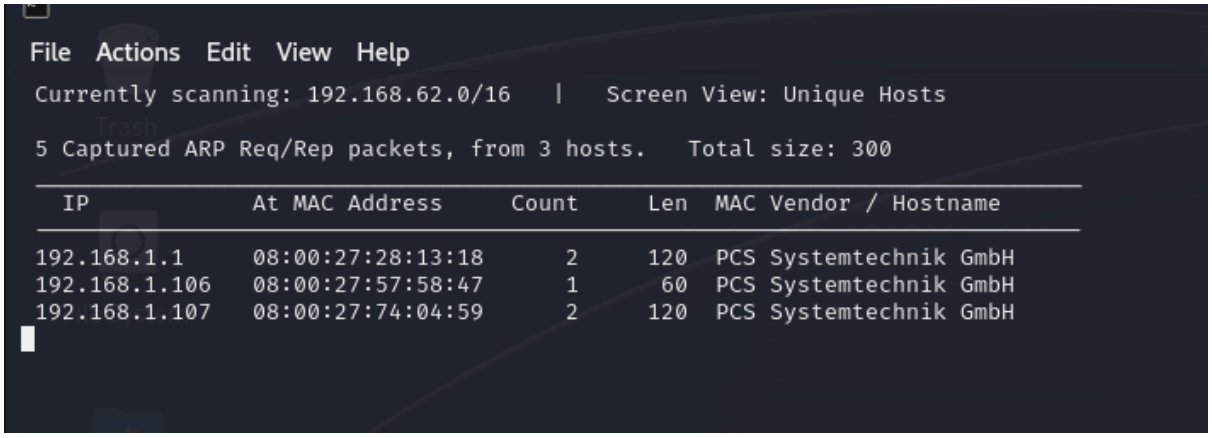
Ethical Hacking Practice #2: Mercury Writeup

Clay Jones

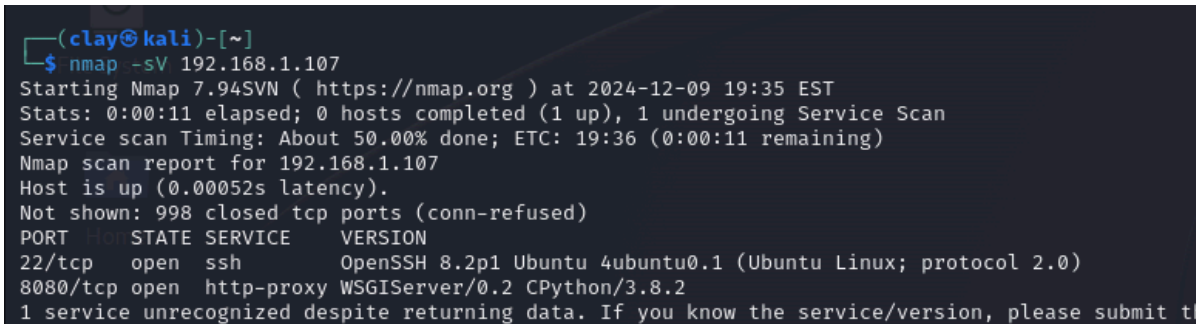
Objective:
Get the credentials to both accounts on the machine.

Step 1:



