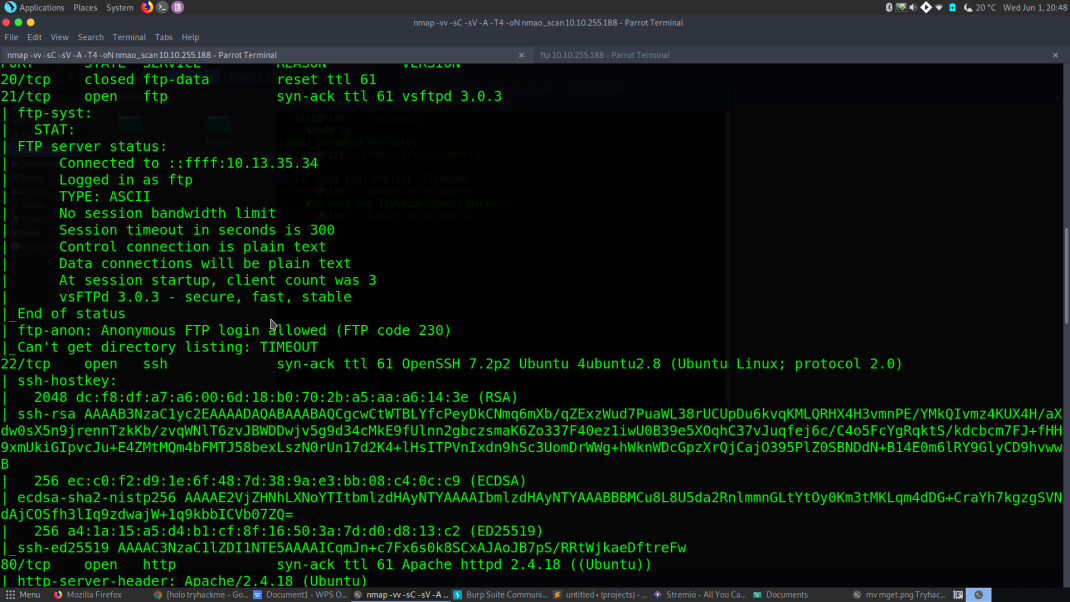
# Bounty Hacker

**Initial recon with nmap**

**nmap -vv -sC -sV -A -T4 -oN nmap\_scan 10.10.255.188**

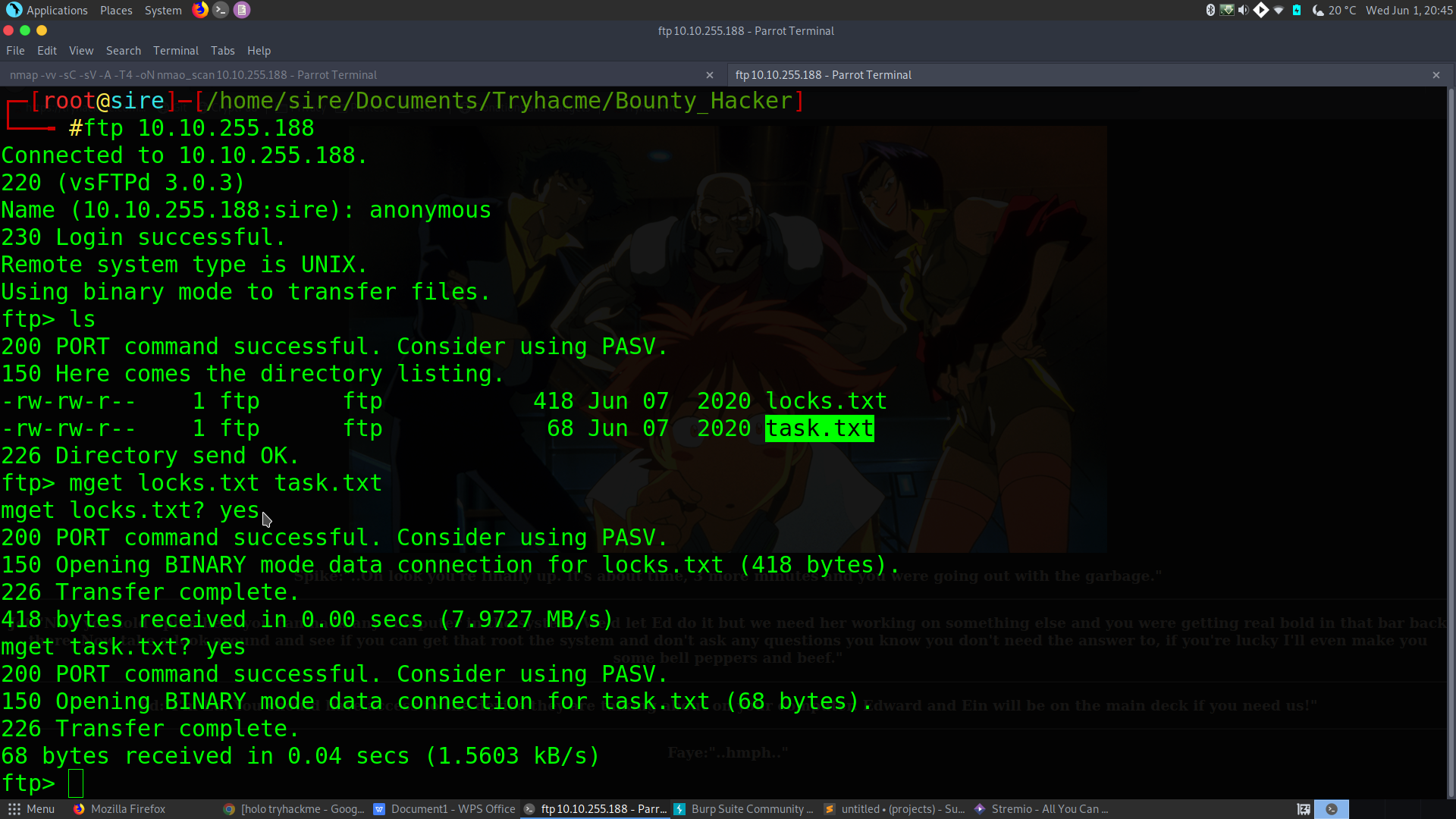


Alot of ports are open under 1000 ports.

