IOT
Firmware Analysis

Name: Isha Gupta

What is firmware?

Firmware is a piece of code residing on the non volatile section of the device allowing and enabling the device to perform different taskrequired for the functioning of the device.
It also helps in functioning of various devices, kernal, boot loader, file system and additional resources.

In this we will extract the firmware and analyse it.

Environment used:
Attify OS

Firmware to be analysed:
OWASP IoTGoat

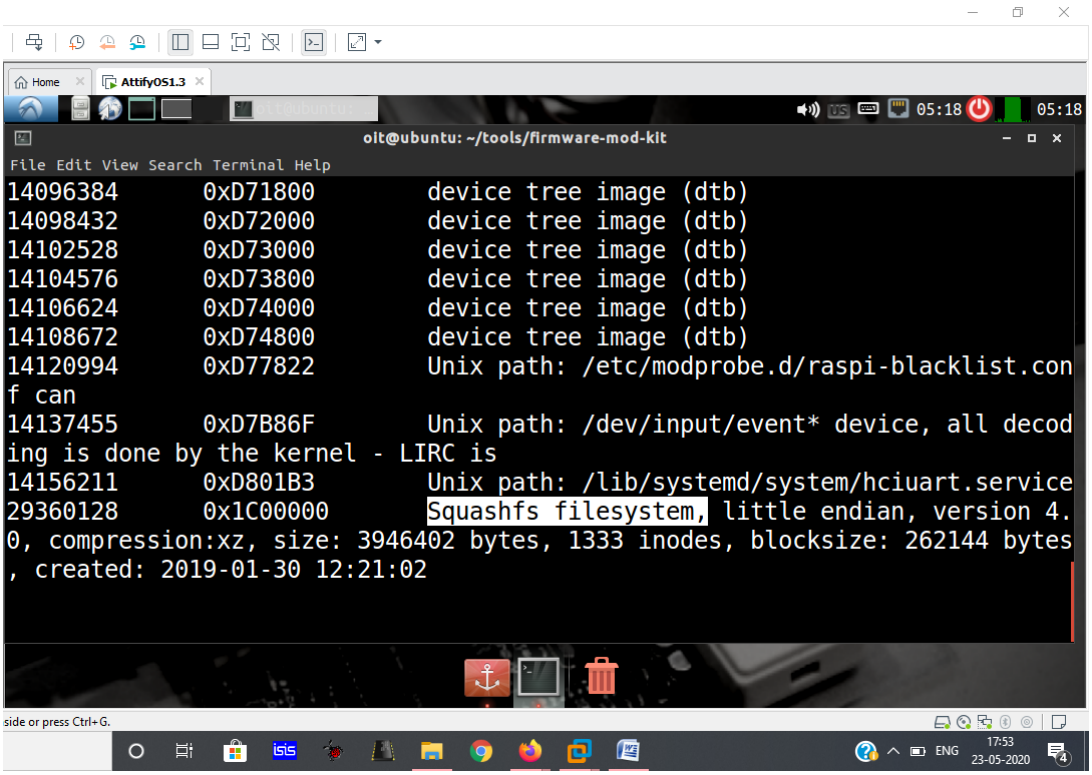
Steps involved :

1)Download the firmware that you want to analyse.

Download link: https://github.com/OWASP/IoTGoat/releases

2)Analyse the firware by using **binwalk tool**.

