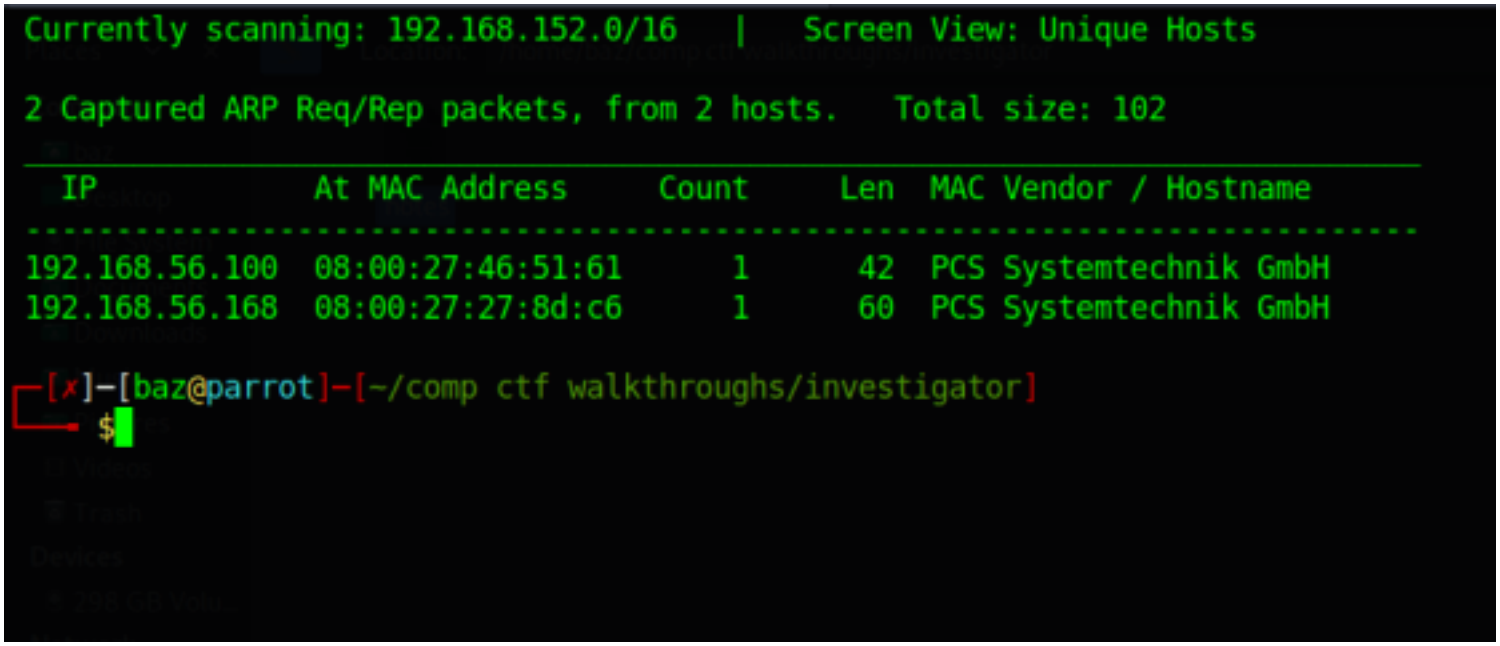
Investigator

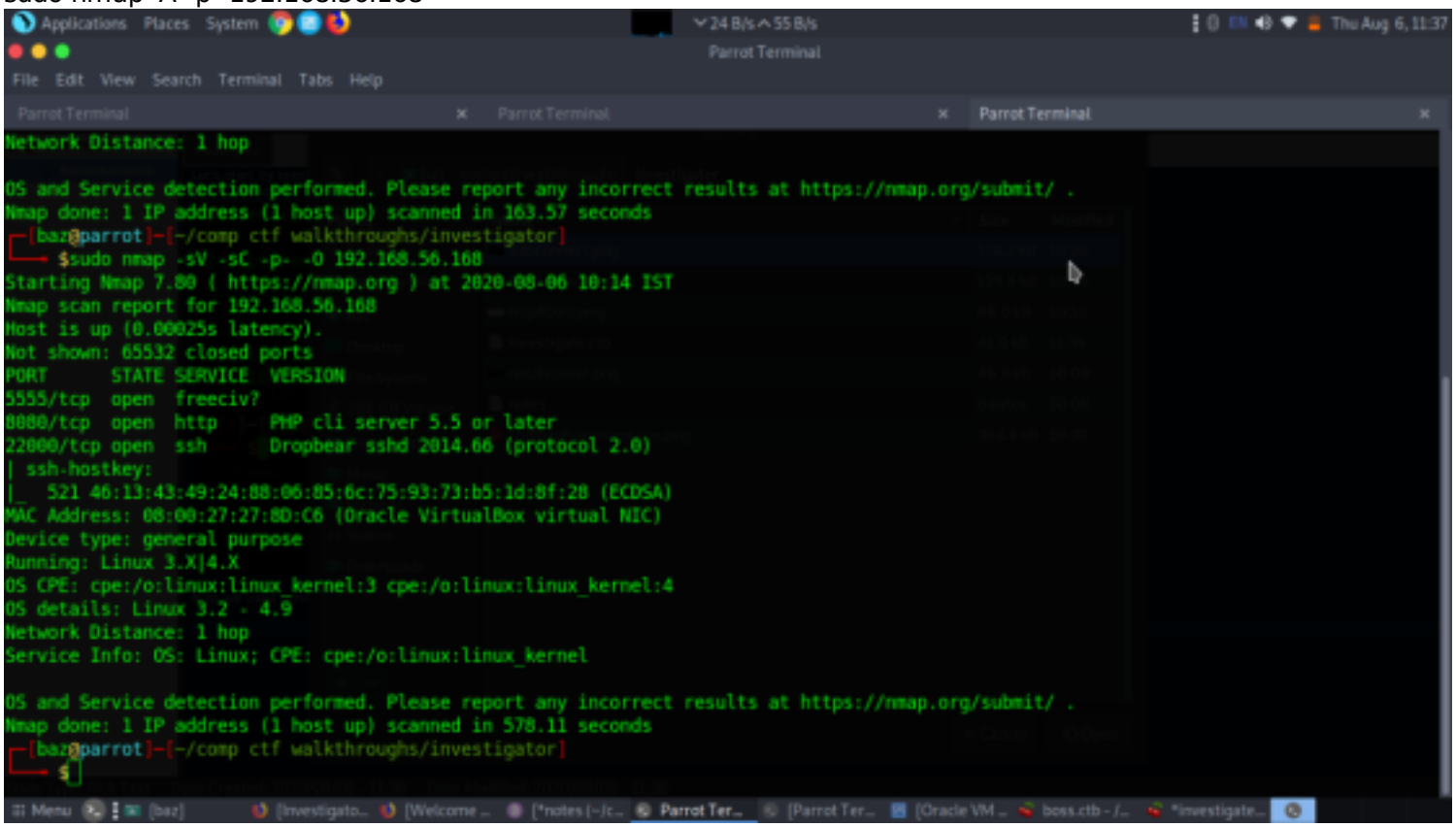
These were the description given by the author:
 The investigator to finish this machine,Its for only beginners, Share your Screen shot on telegram group, Group link will be in flag.
 The main goal is to find user and root flag.
The creator of this ctf is Sivanesh Kumar
Link to download: https://www.vulnhub.com/entry/investigator-1,504/

Reconnaisance

Let's start by identifying target IP
sudo netdiscover -i vboxnet0



Now we used nmap to identiy open ports,services,versions etc.
sudo nmap -A -p- 192.168.56.168