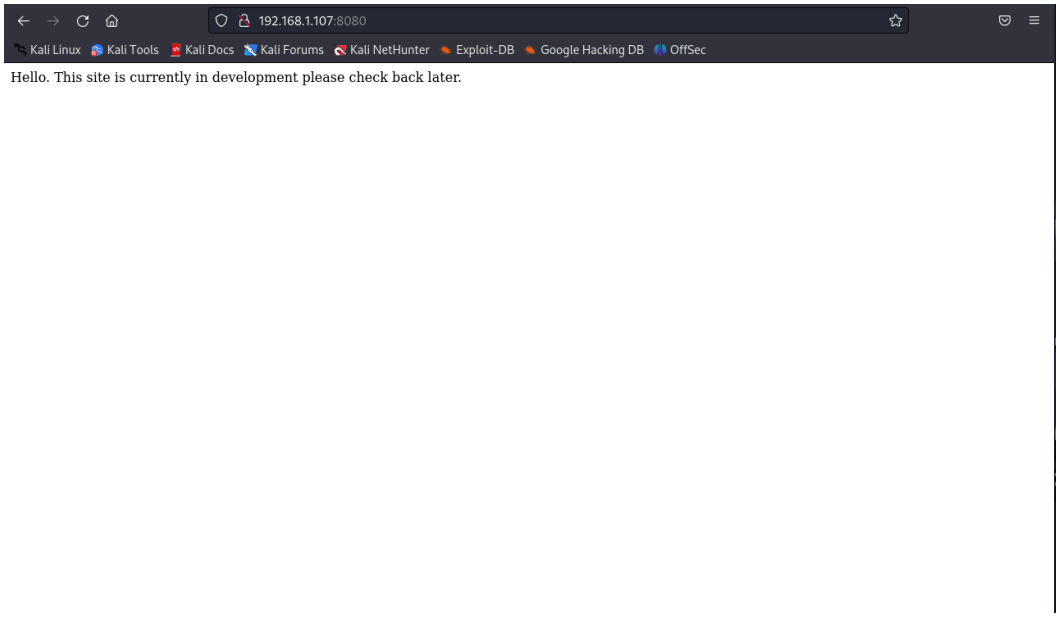
First, I needed to identify the IP address of the machine.

Step 2:



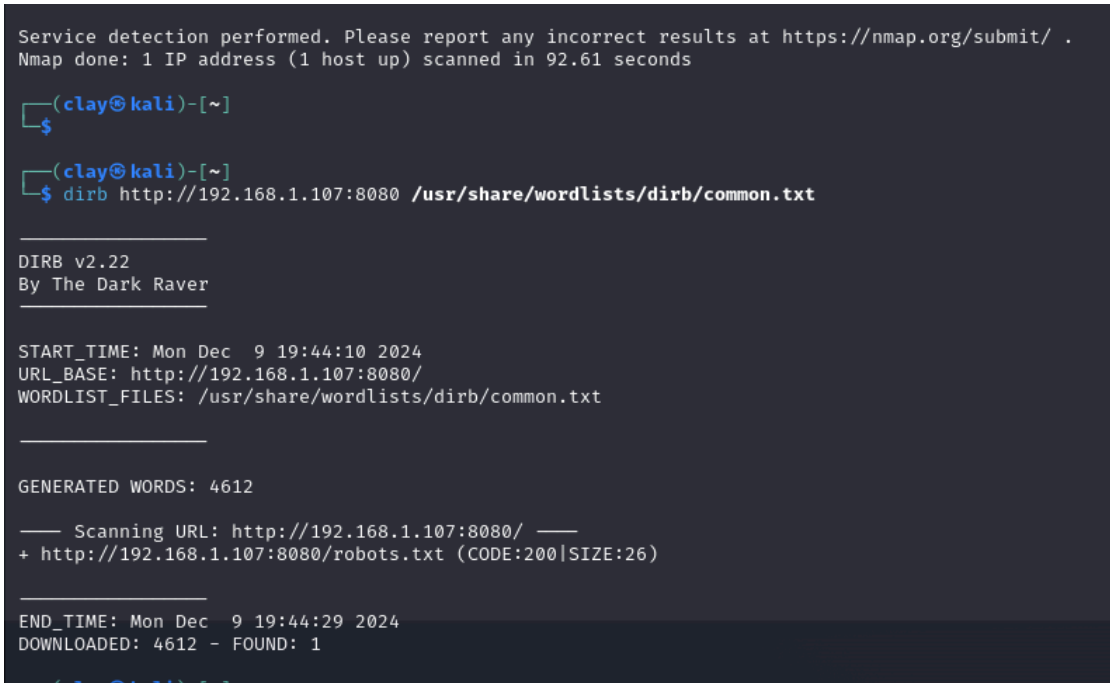
I conducted a service scan on the IP to see the open ports.