binwalk IoTGoat-raspberry-pi2.img

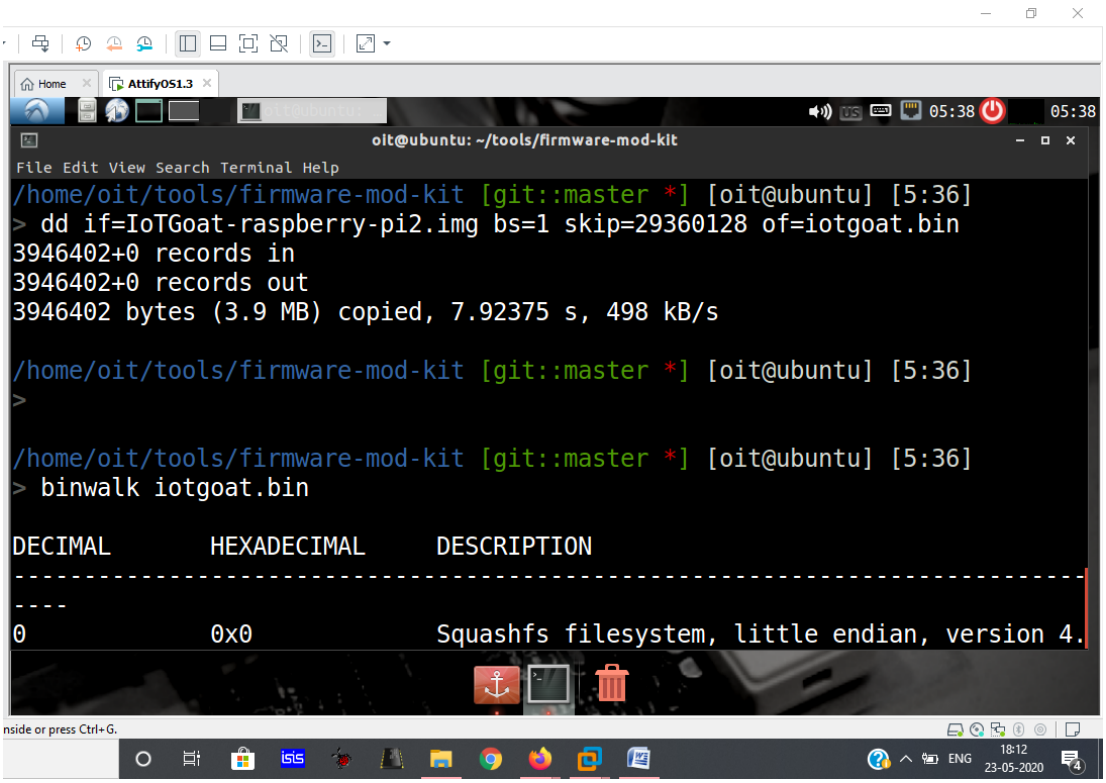


From here we come to know about

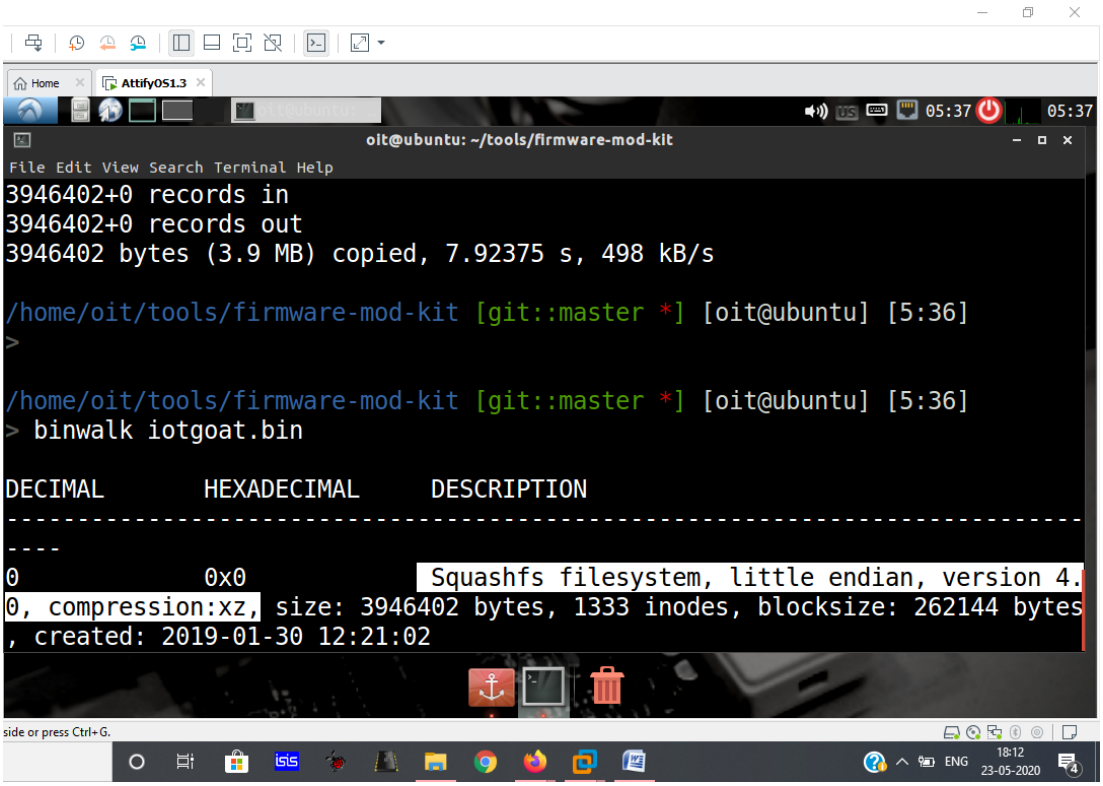
- filesystem - Squashfs
- compression – xz
- address – 29360128

3) We have seen in last step after how many offset it should start extracting i.e. 29360128