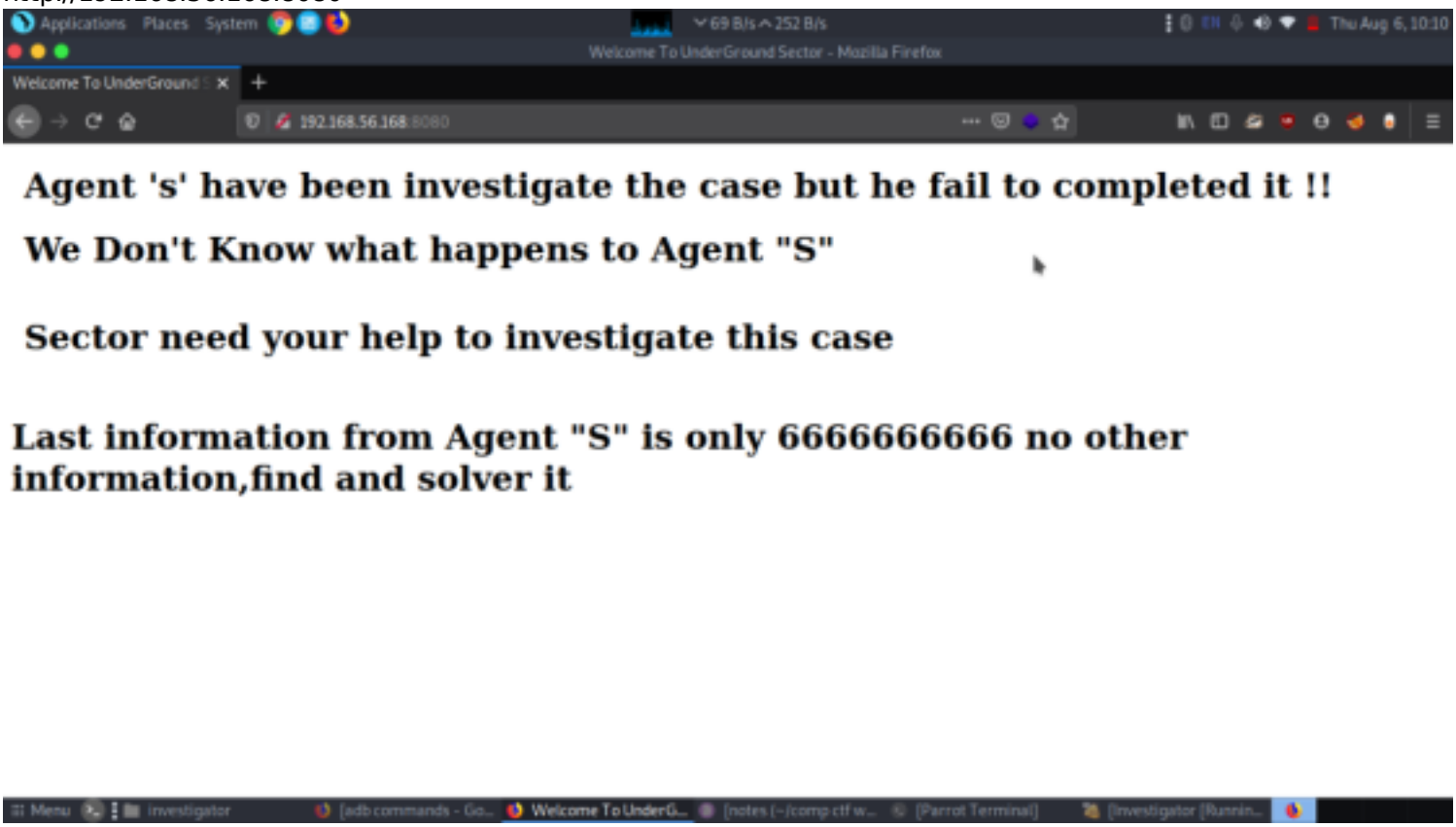


We got to know there is three open ports.