Step 3:



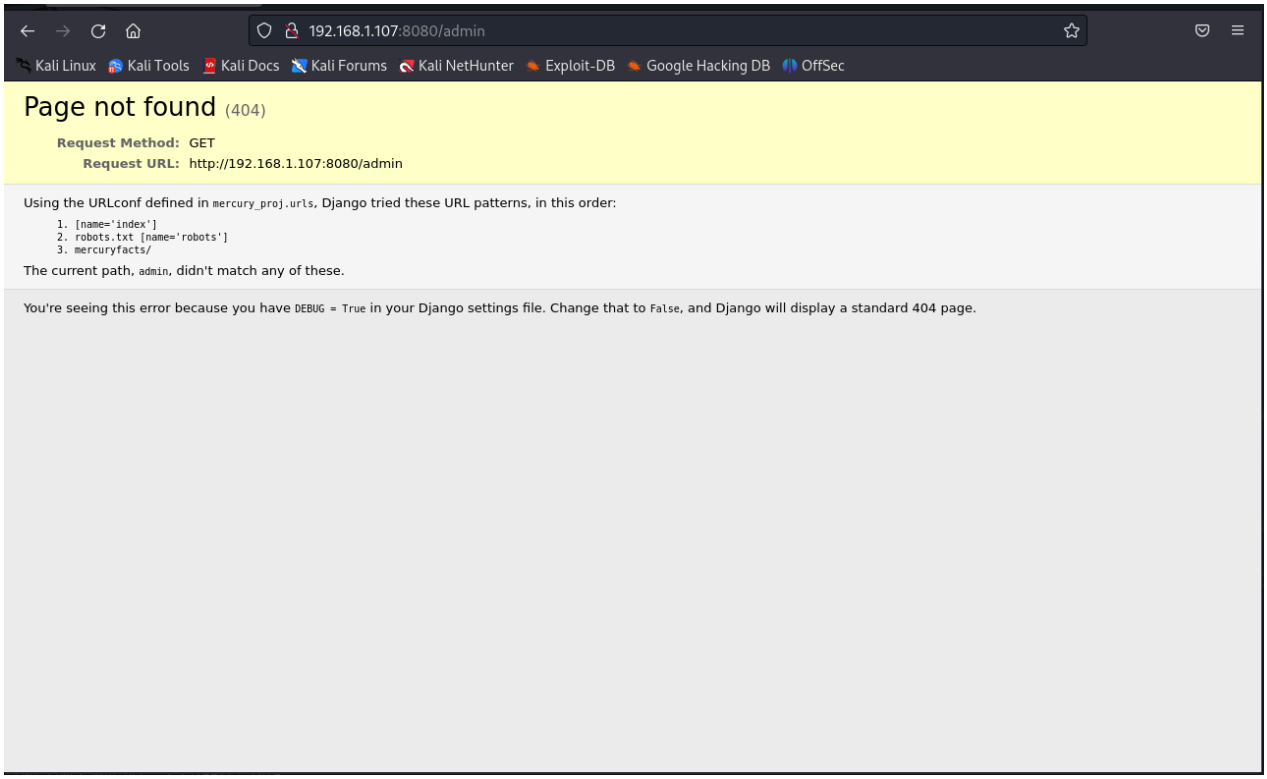
Since the HTTP port was open, I typed the IP into the browser to see if a web server was up. As you can see, this website is still in the development stage!

Step 4:



