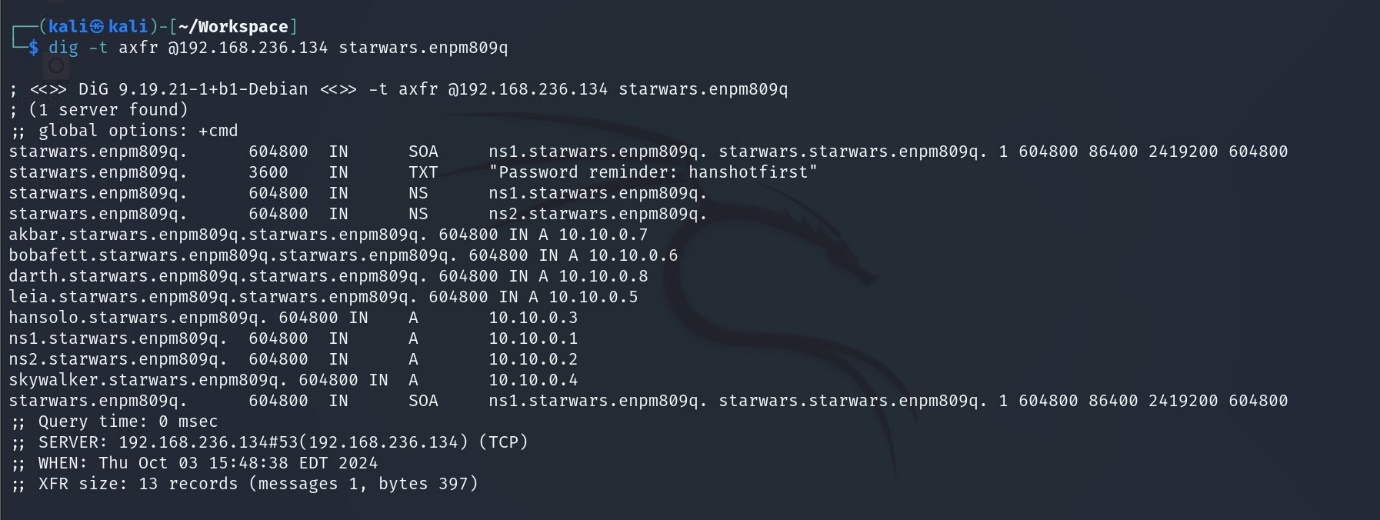
Name: Rithik Sarvesh Bharathiraja

UID: 120395246 (gbr\_2001)

