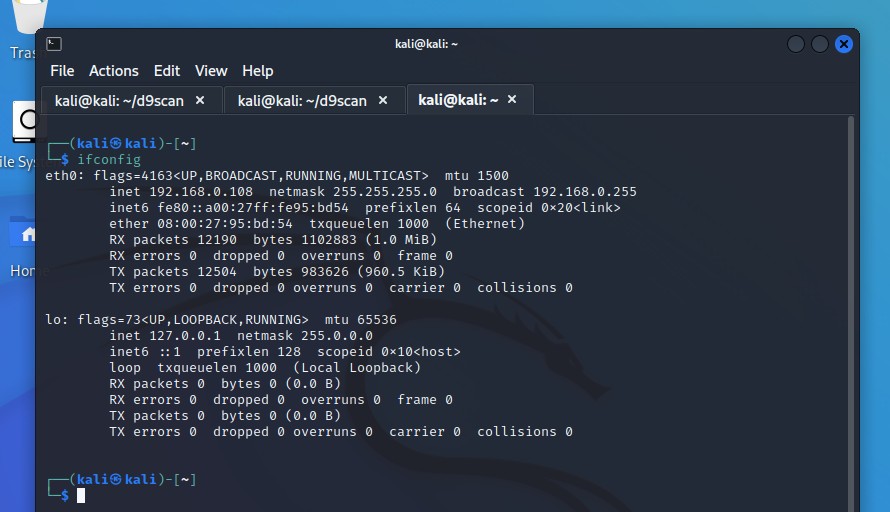
**Student ID:** 22-10440

# Setting up the environment:

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



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

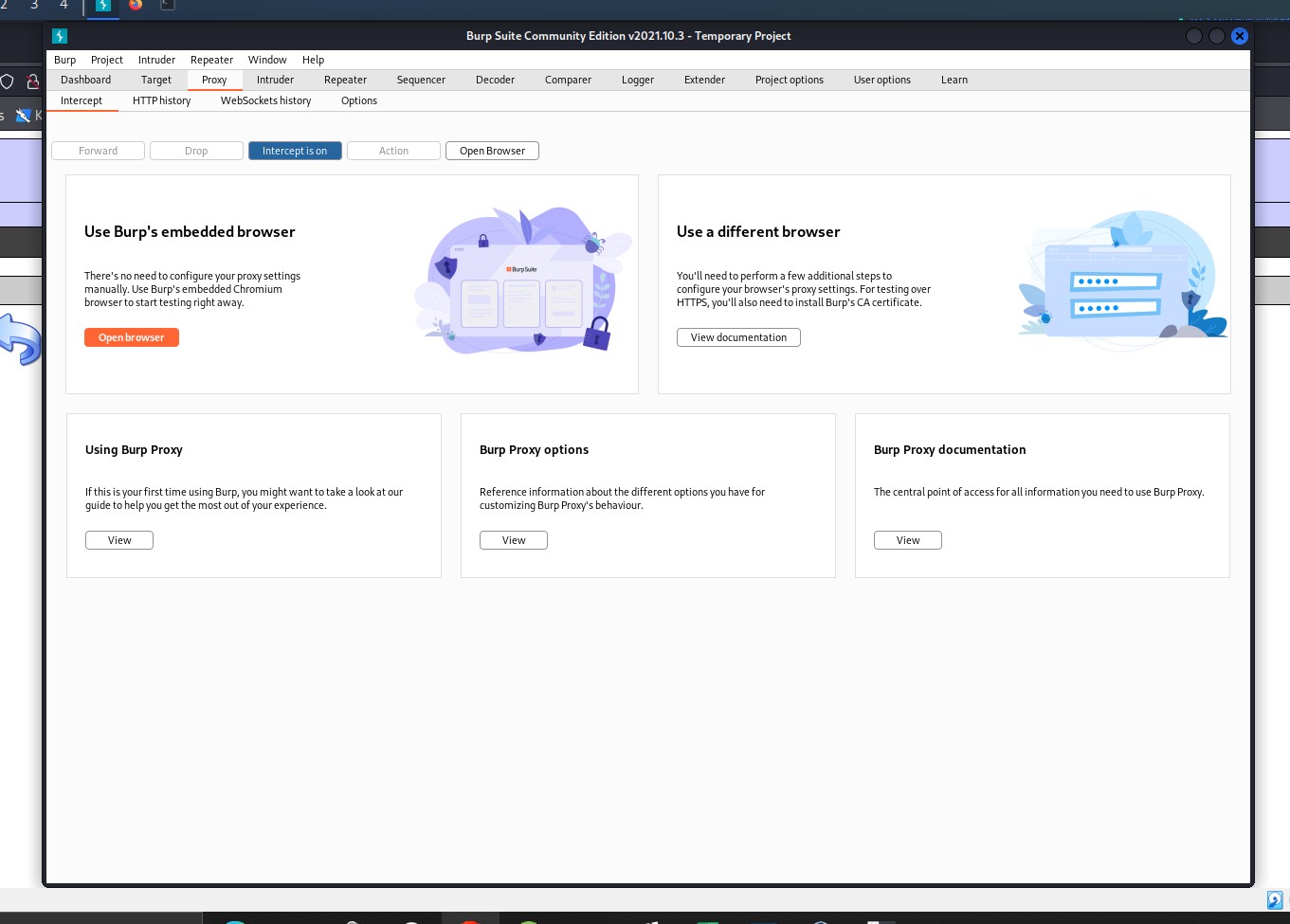


# Steps to perform the attack:

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.