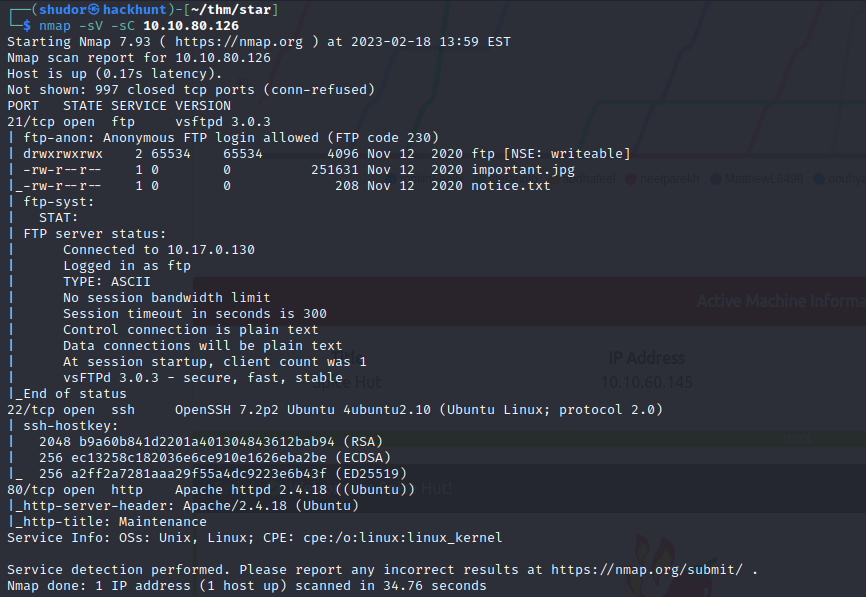
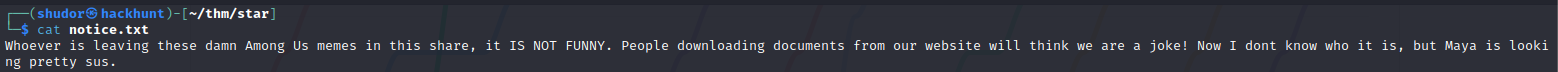
Nmap scan



We have three ports open, FTP running on port 21, SSH running on port 22 and Apache web server running on port 80. We can also see that FTP has anonymous login enabled so let's enumerate it first.

Graphical user interface, text

Description automatically generated



I tried extracting data from the image using exiftool and binwalk but it did not contain any useful information. So we start looking in the webpage.