dd if=IoTGoat-raspberry-pi2.img bs=1 skip=29360128 of=iotgoat.bin

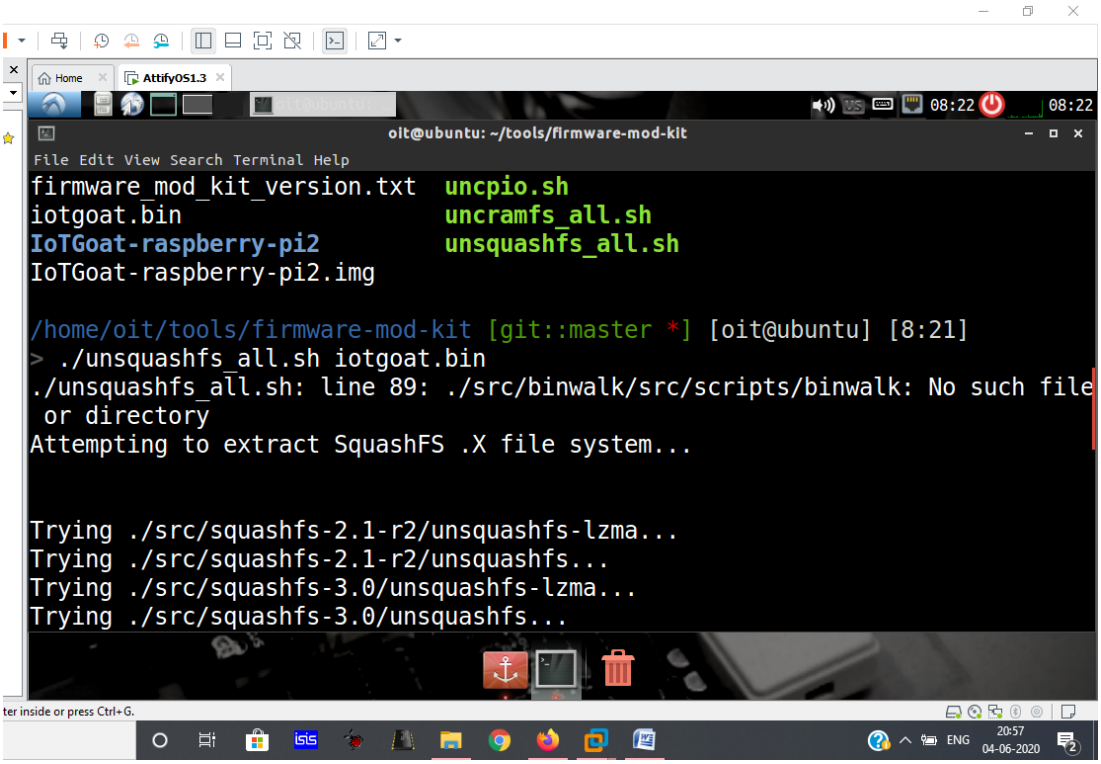


Now, check the output file

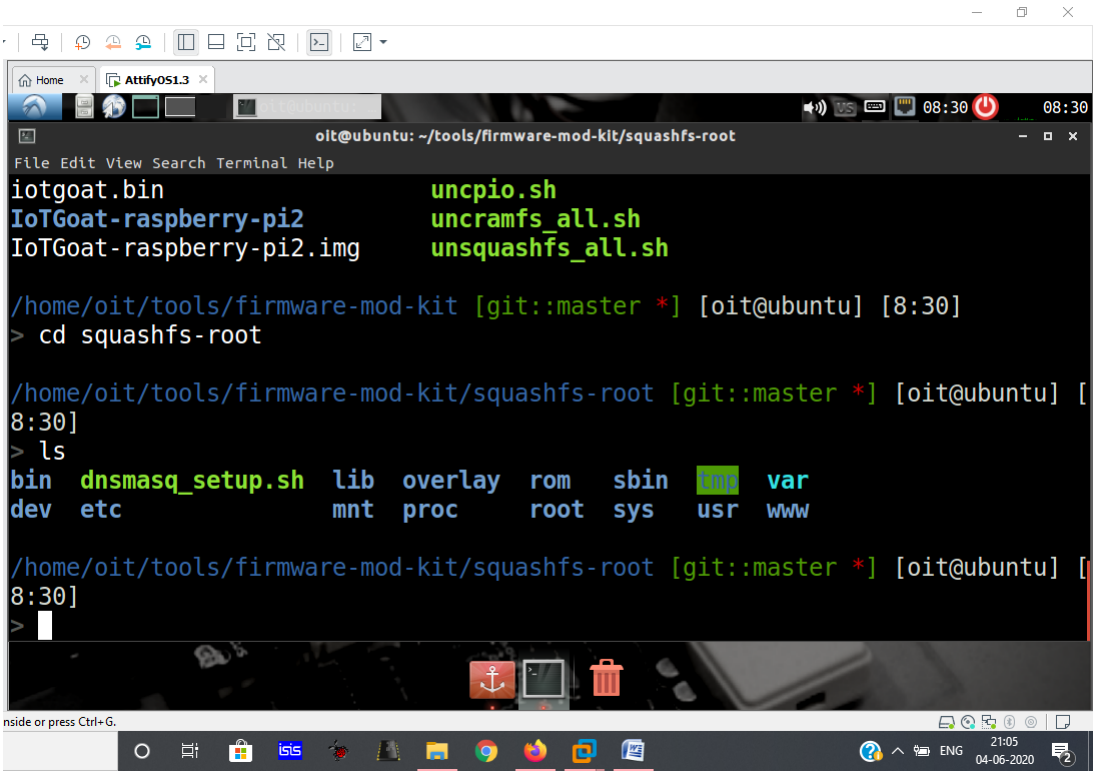


4) Now extract it using

unsquashfs_all.sh iotgoat.bin

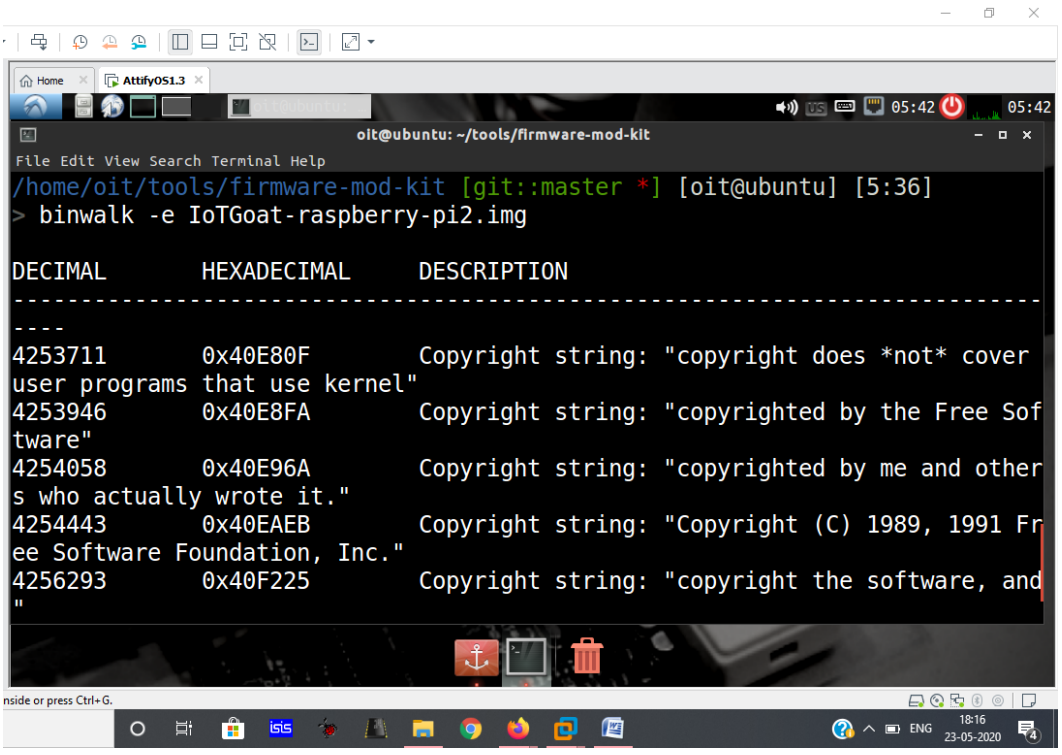


We see squashfs-root with all the root directory



5) Another way to extract this firmware is by using binwalk

binwalk -e IoTGoat-raspberry-pi2.img

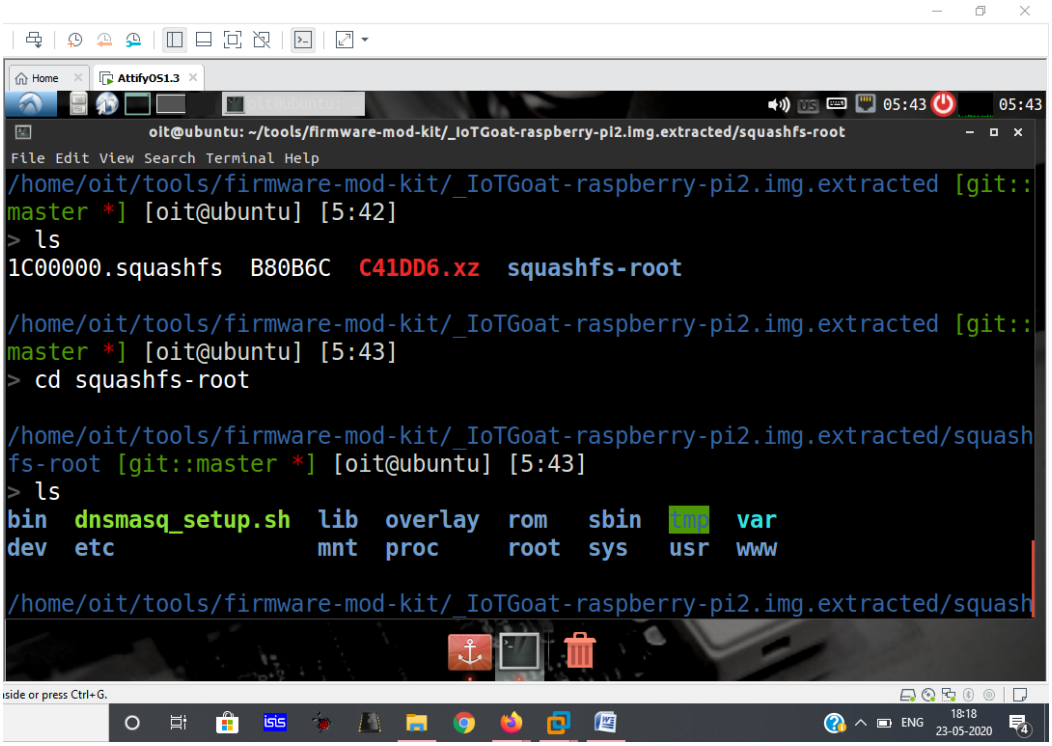


Now go to the extracted file, there we see squashfs-root folder inside which we get root folders of iotgoat firmware