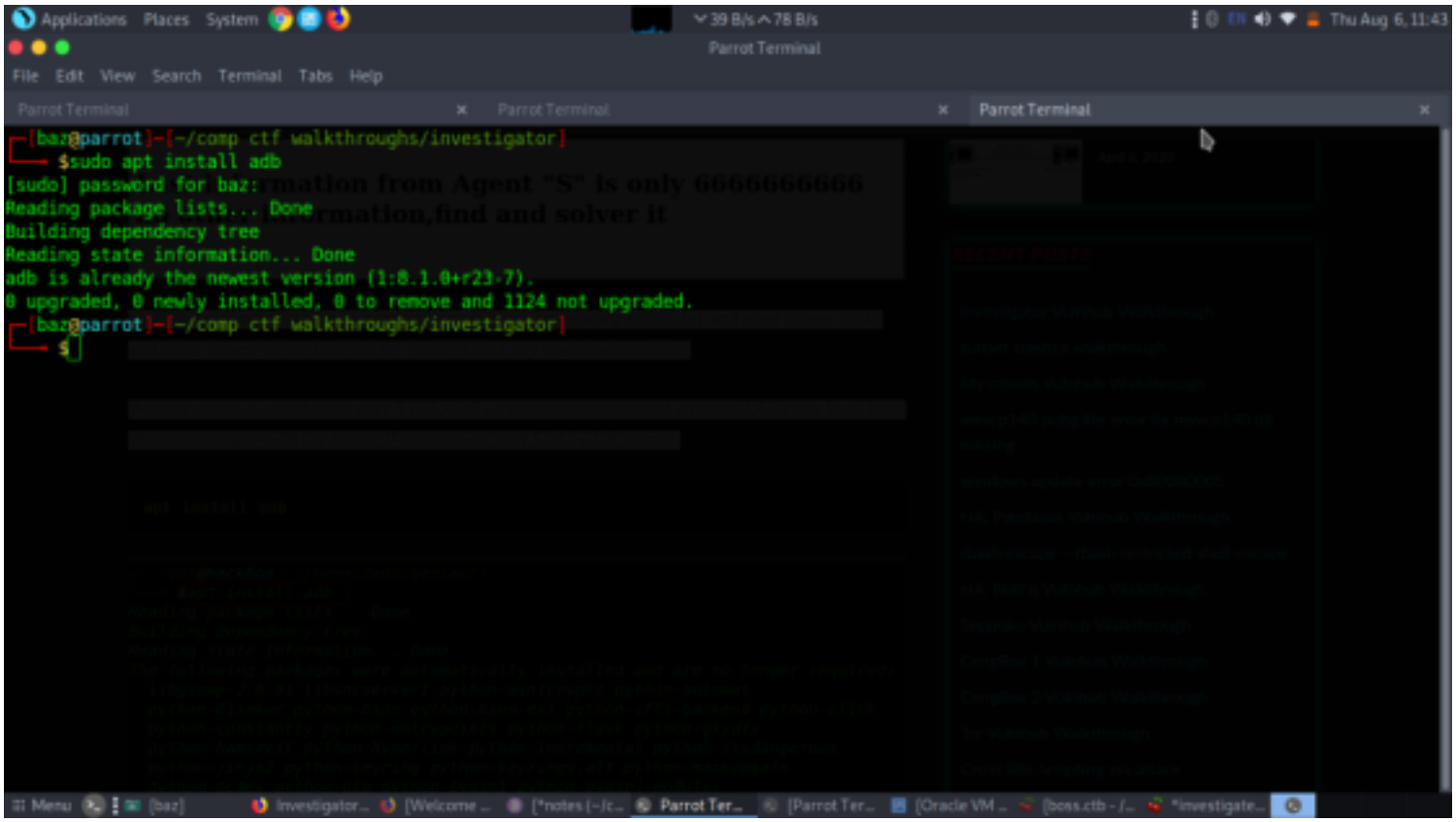
5555- freeciv(Freeciv versions up to 2.0, Hewlett-Packard Data Protector, McAfee EndPoint Encryption Database Server, SAP)
8080(http)
22000(ssh)