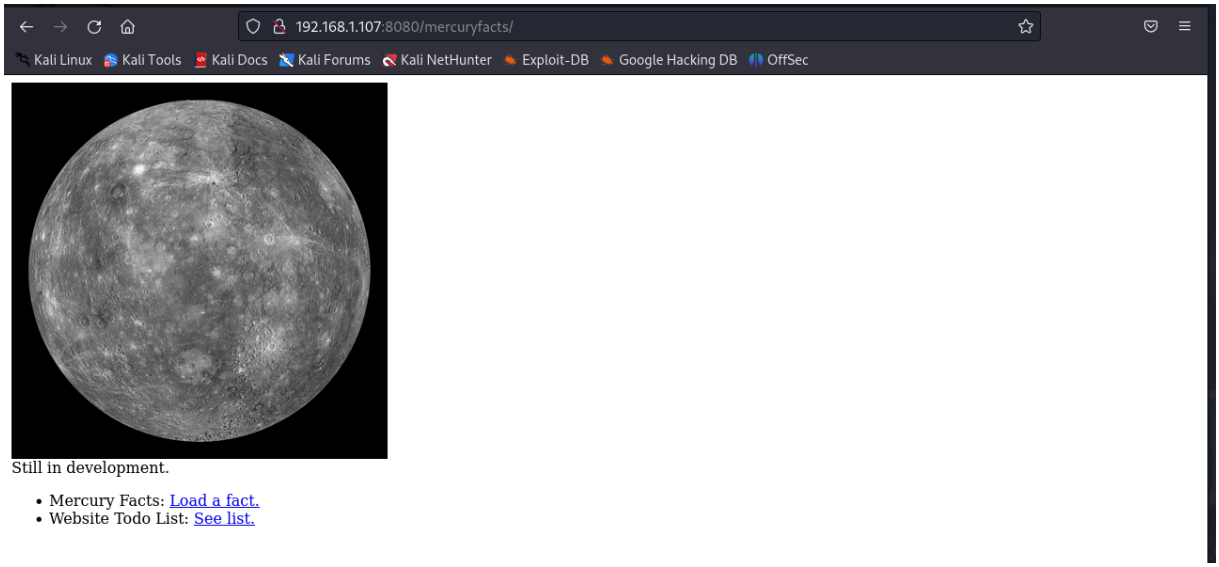
I then used a tool that was new to me called “dirb” which is an online directory scanner. This command was combined with a common word text file provided by Kali Linux. This looked through the directory and found a file called robot.txt.

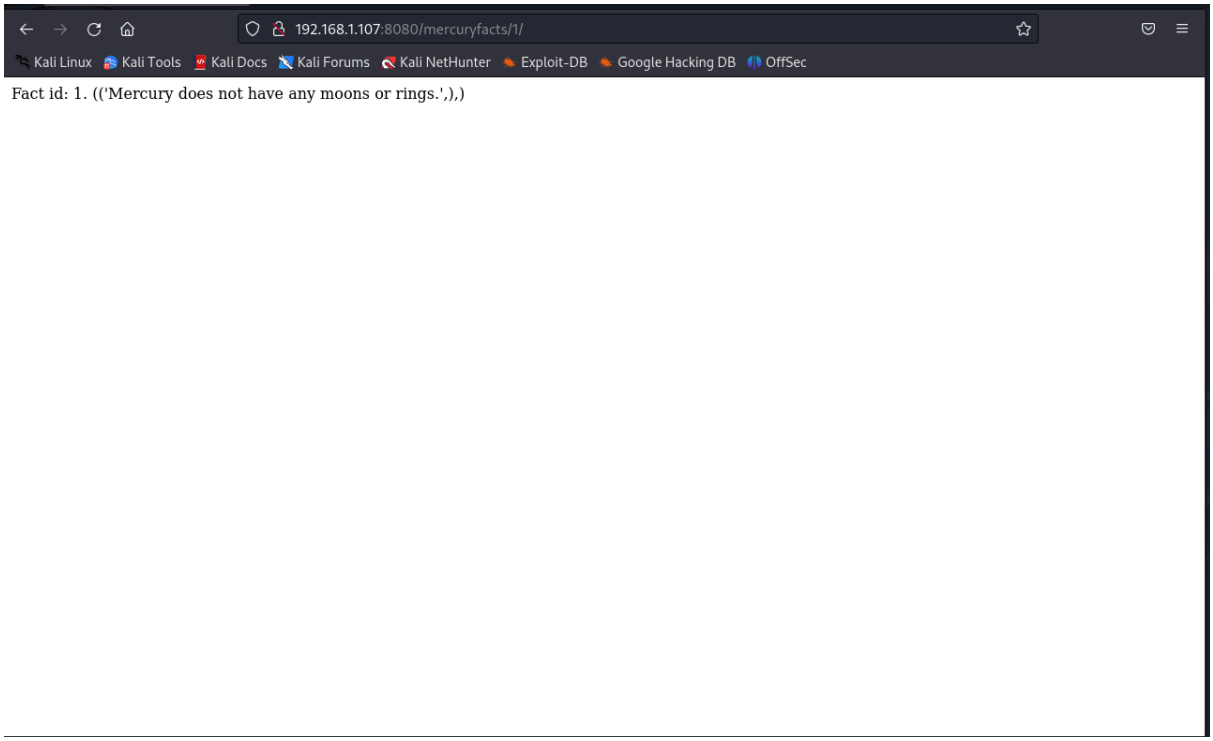
Step 5:



We added the /robots.txt to the link and nothing showed up so I did /admin to attempt some fuzzing and this screen was shown. I saw there was a path called mercuryfacts/.