cd _IoTGoat-raspberry-pi2.img.extracted

cd squashfs-root

ls



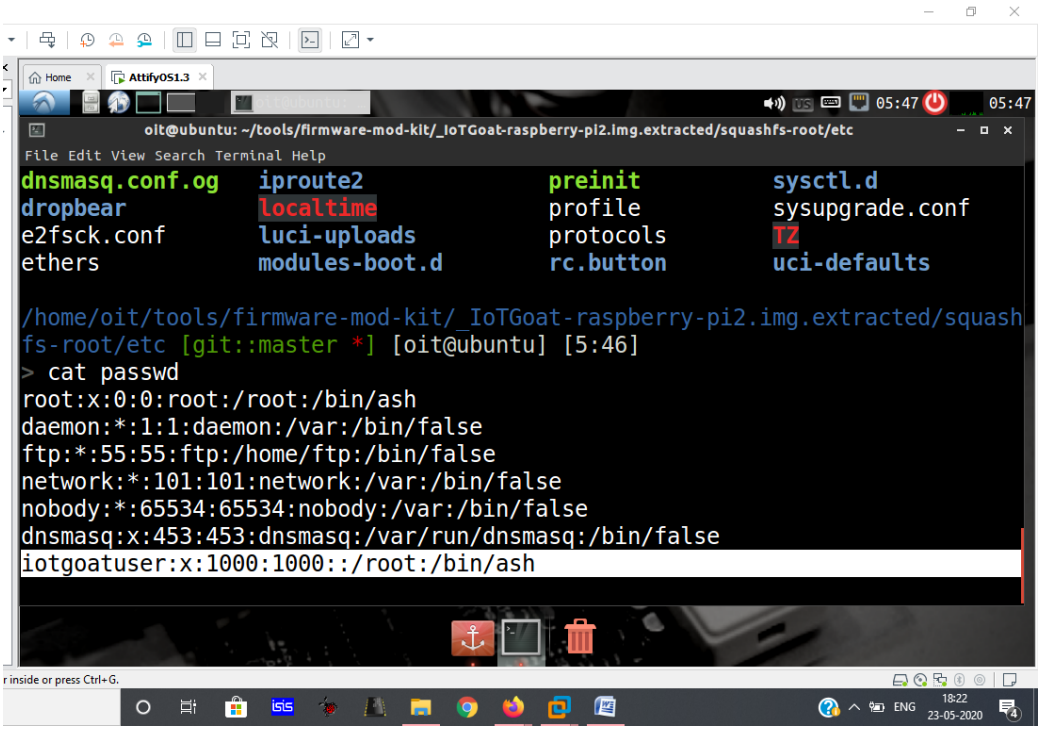
6) Once we are here lets search for some sensetive files.

Go to /etc folder there we see passwd and shadow file

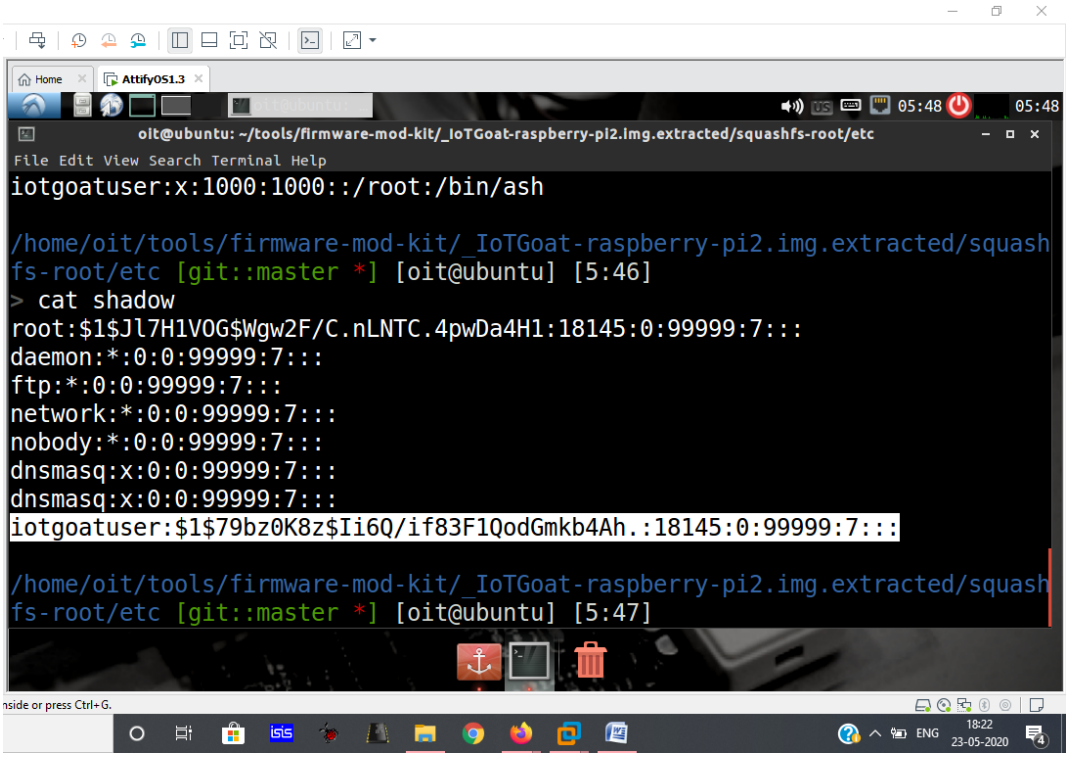
Let's find out what all we can do with that