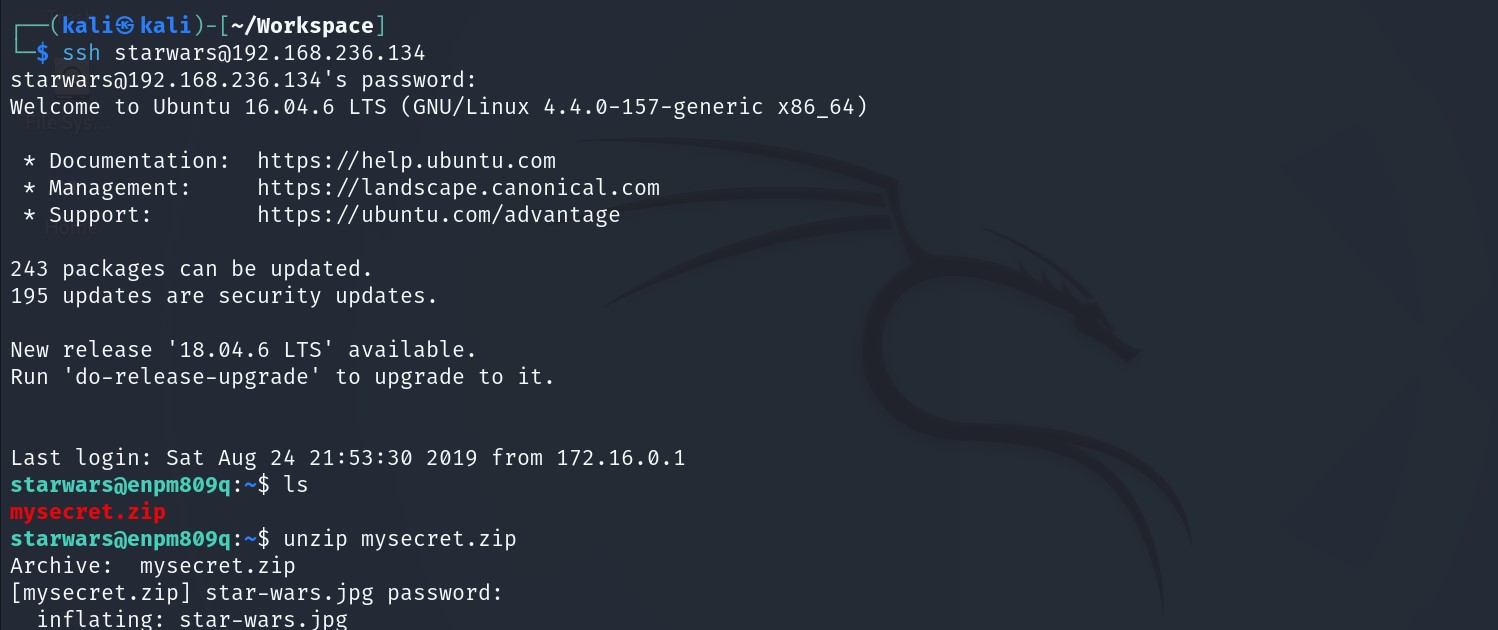
Course: ENPM634

Task: Homework 3

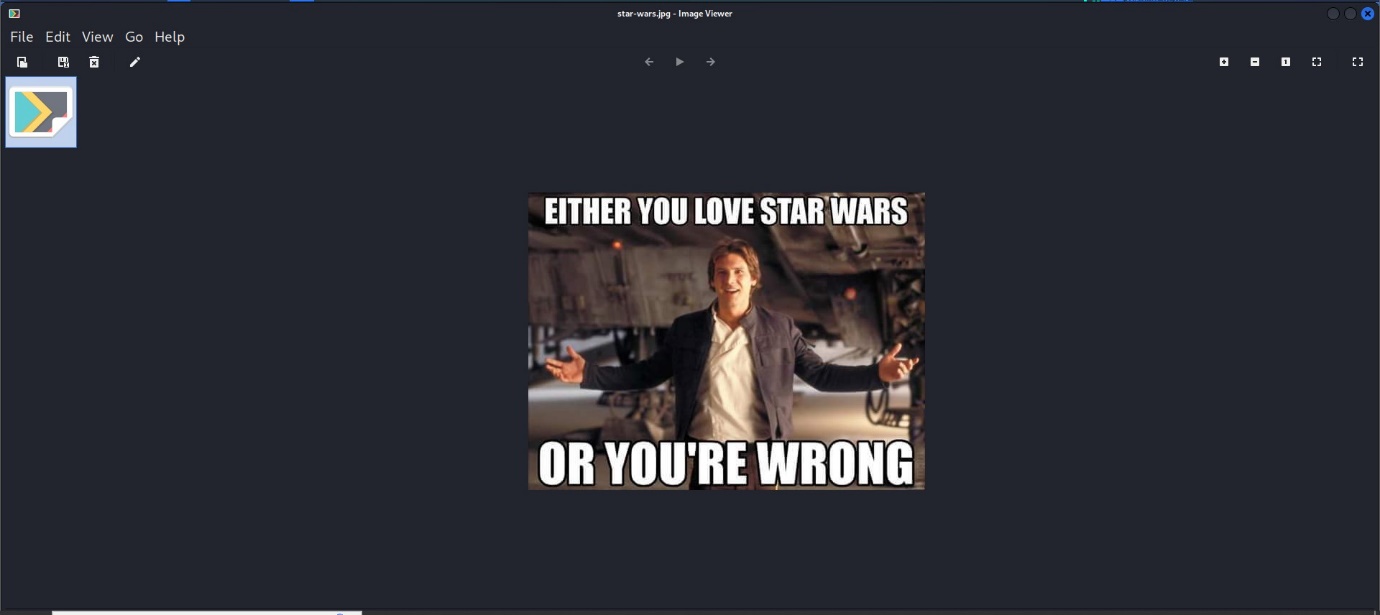
1. DiG command is used to get more DNS information about the DNS Zone starwars.enpm809q. In that, a password reminder is found mentioning “hanshotfirst”