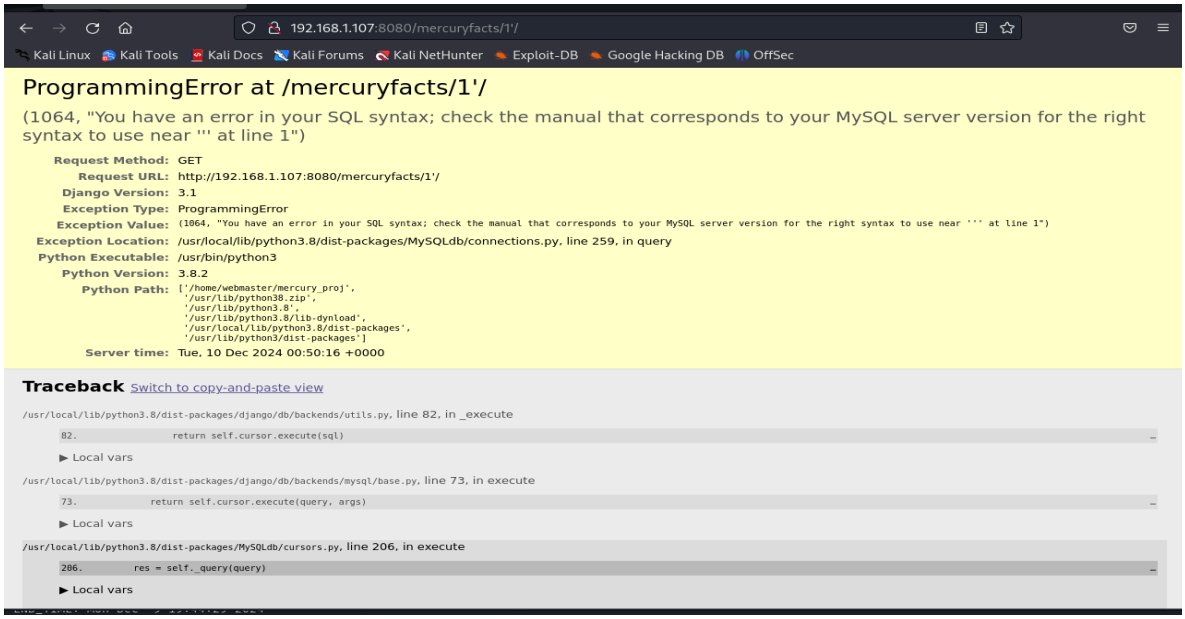
Step 6:





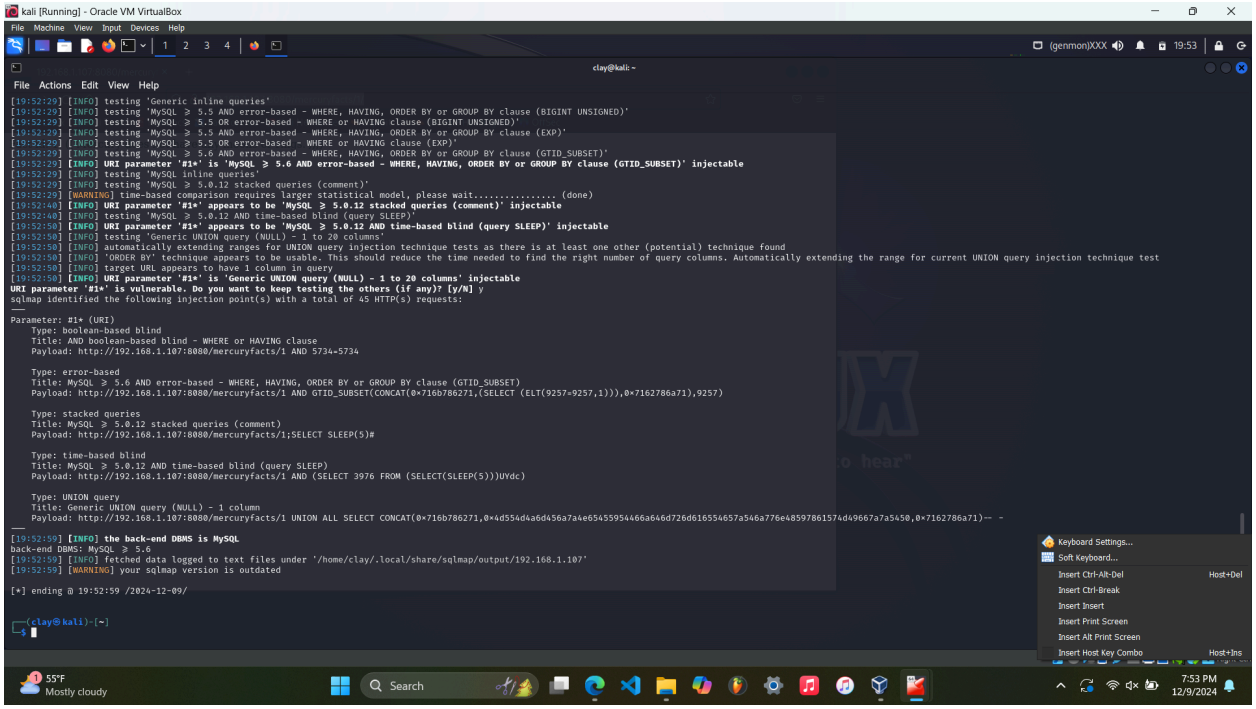
Once that path was typed in we opened the page.

Step 7:



In this step, I tried more attempts at fuzzing. I added a “ ‘ “ next to the one and a programming error showed up. As shown, there is a SQL error. Afterwards, I needed to check for SQL vulnerabilities.

Step 8:



I ran a sqlmap command on the browser link to test for vulnerabilities. It showed that a sql vulnerability was available.

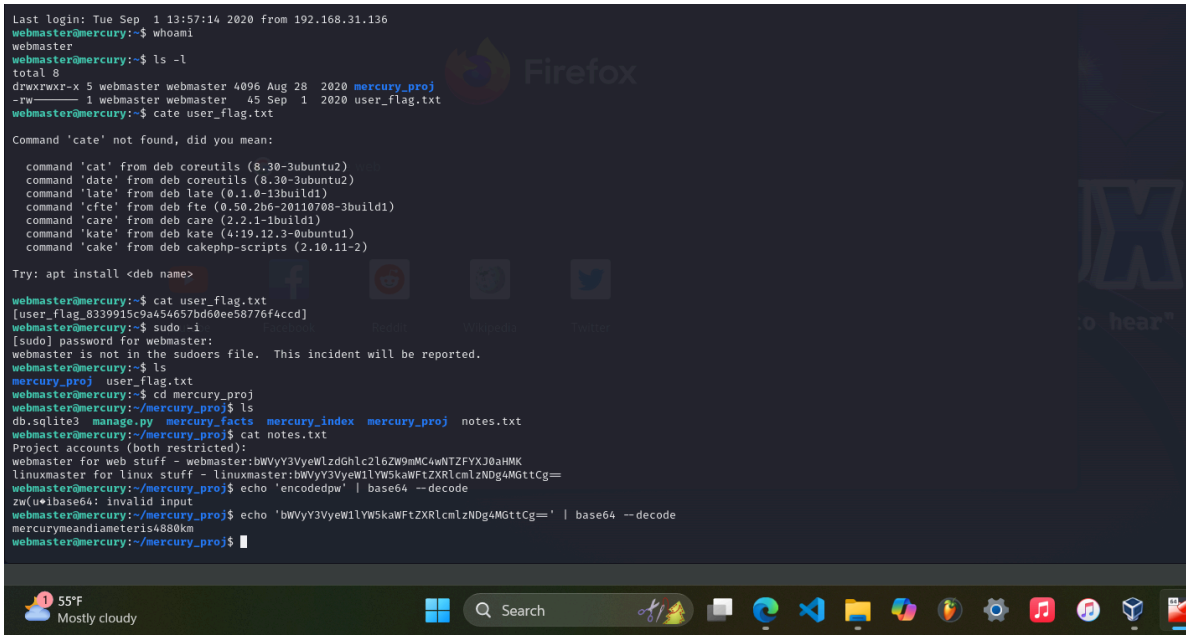
Step 9:

Since the injection worked, I ran the –dump-all command to show the database and I found the login credentials.