cat passwd

Here we see a user named iotgoatuser, now lets check the shadow file



cat shadow

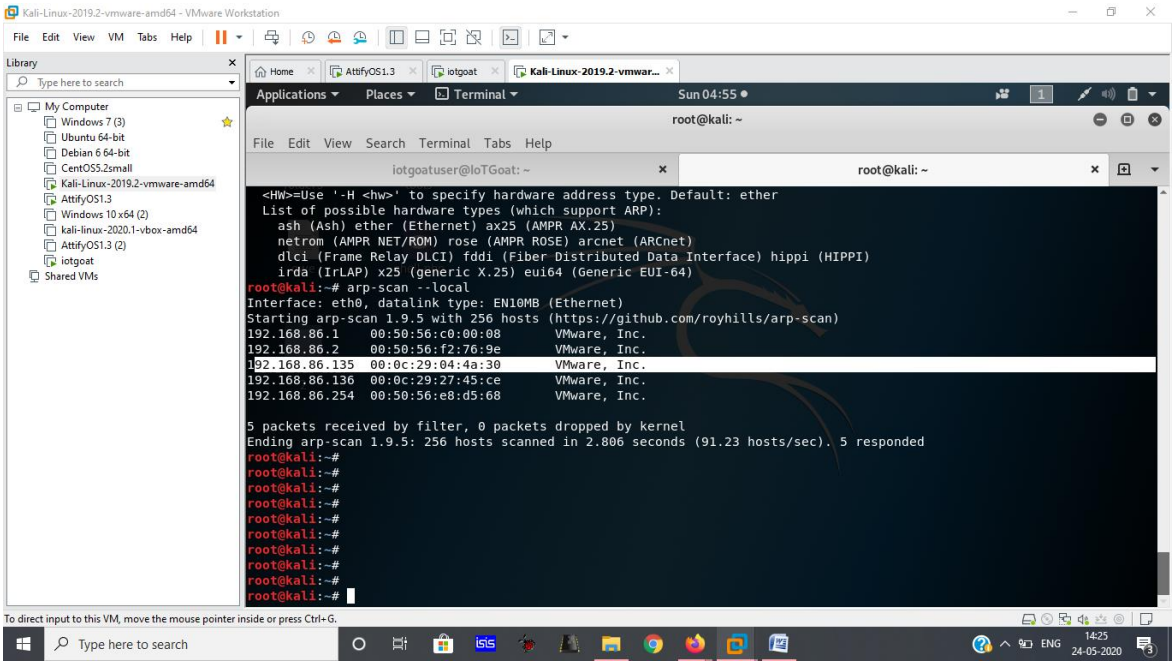


7) Download the IoTGoat vmdk file and run in Vmware

Download link : https://github.com/OWASP/IoTGoat/releases

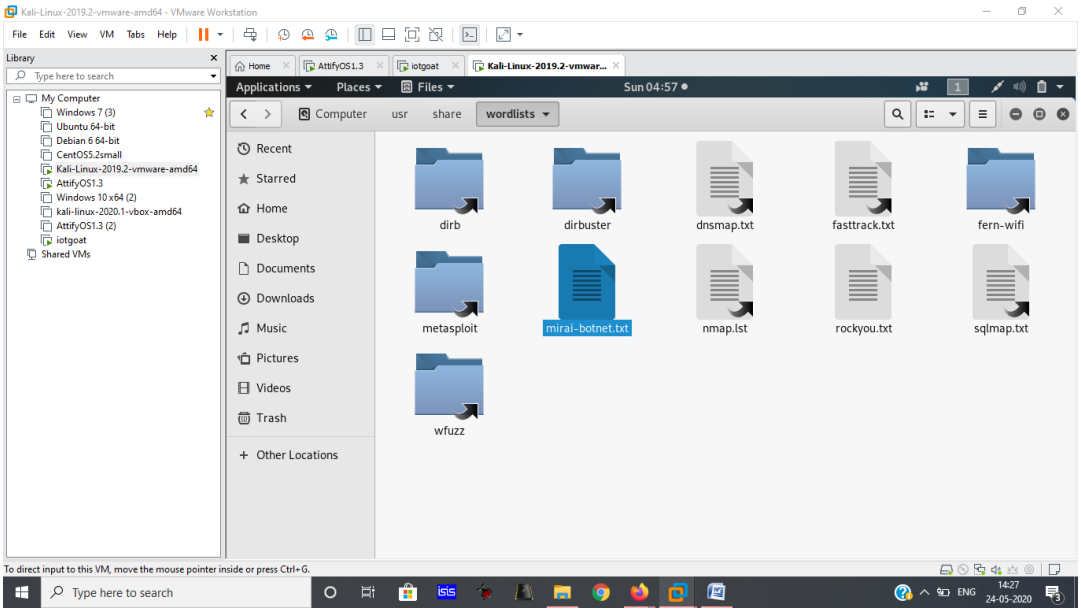
After running that vmdk, go to kali and search for the IP of IotGoat using

arp-scan --local



8) We alredy know the username i.e. iotgoatuser now to fetch the password of IoTGoat download the credential list file from the following link and save it in */usr/share/wordlists*

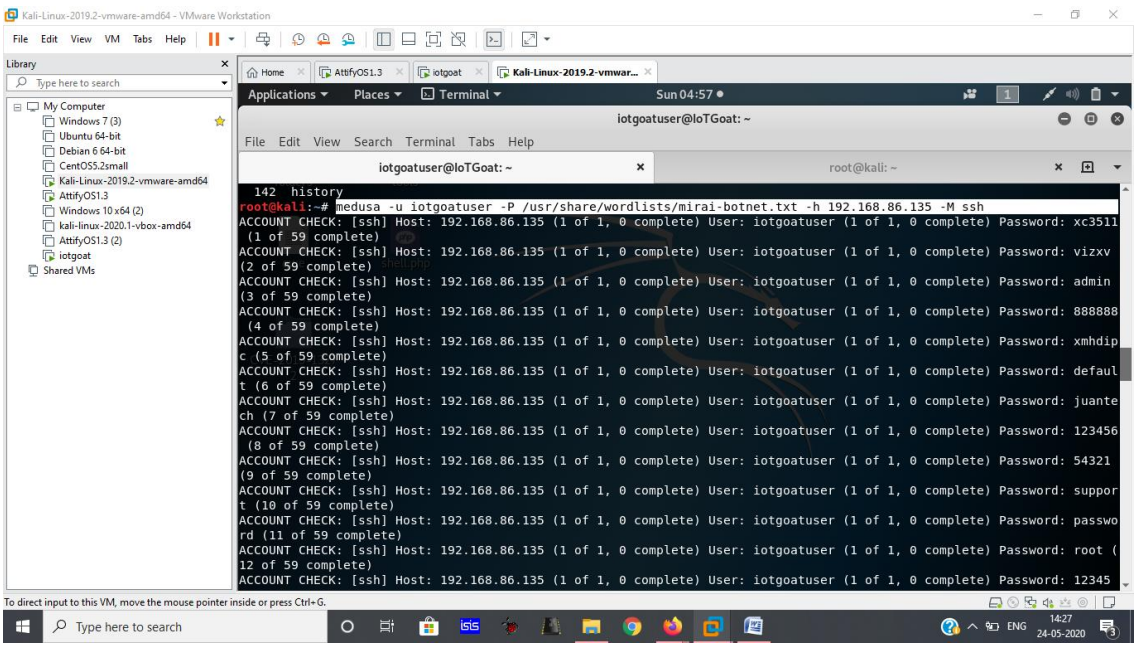
https://github.com/securing/mirai_credentials/blob/master/mirai_creds.txt



9) In order to bruteforce the password for the user iotgoatuser we can use hydra or medusa

I've used medusa for the following using the command

medusa –u iotgoatuser –P /usr/share/wordlists/mirai-botnet.txt –h <IoTGoat IP> -M ssh

