**BUGBOUNTY HACKER**

**Prepared by:** Manasseh Mutugi

**Position:** SOC Analyst

**Date:** April 2025

**Department:** Cybersecurity Research

**Abstract:**

The Bounty Hacker room on TryHackMe is a beginner-friendly Capture The Flag (CTF) challenge designed to simulate a real-world scenario where a bug bounty hunter is tasked with gaining unauthorized access to a misconfigured Linux-based web server.

**Objective:**

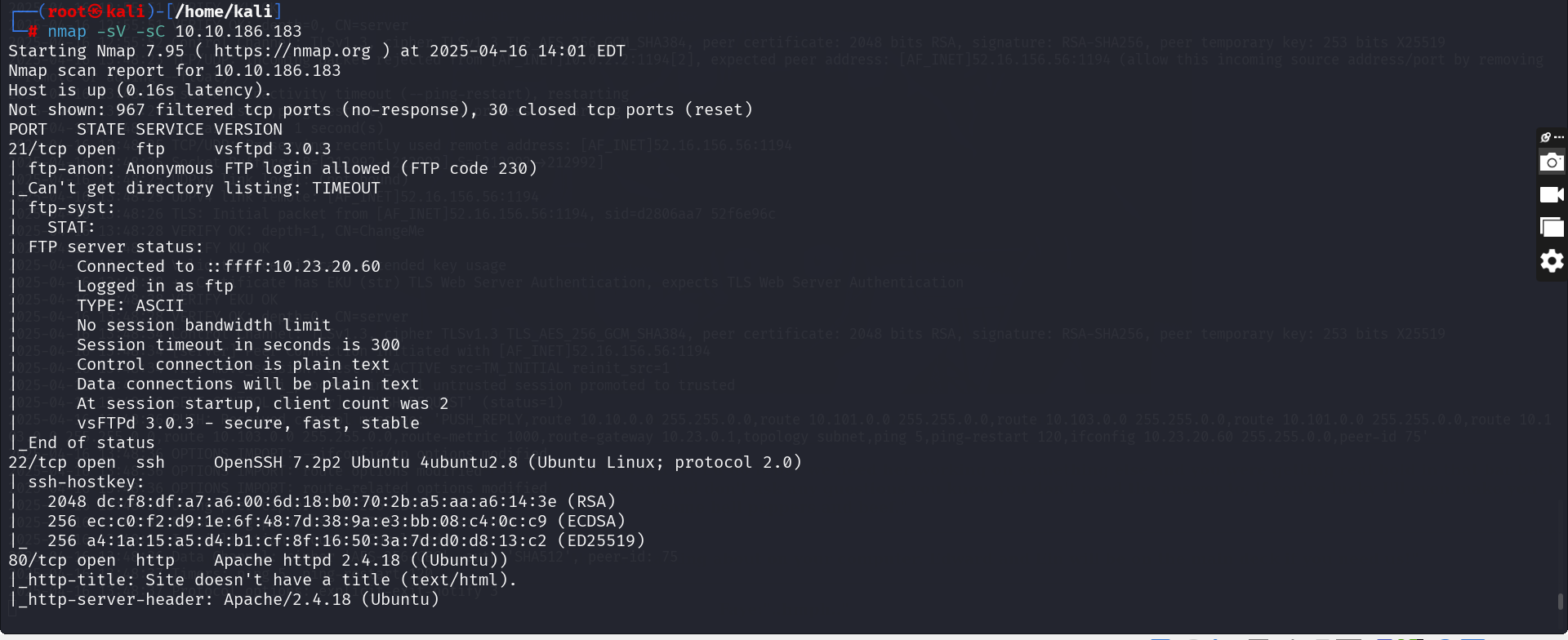
To identify and exploit weak credentials and misconfigurations in order to gain initial access, escalate privileges, and retrieve user and root flags — demonstrating basic offensive security skills and enumeration techniques.