Step 10:

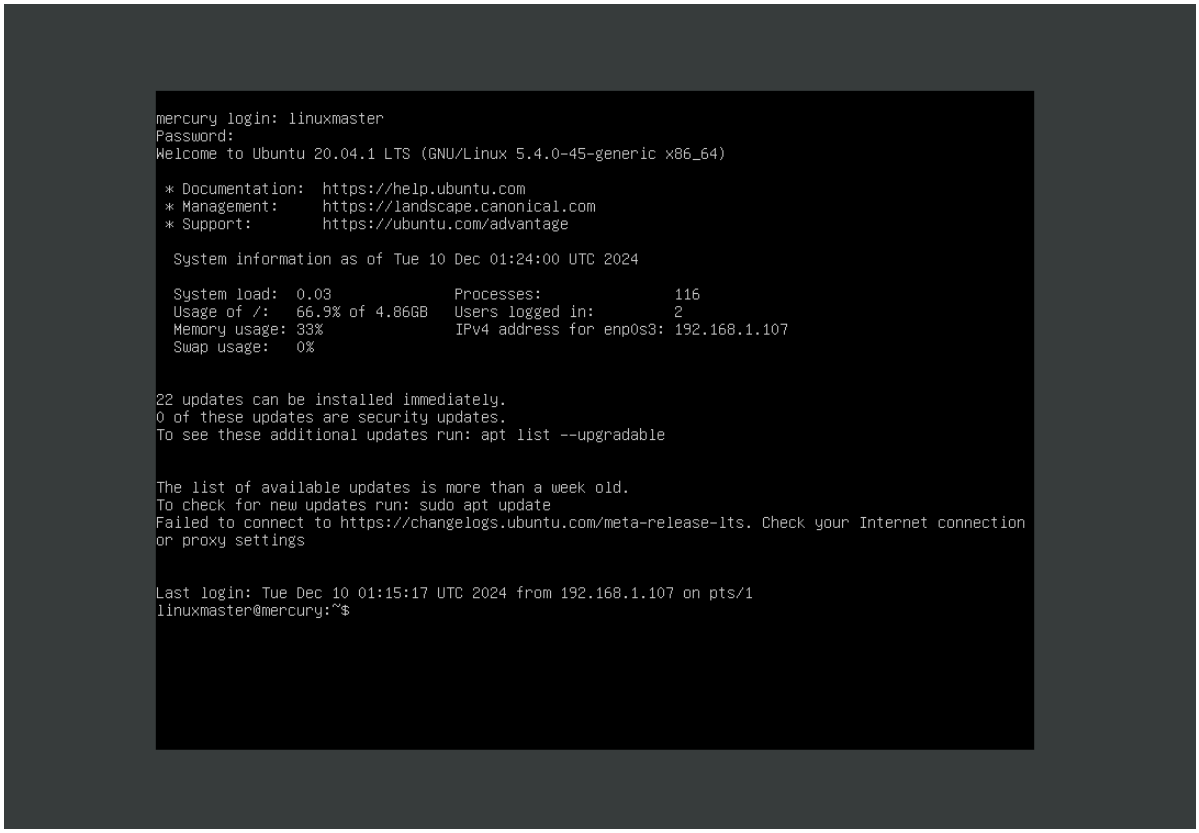
Since port 22 was open and the credentials were found. I could SSH to gain access.

Step 11:



After I got access to the command line, I went into the mercury project folder and I found a file called notes.txt. This file contained encrypted passwords to two accounts. The passwords were decoded and I found the credentials to the linux master account.

Step 12:



Afterwards, I used the credentials to login to the linux master account.

Lesson Learned:
Never publish/deploy an unfinished application!