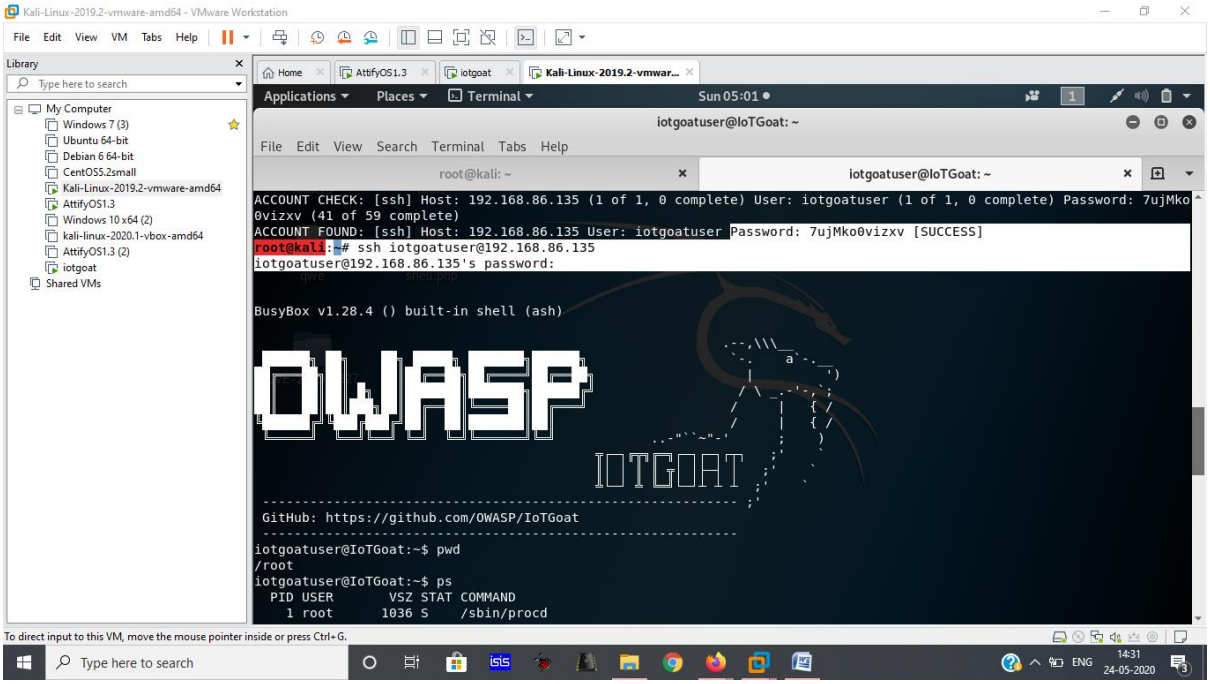


From here we got to know the password is **7ujMko0vizxv**

10)Now we can take ssh connecten of the machine using the command

ssh iotgoatuser@IP

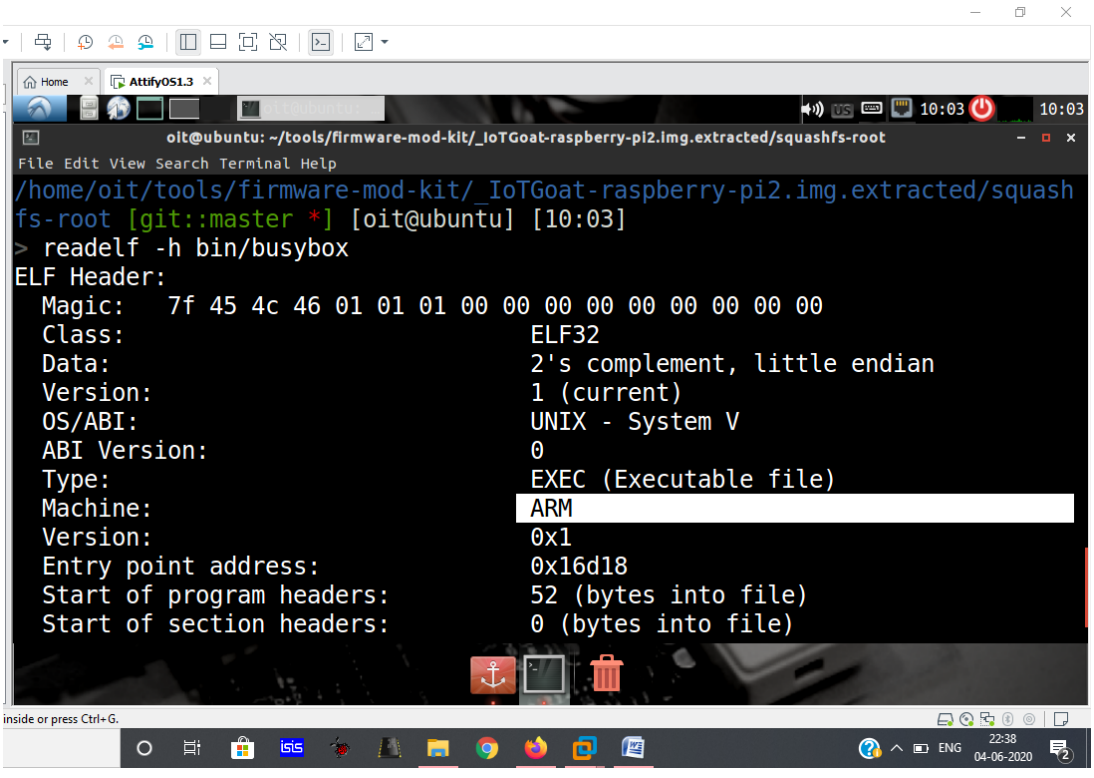
enter password in the next step and we will get the ssh connection of the machine



11) Let's get back to our attify OS and look for some juicy information.

For emulation find the architecture

Below we see that it is **ARM** architecture by *readelf –h bin/busybox*



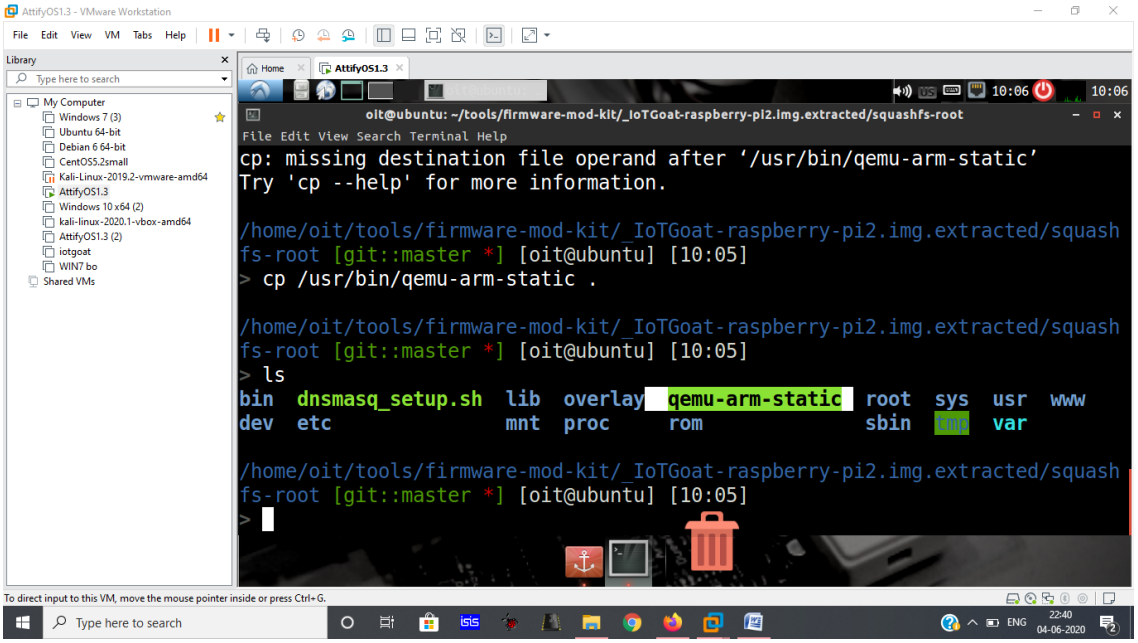
Now let's copy qemu for the ARM architecture

To see qemu for ARM path use

which qemu-arm-static

cp /usr/bim/qemu-arm-static .