**Skills Developed:**

* **Enumeration** with Nmap to identify open services and their versions
* **Brute-force attack** using Hydra on an exposed SSH service
* **FTP analysis** and basic file transfers
* Gaining shell access through **SSH login**
* **Privilege escalation** via enumeration of sudo permissions and exploiting misconfigured binaries
* Basic **Linux post-exploitation techniques**

**Room: Bounty Hacker**

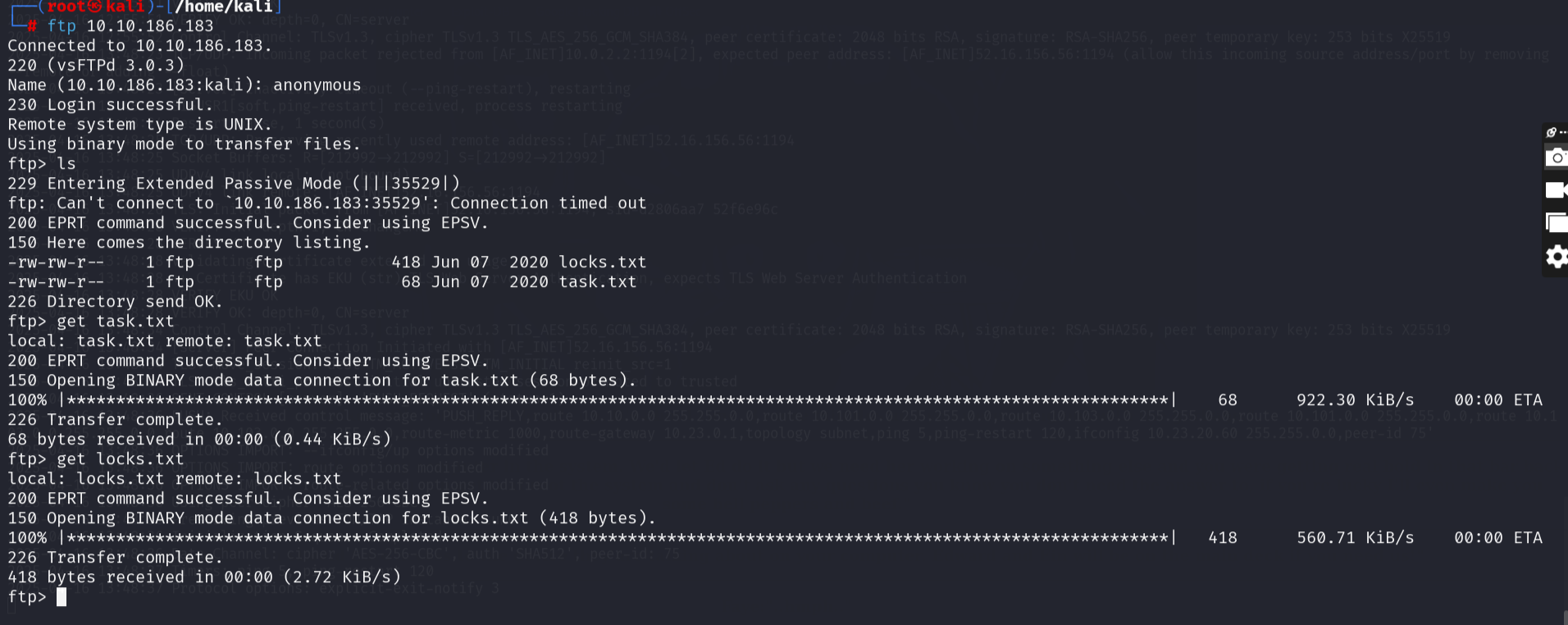
Using Nmap tool I scanned the IP addressto get the open ports



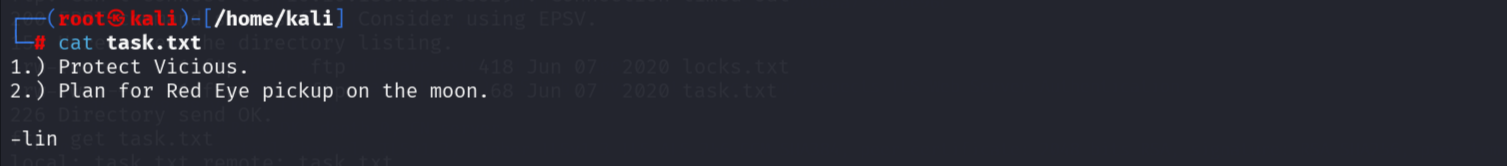
I decided to use FTP to access the machine as shown below

Password is  **anonymous** by default

On listing the files **locks.txt** and  **task .txt** are displayed and to download them I used the **get** command.



