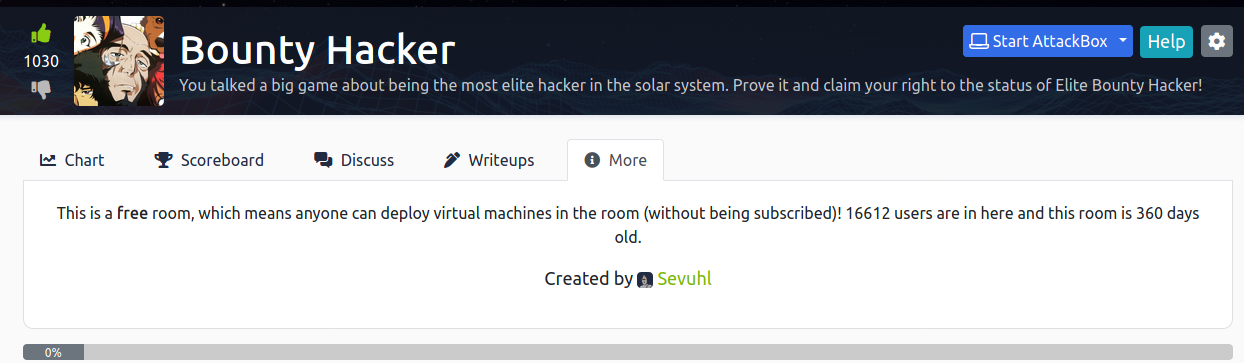
**Bounty Hacker write-up**

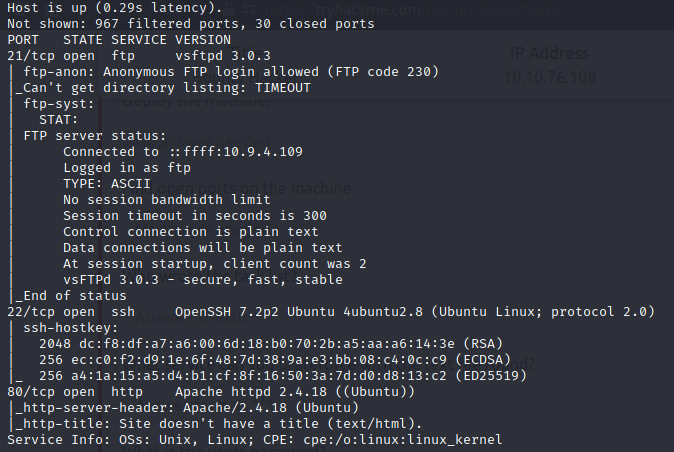
This is write-up for Bounty Hacker in TryHackMe which is Bounty Hunters inspired CTF that we have to gain access to target machine and elevate our privilege to rock this box

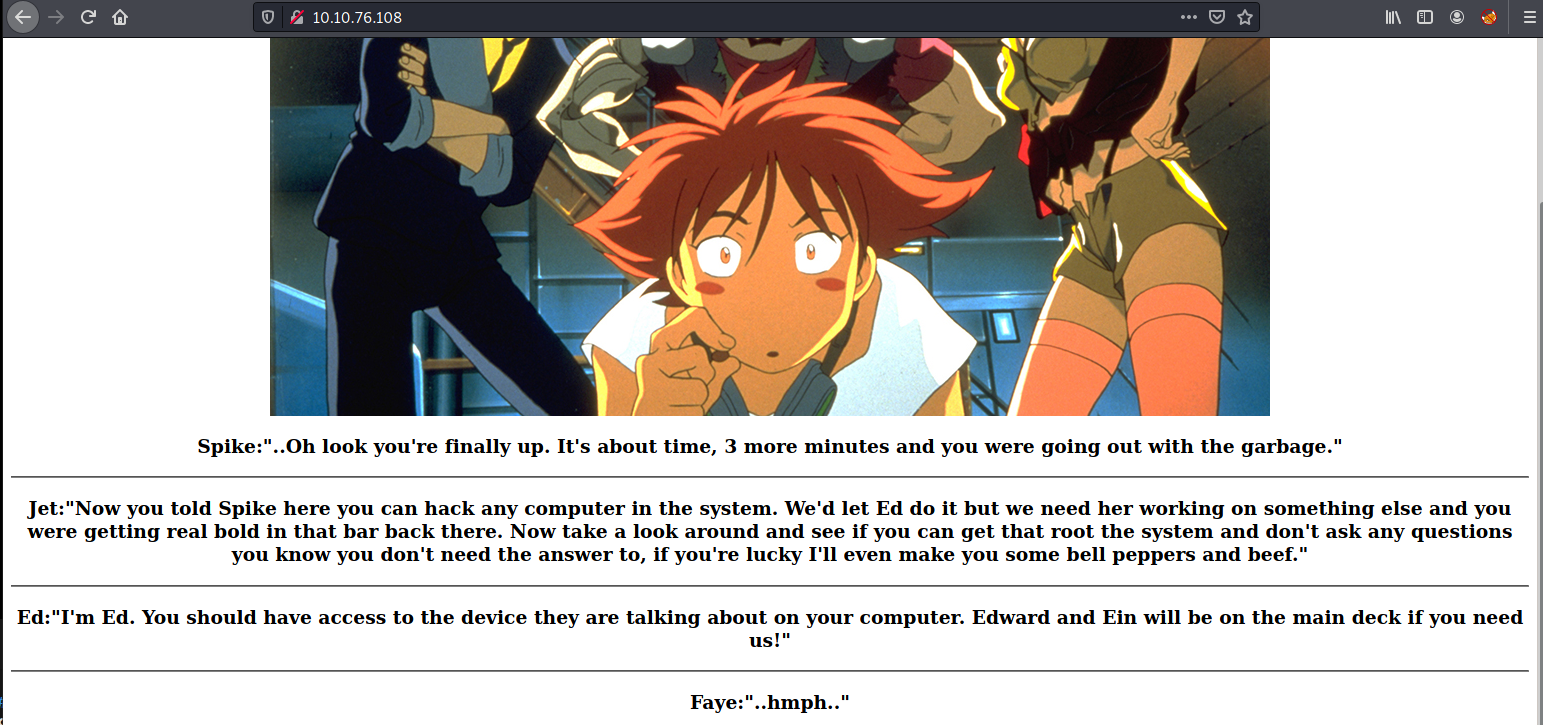
Site: <https://tryhackme.com/room/cowboyhacker>