Enumeration

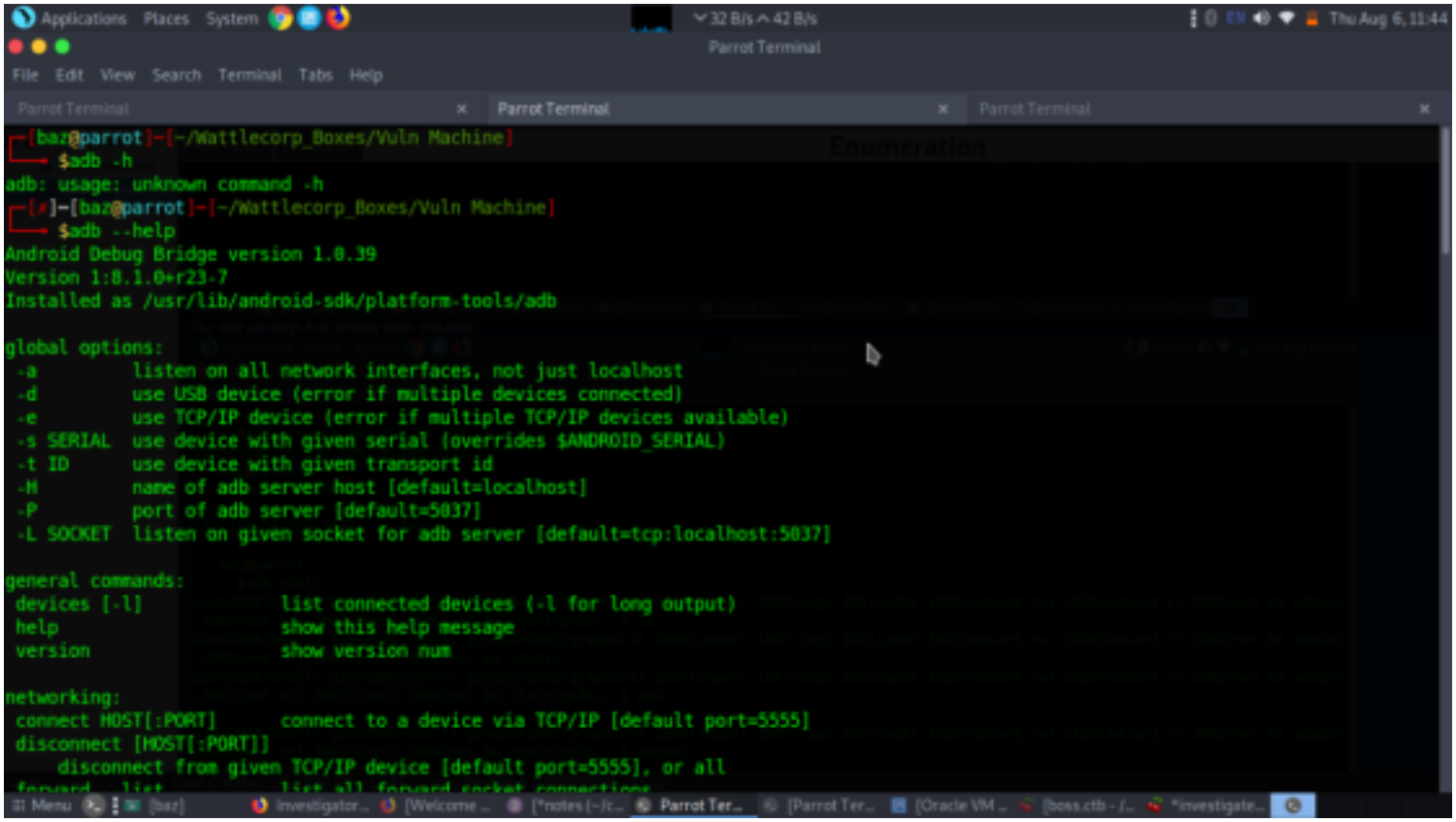
Let's start by looking port 8080
http://192.168.56.168:8080