Text

Description automatically generated

No information is found in the webpage so we start using gobuster

Text

Description automatically generated

There is a directory named files which contains the same content as the FTP

Graphical user interface, text, application

Description automatically generated

Trying to upload reverse shell in the file directory

Graphical user interface

Description automatically generated with medium confidence

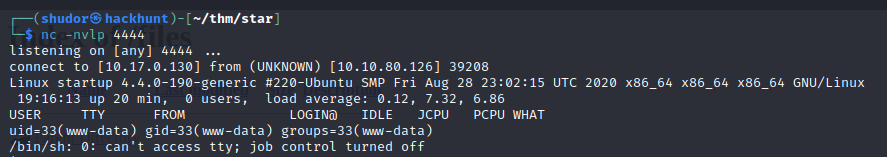
Reverse shell is uploaded

Before running the reverse shell in webpage we will run the netcat listner

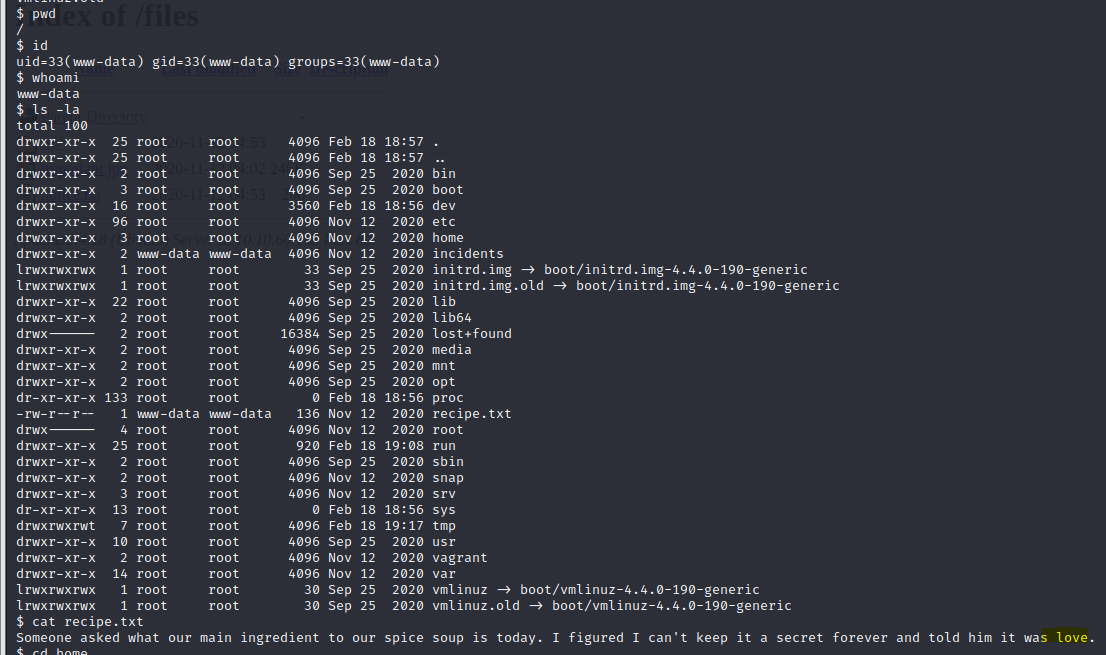
Text

Description automatically generated

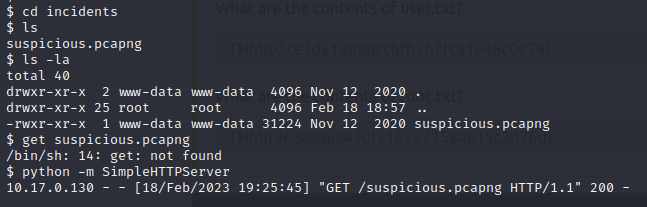
After running the php reverse shell, we will get a reverse shell back into our system.



What is the secret spicy soup recipe?



Inside the incidents directory, we have a file named suspicious.pcapng. I downloaded this file on my computer and opened it with ettercap.



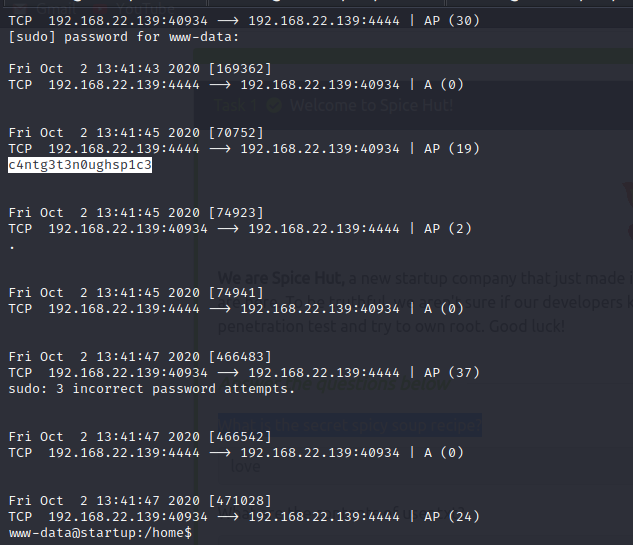
A screenshot of a computer

Description automatically generated with medium confidence

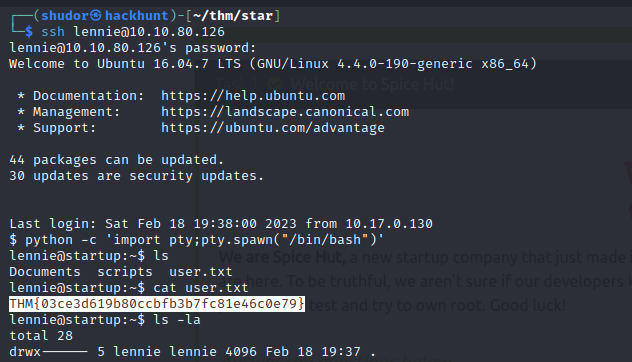
Text

Description automatically generated

I got the password for Lennie



With help of this I am able to login in Lennie profile and got the user.txt



What are the contents of root.txt

