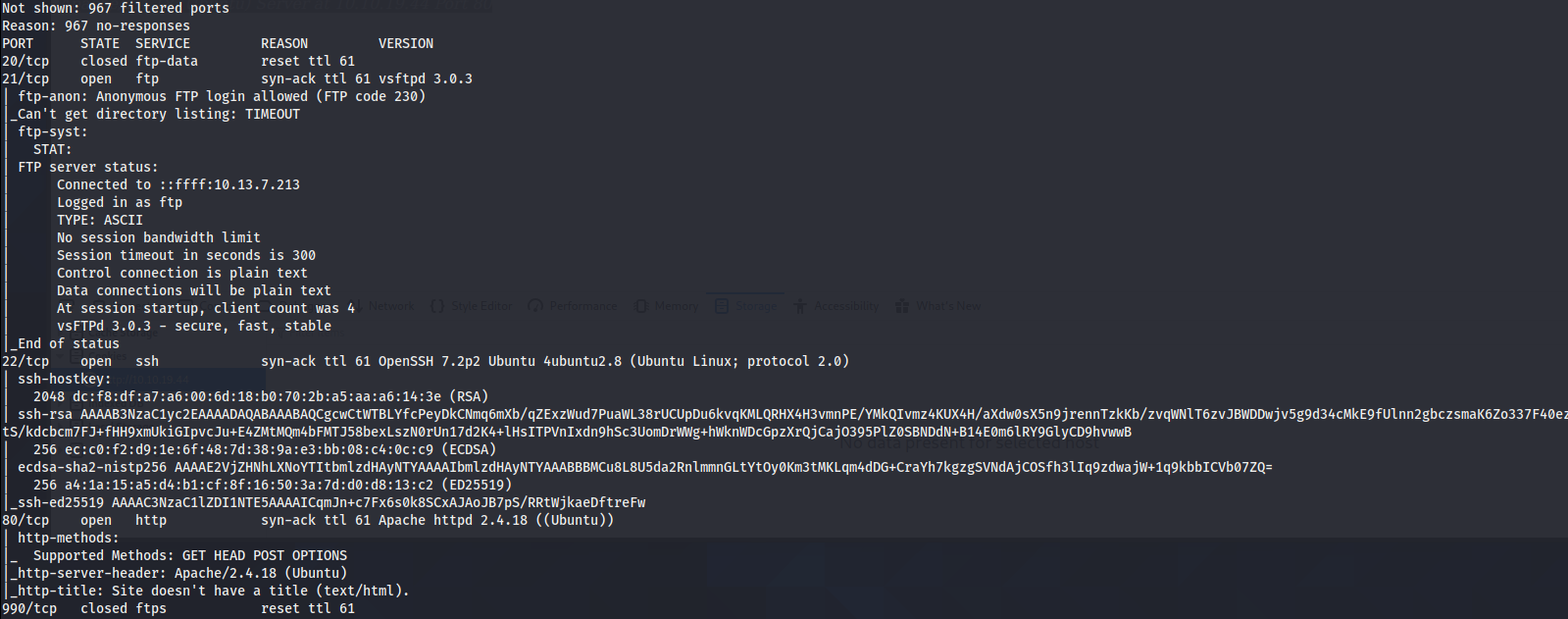
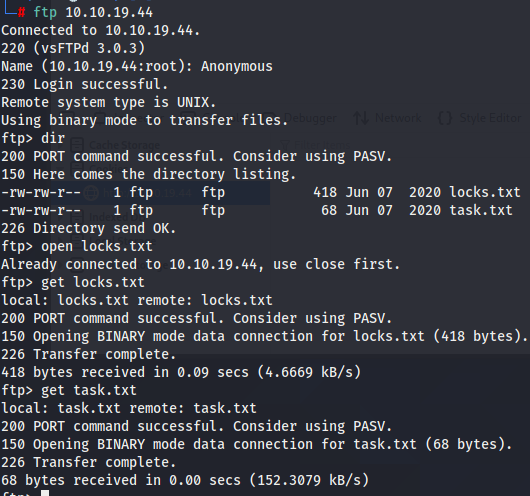
As always, the first thing I did when approaching a new box was the usual NMAP scan:

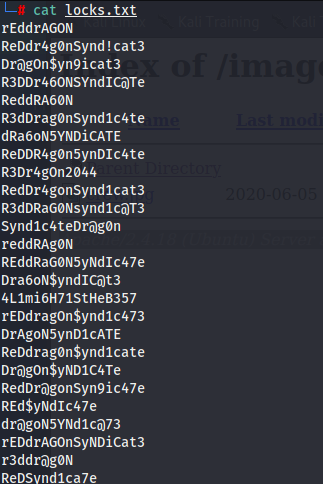
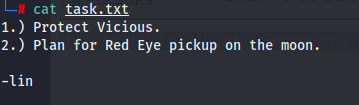




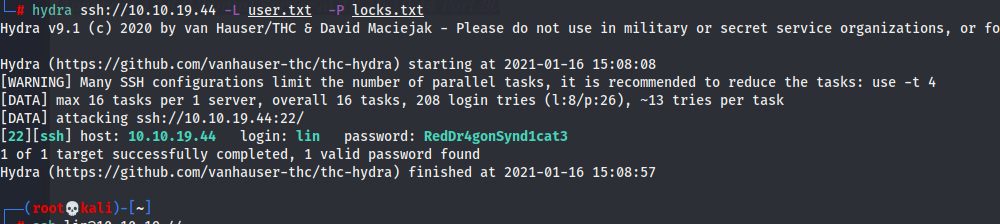
This gave me some really good information. The scan showed so many open ports to work with and check out. However, at the same token, right away I noticed that the FTP server allows for Anonymous login. So that might be worth checking out.



The anonymous login worked! This allowed me to check out the entire directory and find some text files with some useful information. I used the **get** function to download them to my Kali VM.



The first text file, locks.txt, had a list of strings that appear to be potential passwords. So I definitely kept that on the back burner. The other text file had a list of tasks for this ‘lin’ person to do. Which included protecting Vicious. Since I watch Cowboy Bebop, I understand that for this box there could only be about 7 potential users on this machine. So, I compiled a list for Jet, Spike, Faye, Ed, Ein, lin, and Vicious. This became my user.txt list.

By having a comprehensive user and password list, I can brute force the ssh port to find a user/password match. By using the tool **hydra,** I can iterate through all passwords and users I must find a match. Which it eventually did…

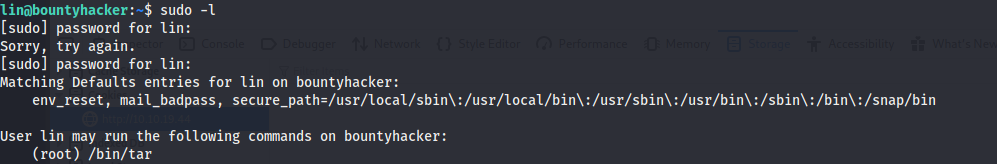
Using this new username/password combo that we acquired, I can ssh into the machine no problems. Once I am in, I have no problem finding the first flag called **user.txt**.





There is still one more flag to get in this room. That would be the flag that is within the root.txt file. The issue here, however, is that I am only a user and not the root user. Any attempts to access the root account or the root directory is met with **Permission Denied**. So what do I do?

First thing I do is see if the user that I used to ssh in has any inherent sudo privileges I can exploit. Lo and behold, they do! They can run the command **/bin/tar** as a root user.



After doing some research, I found this command:

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

This basically exploits the fact that the user has access to this, then escalates to the root account.

Running that command gives me root and the flag!