**Qstn: Who wrote the task list?** Lin



To get the password to the user I used **hydra**

*hydra -l lin -P locks.txt ssh://10.10.186.183*

**command result**

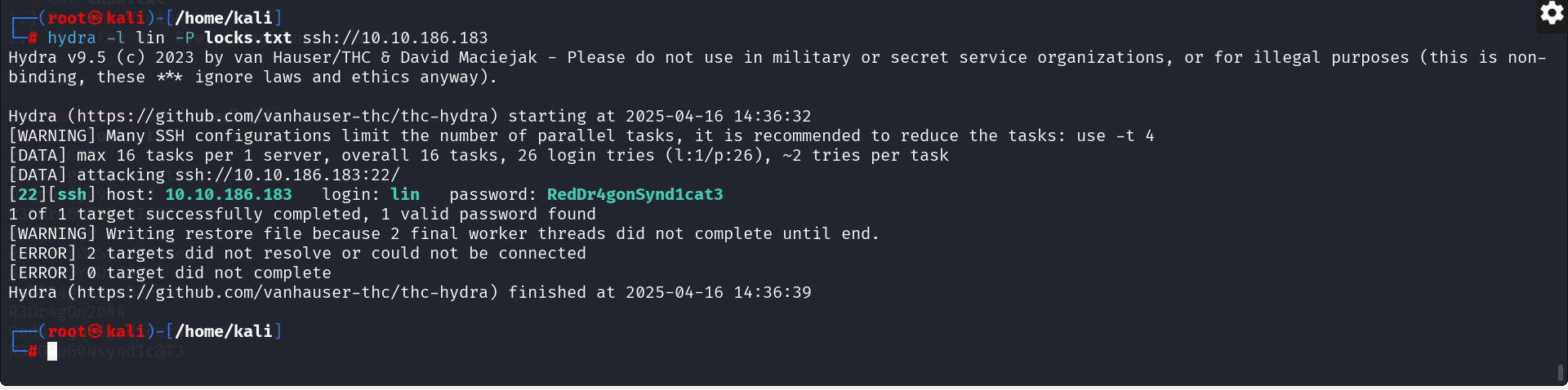
hydra runs hydra tool

-l use specified login

-P use password list from file

ssh:// target ssh port 22

$IP exported ip address

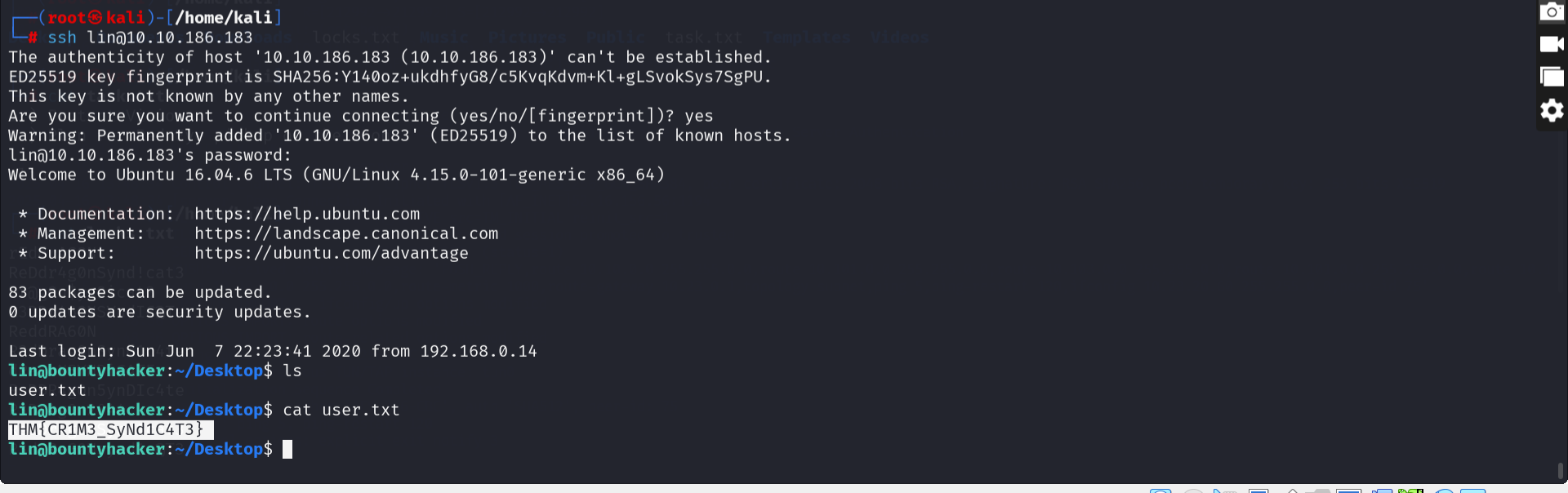


To get the **user.txt.** I had to login to the machine using **ssh** since the port was open