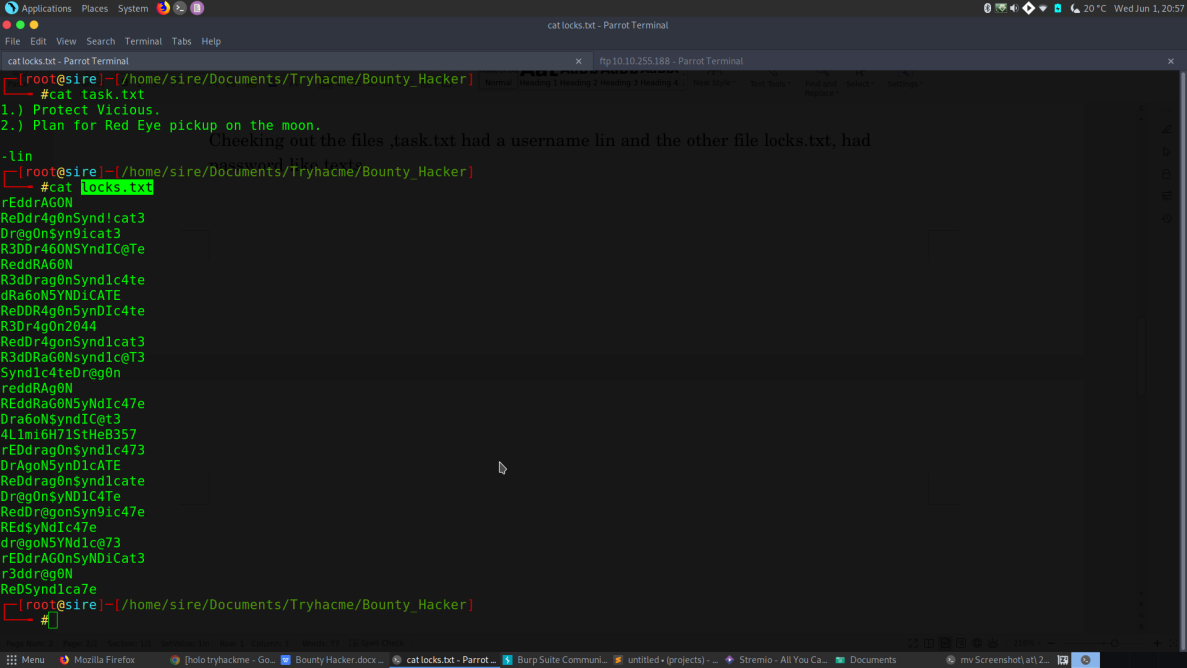
But my attention was cought by 3 ports

1. port 80 where there was a webserver
2. port 22 ofcouse because it is ssh
3. port 21 ftp and there was anonymous log in where there were 2 text files

**FTP(port 21) recon**

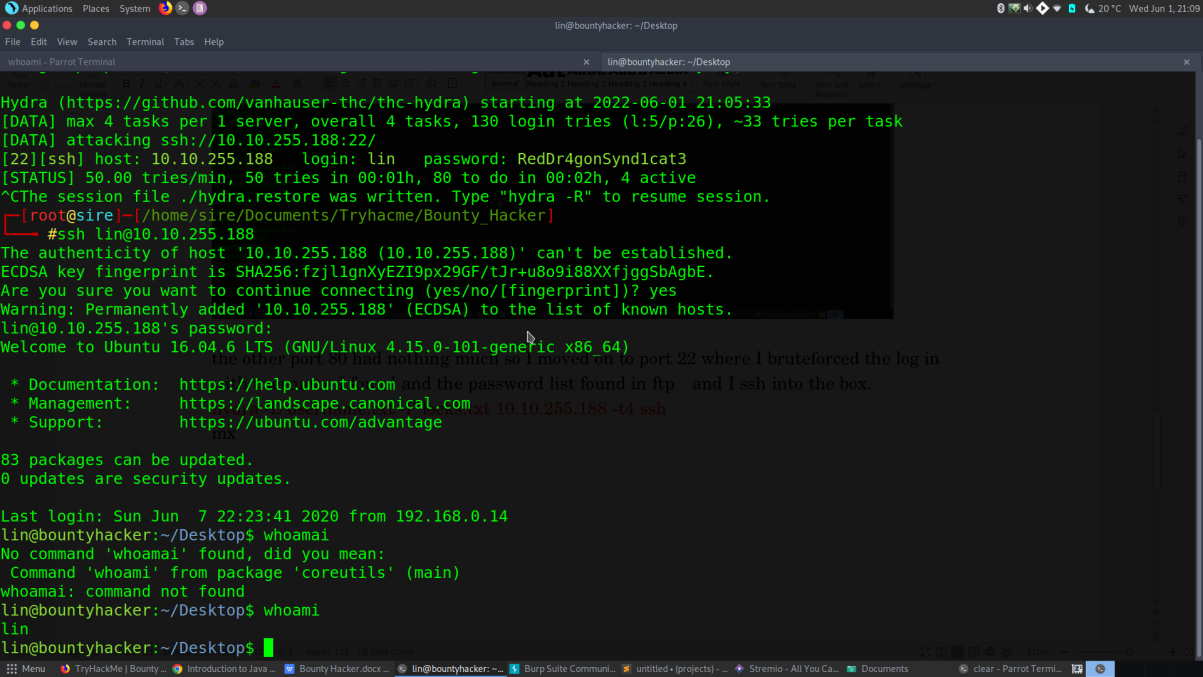


Cheeking out the files ,task.txt had a username lin and the other file locks.txt, had password like texts



the other port 80 had nothing much so I moved on to port 22 where I bruteforced the log in with username(lin) and the password list found in port 21(ftp)