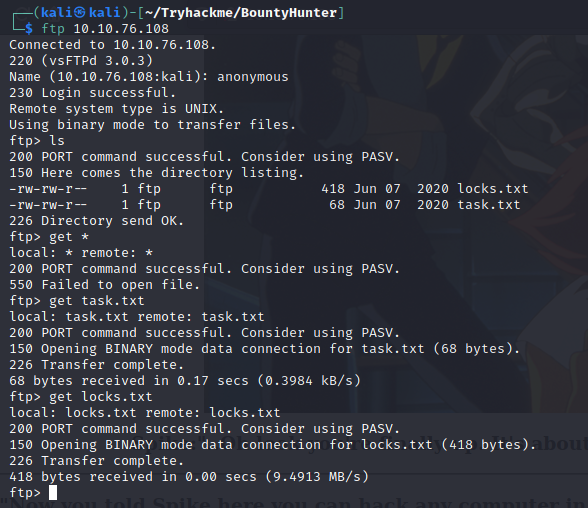
**Find open ports on the machine**

Using nmap to scan and we found that port 21,22 and 80 are opened which we can use anonymous user to login ftp server, ssh is running that we can connect if we got username and web server

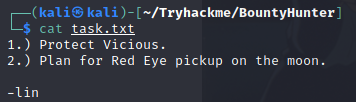


In Website we will see some of conversation among these bounty hunters and nothing else, we can use gobuster here while gobuster is running let’s check FTP server

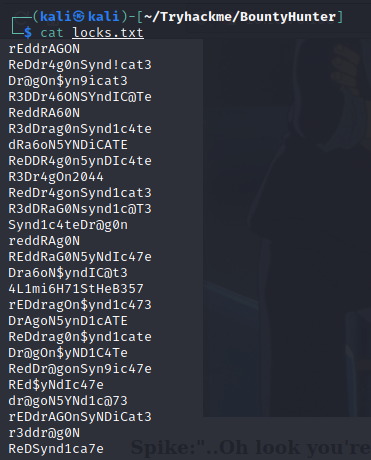
After connect to FTP server we will see 2 text files here, download both of them to read



And we got that lin is potentially a username for ssh



And other text file is dictionary file which we can bruteforce using this



**Who wrote the task list?**

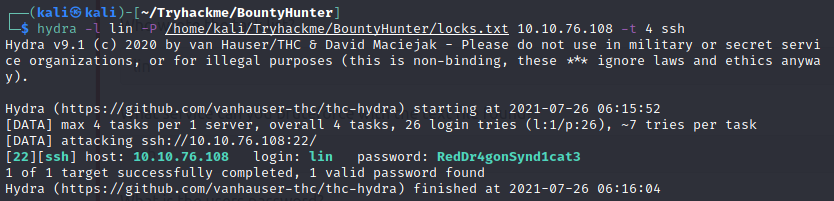


**What service can you bruteforce with the text file found?**



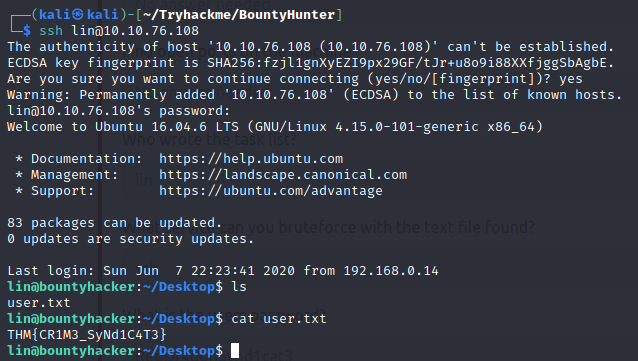
**What is the users password?**

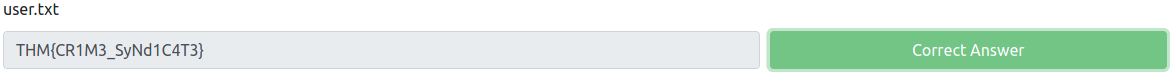
Use hydra to bruteforce password of this ssh



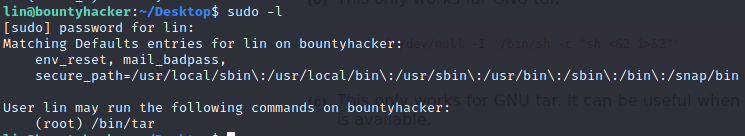


Now it’s time to connect using ssh and first thing we see is user flag

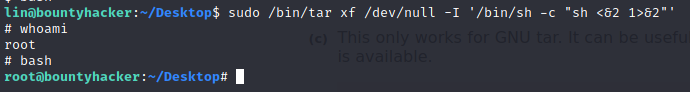




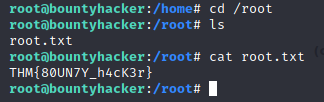
Now try to elevate our privilege which we found that lin can use tar as root



We can find a way to get root shell in [GTFOBins](https://gtfobins.github.io/gtfobins/tar/)



Now go to root directory and capture root flag





All Answers and flags