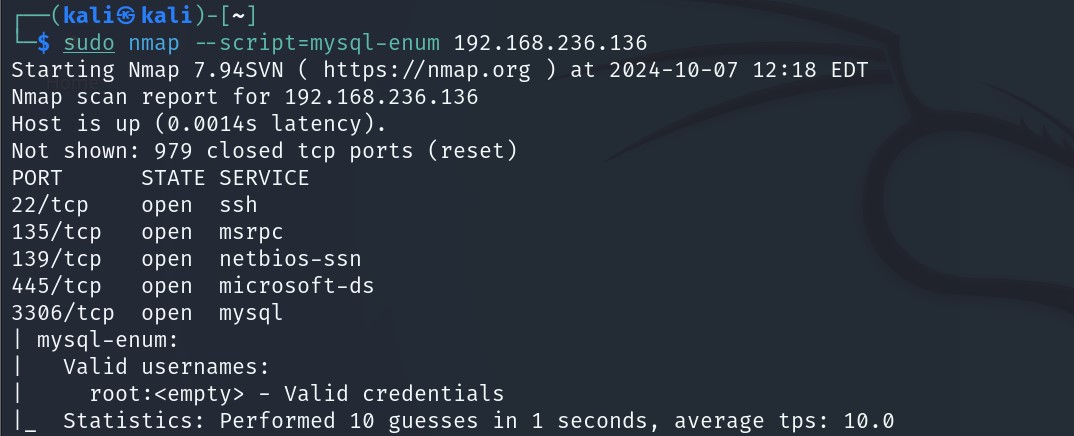
So, ssh is used to get access into the machine and the credentials worked. A zip file named mysecret.zip was found in the home directory. After unzipping it with the password “hanshotfirst”, an image file was found.



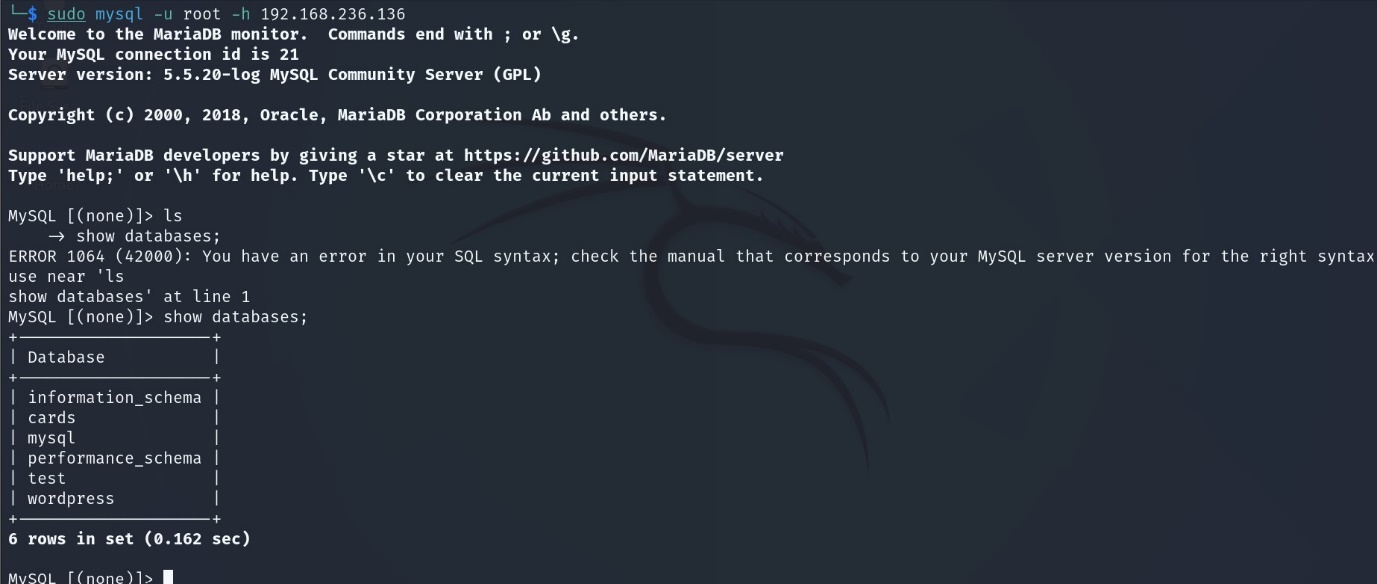
As like it was mentioned in the question, the image referred to the star wars. Thus flag1 is found.