**hydra -L username.txt -P locks.txt 10.10.255.188 -t4 ssh**



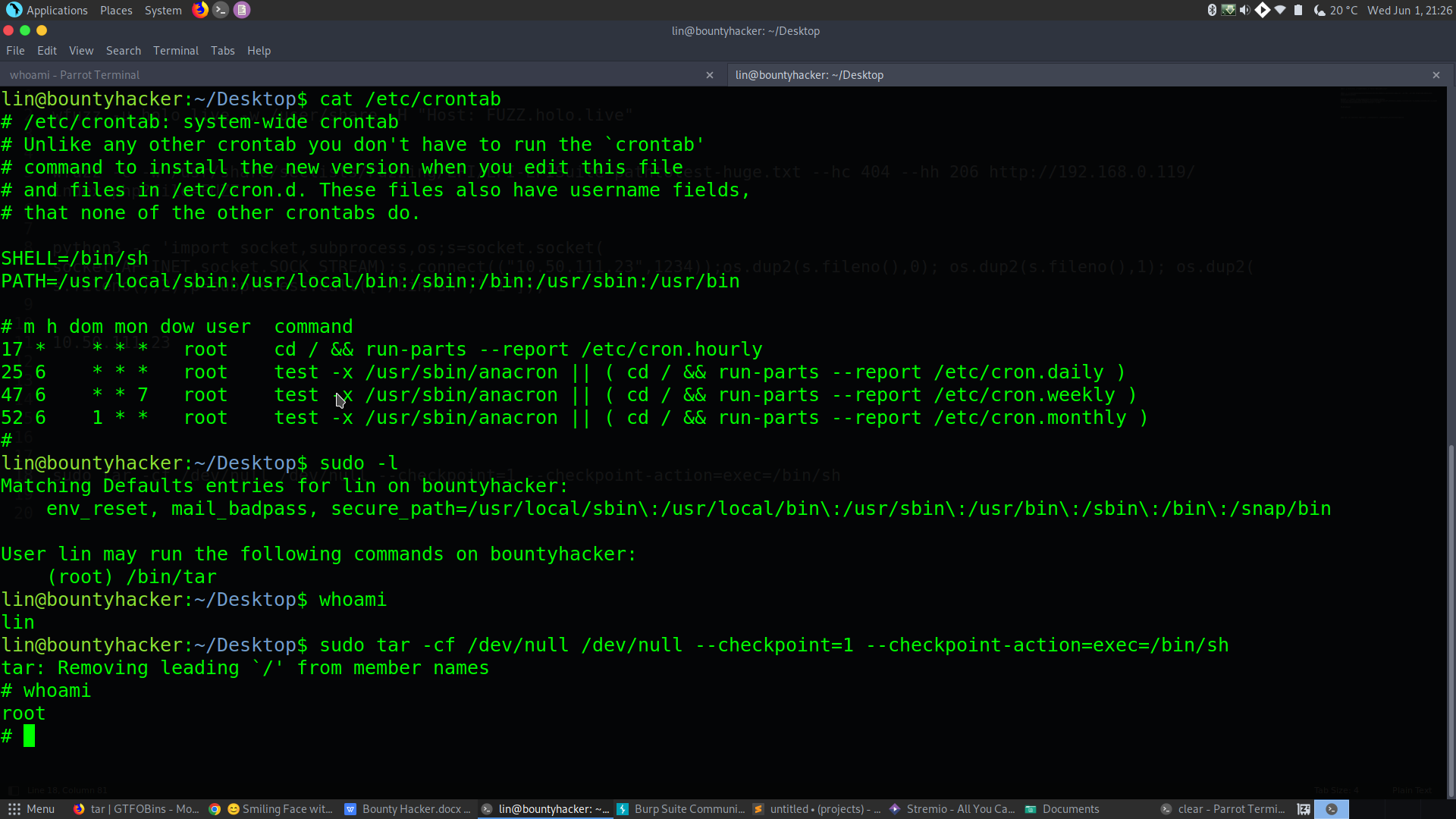
Lucky me,I was able to find lin’s password where I proceeded logging in.

I pocked around like eveywhere even checked crontab and found nothing

But cheking the allowed (and forbidden) commands for the invoking user -lin on the the machine,I found luck :)

User lin was allowed to run /bin/tar with root permission.Cheking GTFOBins,I found a way to elevate my privilege to root with the following command

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



**MACHINE POWNED**

:)