ls

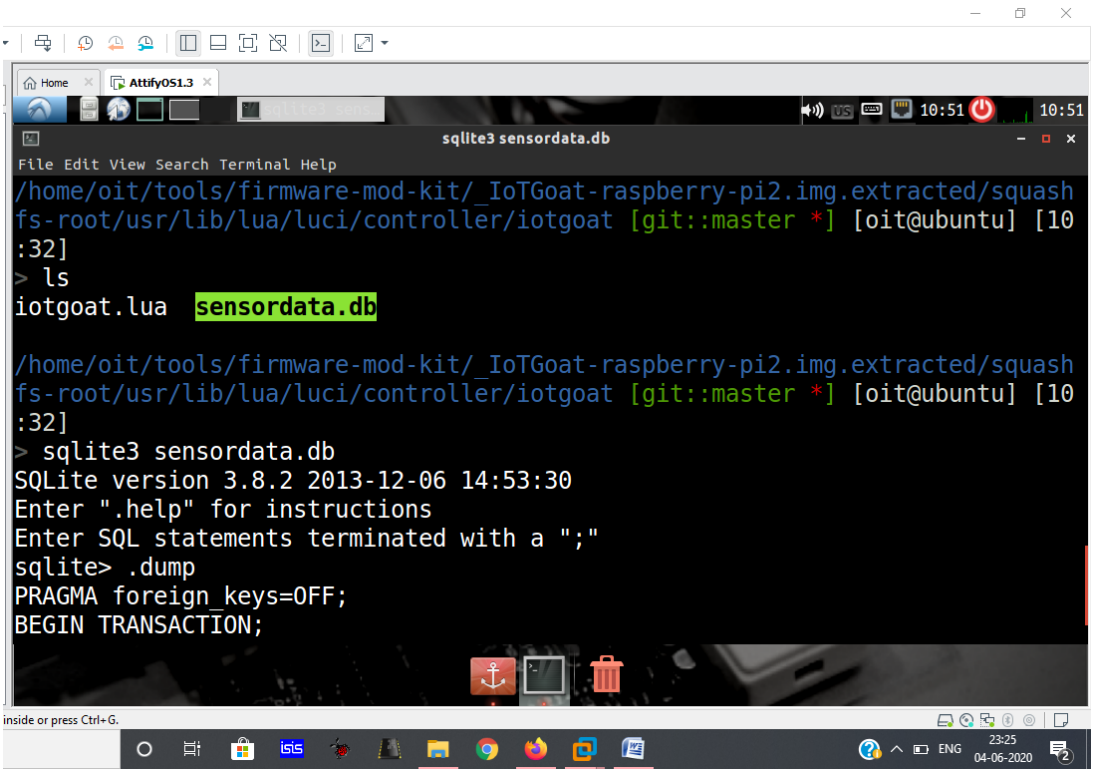


sudo chroot . ./qemu-arm-static ./bin/busybox

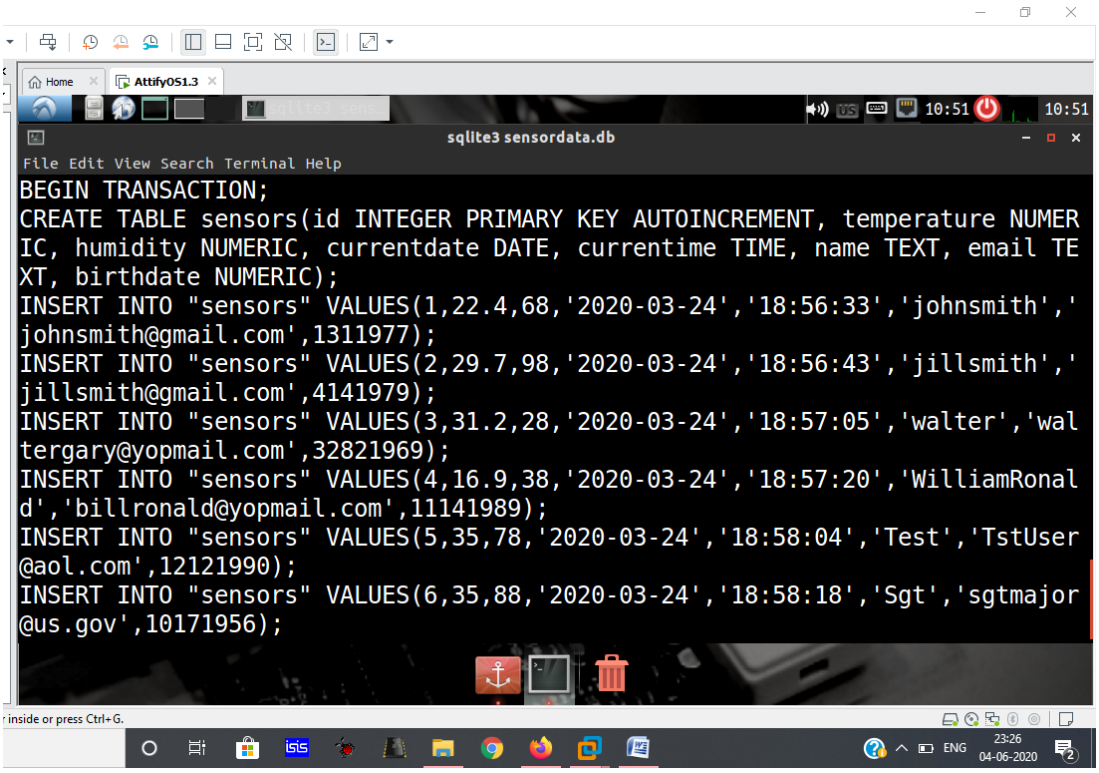
12)If we go to */home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs- root/usr/lib/lua/luci/controller/iotgoat*