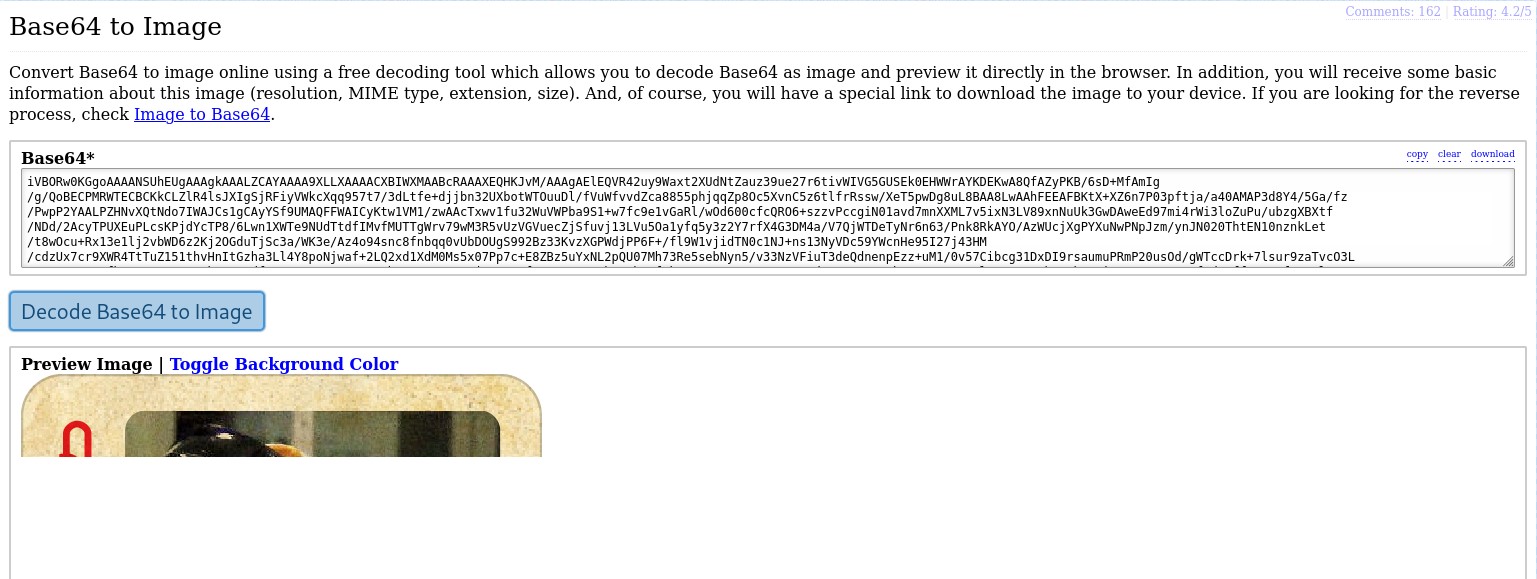


1. As mentioned in the question, mysql-enum script is used to enumerate the machine for mysql. Later, it was found that the mysql server was running with the default credentials(root:no password)