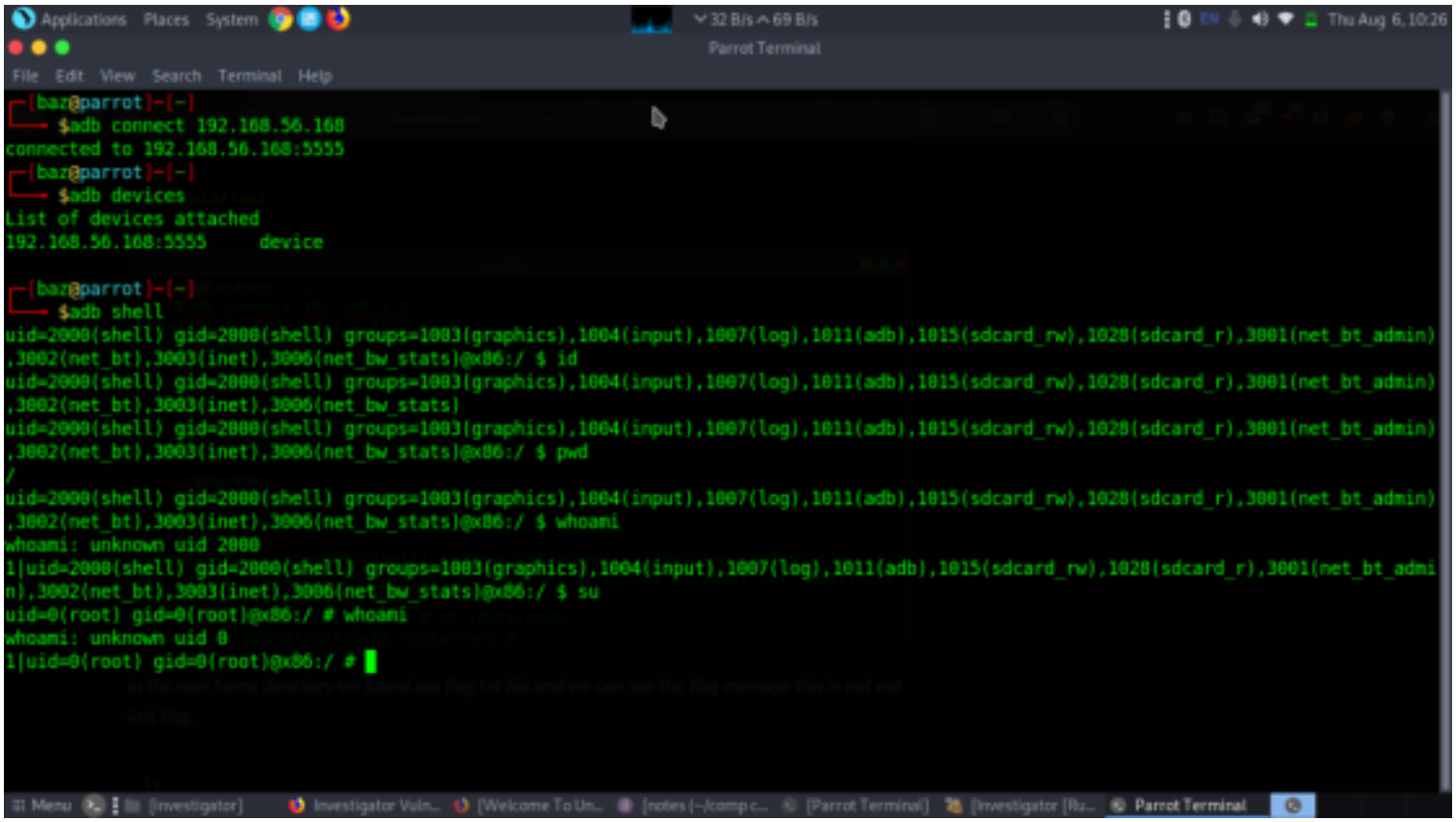
ports 8080 is not given much more information, we try reading robots.txt and page source code and other enumeration tool but we couldn’t find any useful information.
then we move our next open port 5555 ADB server enumeration first we install ADB our local host then we connect with the target IP address on port 5555 ADB service.
sudo apt install adb



