**Name: Hamza Khan**

**Roll Number: 22-10208**

**Course: COMP 421**

**Section: A**

**Instructor: Dr. Saad Saleem**

Step1: I downloaded and installed metasploitable2.

Step2: I used the command “ifconfig” to see the IP address assigned to metasploitable2.

Step3: I launched kali and using terminal I used the “ifconfig” command to see the INET address and the netmask.

Step4: In metasploitable2, I used the command “sudo ifconfig eth0 192.168.1.2 netmask[same as kali]”.

Step5: I used the command “ifconfig” to see if the ip address and netmask are assigned properly.

Step6: I came back to kali and used the “ping” command along with the IP address assigned to metasploitable2, to see if we can ping metasploitable2.

Step7: I entered the same ip address in the browser.

Step8: I selected “Mutillidae” from the options given.

Step9: From the options given, I selected “SQL injection🡪 extract data”.

Step10: I then launched “berpsuite” application that was already present in kali.

Step11: Berpsuite captures the request that we will use in SQL map to enumerate the database.

Step12: I used the option “proxy” from the given options. After setting it up with my browser settings, I was able to receive incoming HTTP requests coming from the brower.

Step13: The request was then captured by the Berpsuite application. I saved it into a text file for further scan of any exploitation.

Step14: Then I used SQL map.

Step15: Then I used the command “sqlmap -r /home/kali/Desktop/extract.txt –dbs” , it checks the database and see if there are any vulnerabilities.

Results:

[12:37:07] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (XSS) attacks

12:37:29] [WARNING] GET parameter 'page' does not seem to be injectable

[12:37:29] [WARNING] GET parameter 'username' does not appear to be dynamic

[WARNING] GET parameter 'username' does not seem to be injectable

[WARNING] GET parameter 'password' does not appear to be dynamic

[WARNING] GET parameter 'password' does not seem to be injectable

[WARNING] heuristic (basic) test shows that GET parameter 'user-info-php-submit-button' might not be injectable

[WARNING] GET parameter 'user-info-php-submit-button' does not seem to be injectable

[CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests.

Text

Description automatically generatedText

Description automatically generatedText

Description automatically generated

I couldn’t extract any data from the webserver, as it was not injectable.