MySQL server connection is established through CLI. Inside the cards database, there was a table called queen\_of\_hearts. Content of the table was found to be encoded in BASE64. With the rest of the data, it could be assumed that it could be an image. Using an online website, BASE64 is converted into an image and the result was an corrupted picture of queen of hearts.

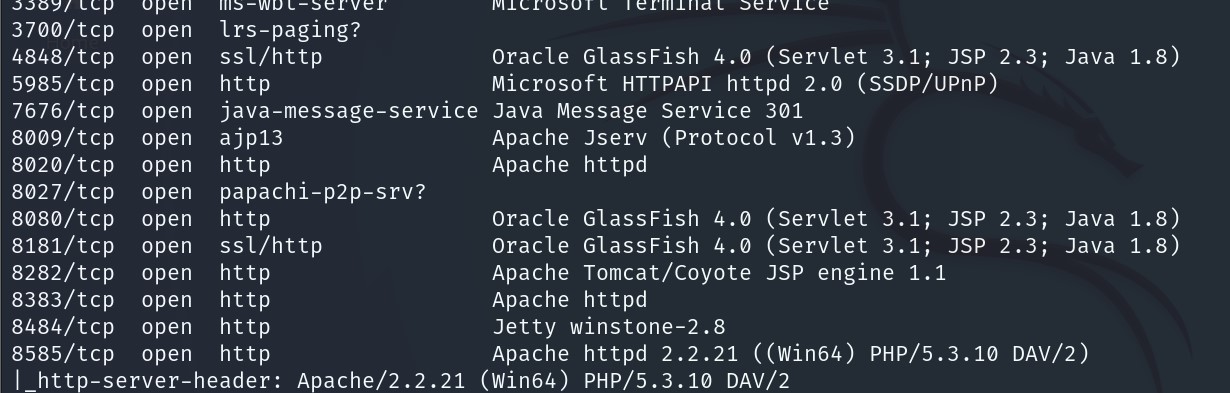




Below information is the metadata of the extracted image.



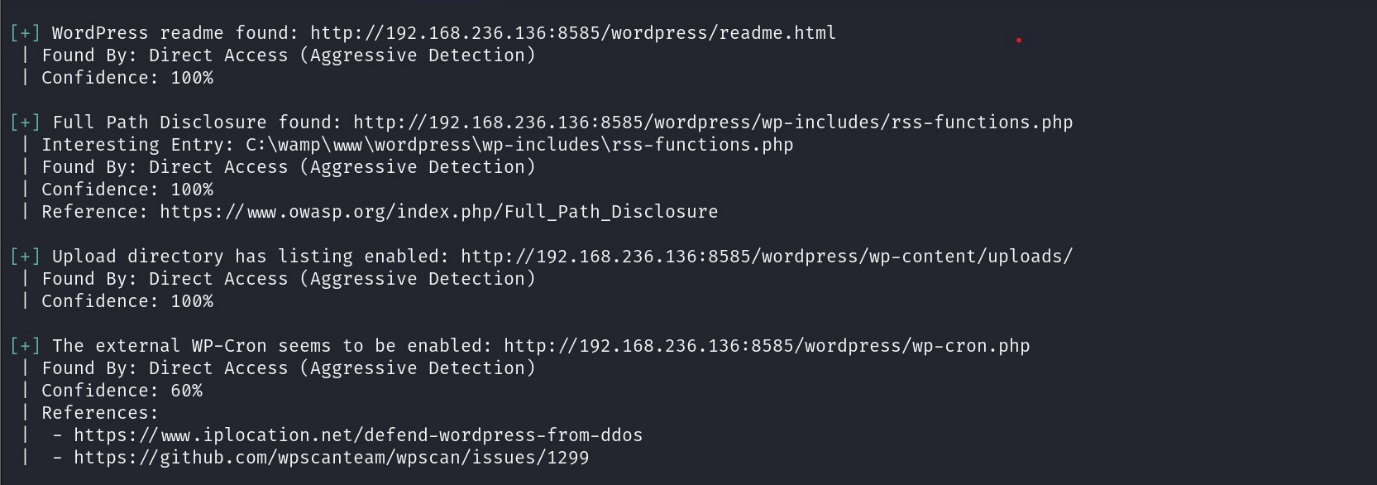
1. Nmap is used to find the open ports in the machine. At the end, it was found that wordpress was hosted on the port 8585 through Wamp server.