Our adb package has already been installed
man adb

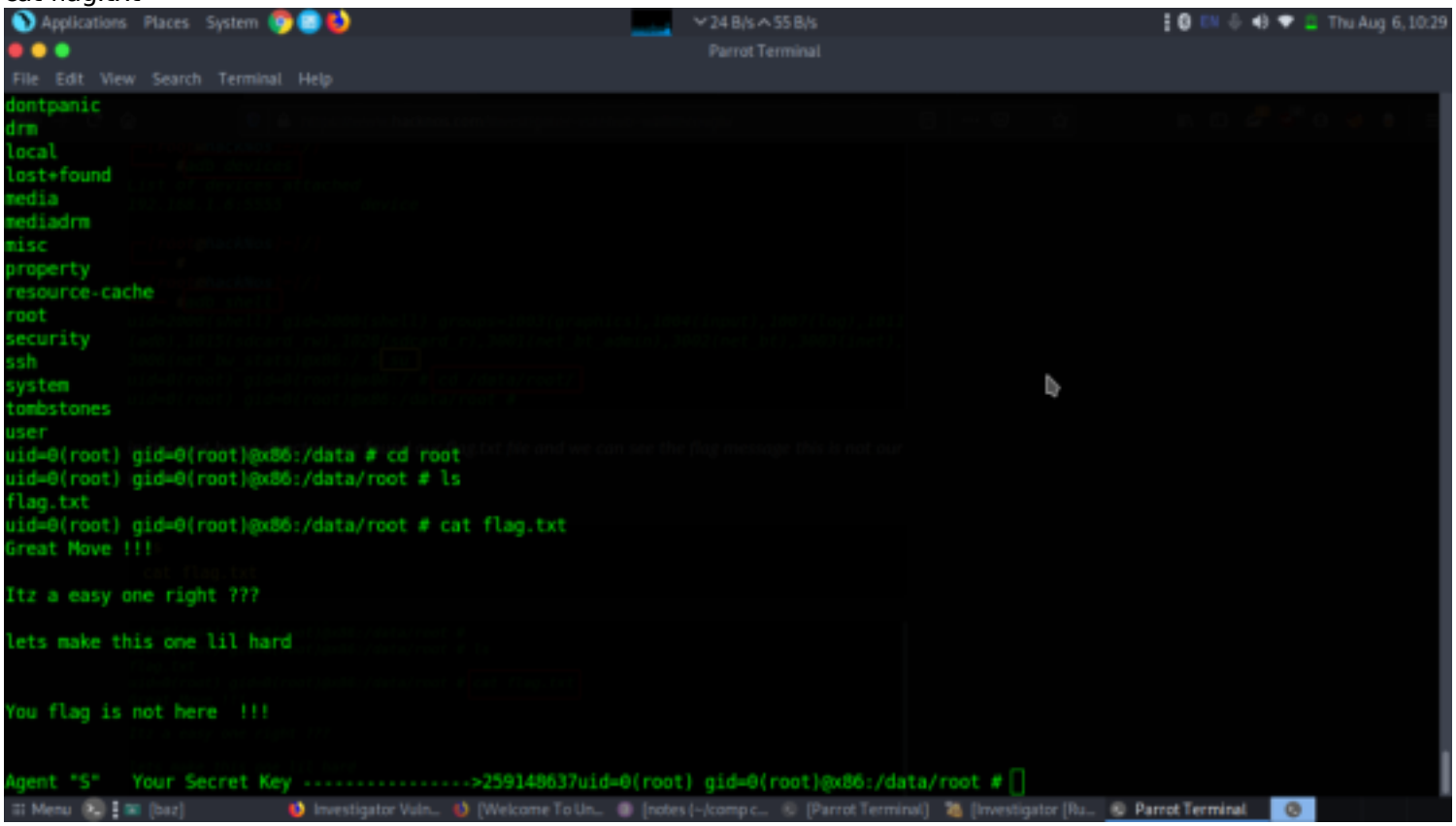


Now let's connect using the options from the manual page.
abd connect 192.168.56.168
adb devices
adb shell
id



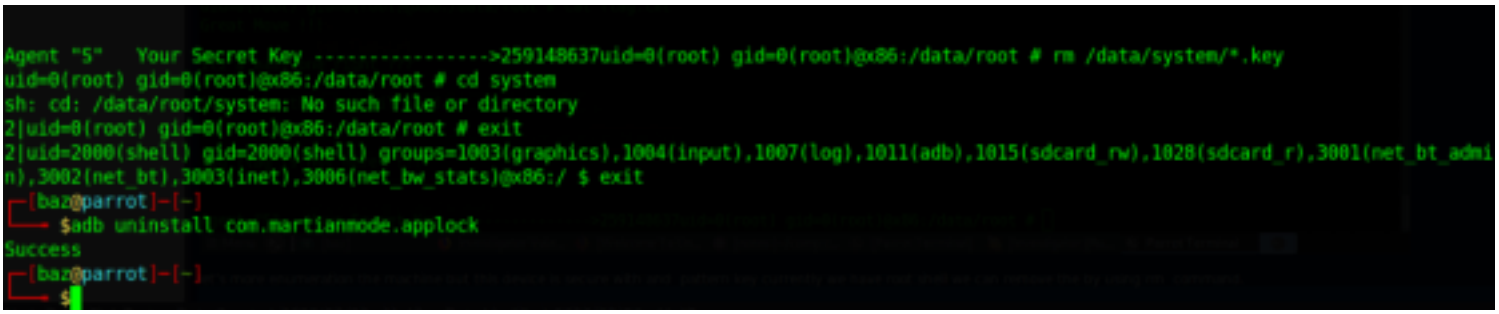
Exploitation

Now let's check for the flags.
in the root home directory we found our flag.txt file and we can see the flag message this is not our last flag.
cd /data/root
cat flag.txt



let’s more enumeration the machine but this device is secure with and pattern key currently we have root shell we can remove the by using rm command.
rm /data/system/*.key

target screen lock is bypass successfully and we open many android application but they are protected third party app lock let’s move back the adb console and remove the app lock.
`adb uninstall com.martianmode.applock`



Finally we got our final flag in the messaging application. our challenge is successfully completed by reading the message.