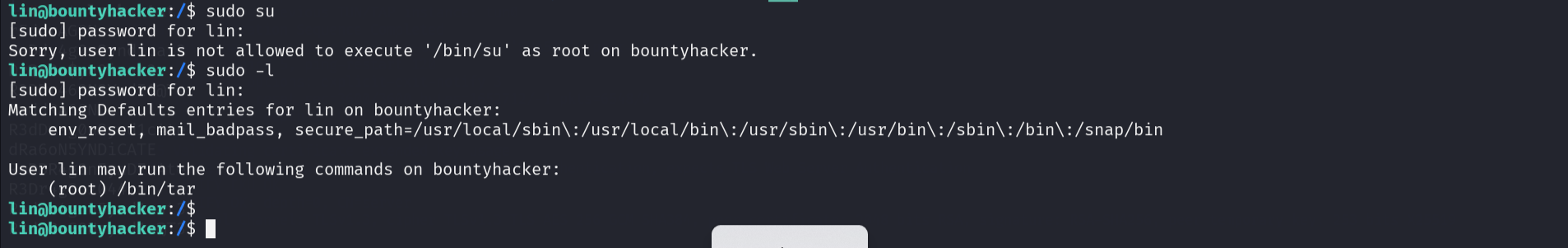
*Ssh* [*lin@10.10.186.183*](mailto:lin@10.10.186.183)and input the password which we found earlier using hydra to be **RedDr4gonSynd1cat3**



On listing the files using **ls,** I used the **cat** command to capture the flag which is **THM{CR1M3\_SyNd1C4T3}**



but simply using **sudo -l** to list commands run as sudo reveals that our lin can use **tar** command as sudo.

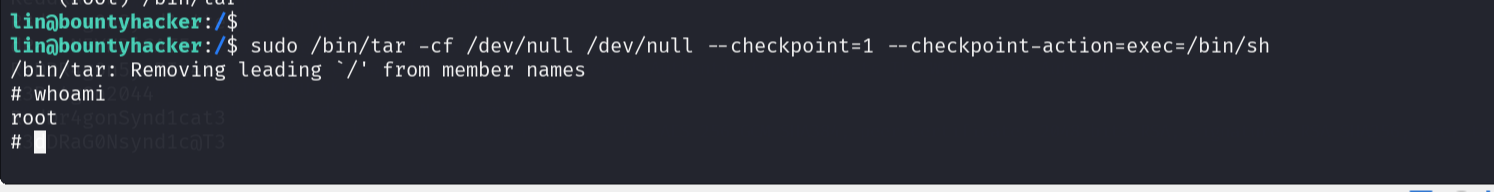


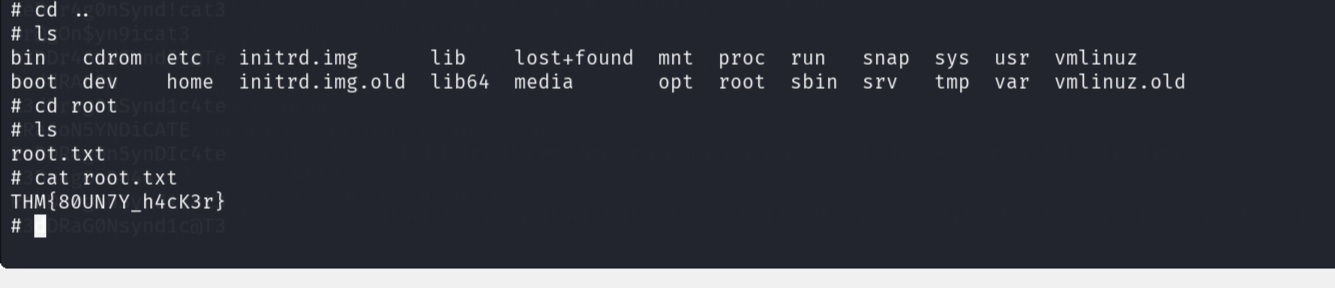
Quick look at [GTFOBins](https://gtfobins.github.io/) and search for tar bin shows us that we can use it to escalate things:



so I used the command:

*sudo /bin/tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh*



and the path to file **is /root/root.txt**. Cat out the file or less it, or nano it, 

*\*The Bounty Hacker room is a perfect entry point for those starting in cybersecurity or ethical hacking, reinforcing the critical importance of secure configurations and access controls in modern systems.\**