WPScan is used to get information about any vulnerabilties (plugins) present in the wordpress.

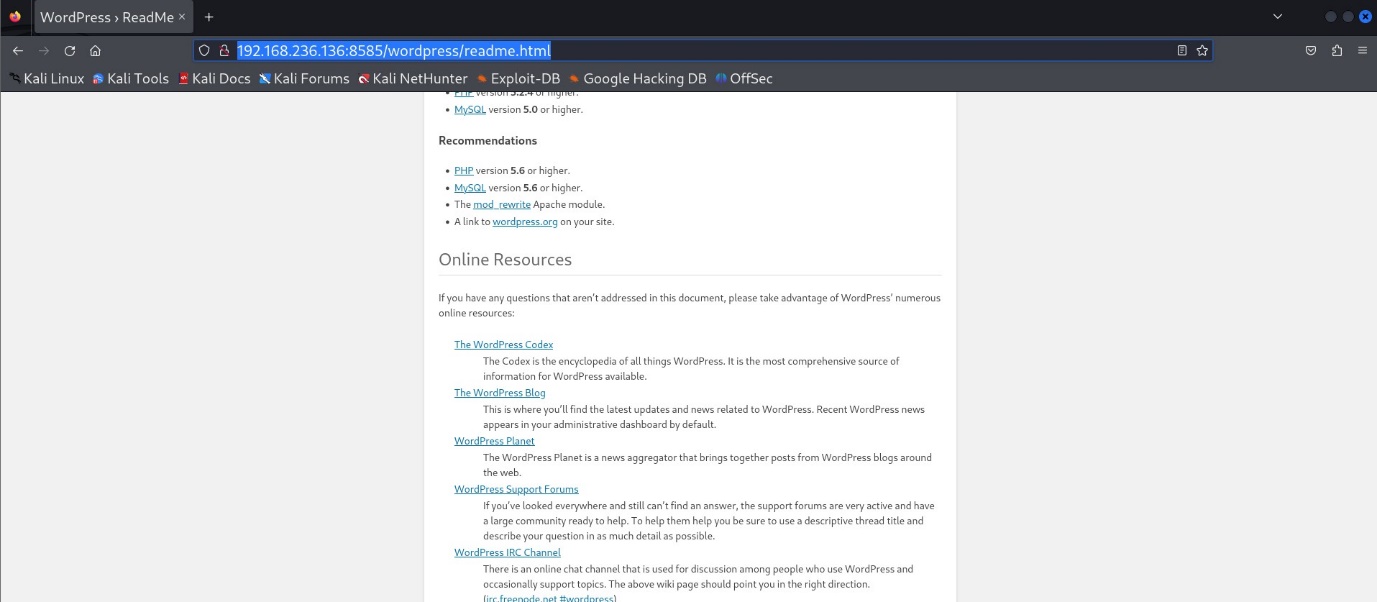


And, the result showed that there are many vulnerabilities in it already.





To verify, we used the vulnerable URL found by the WPScan and readme was available to the public.



As part of the enumeration, in the MySQL server, there was a database called ‘wordpress’. In that, wp\_users table was found with the information which could give unauthorized access to the machine.