We see a db file

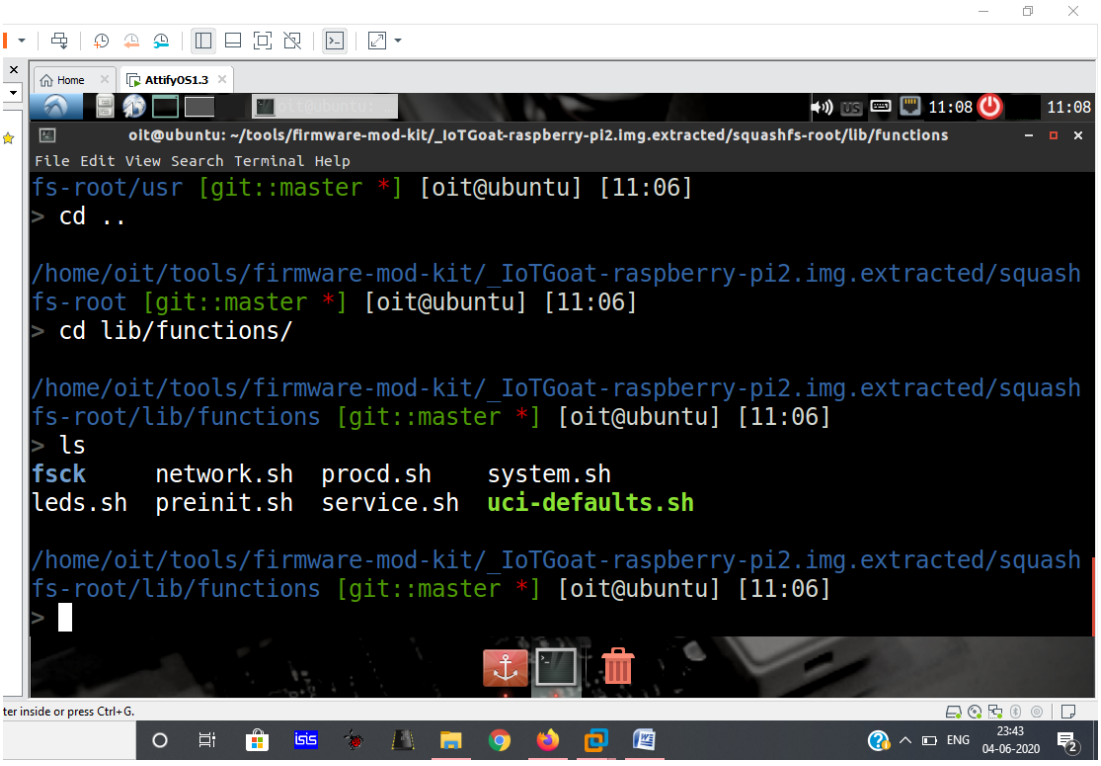
Let's open it by *sqlite3 sensordata.db*



We see plenty of email ID with birth date

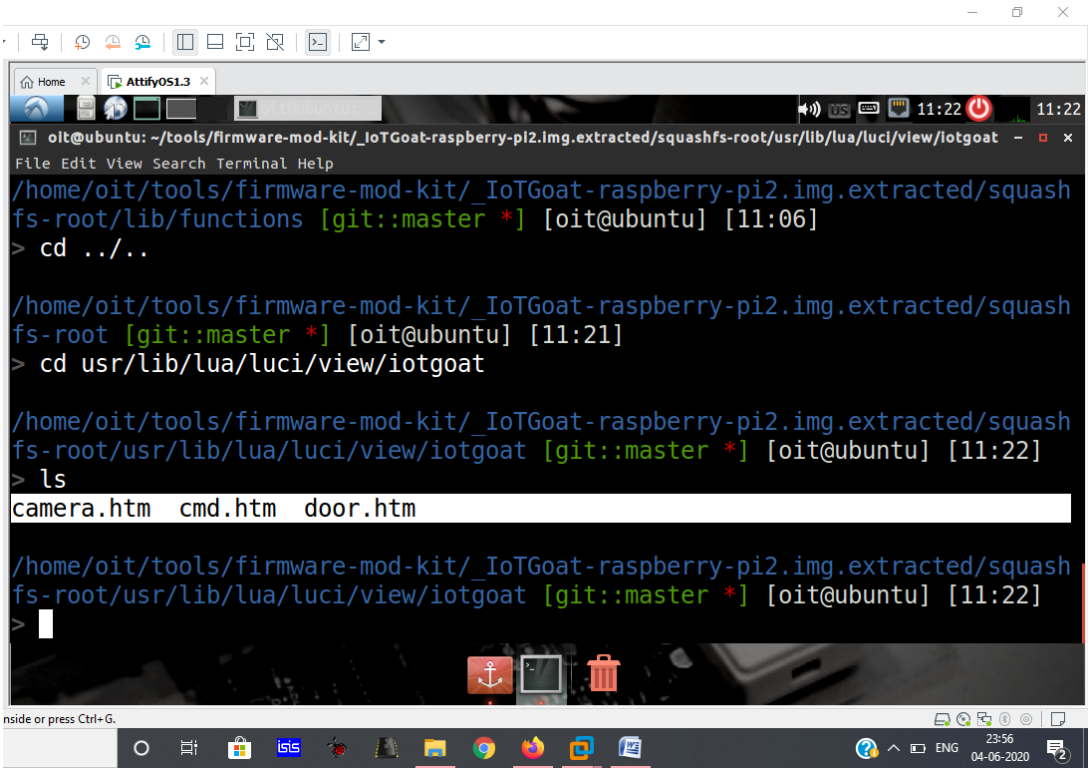


13)We also see various shell script files in /lib/functions

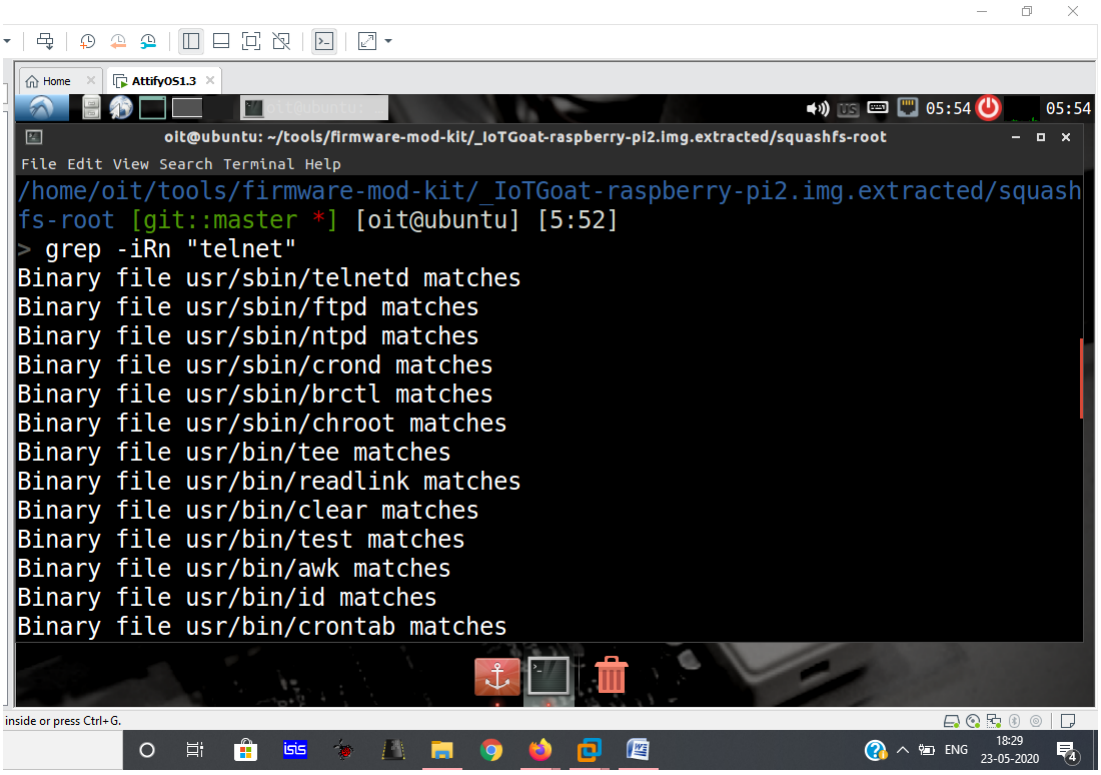


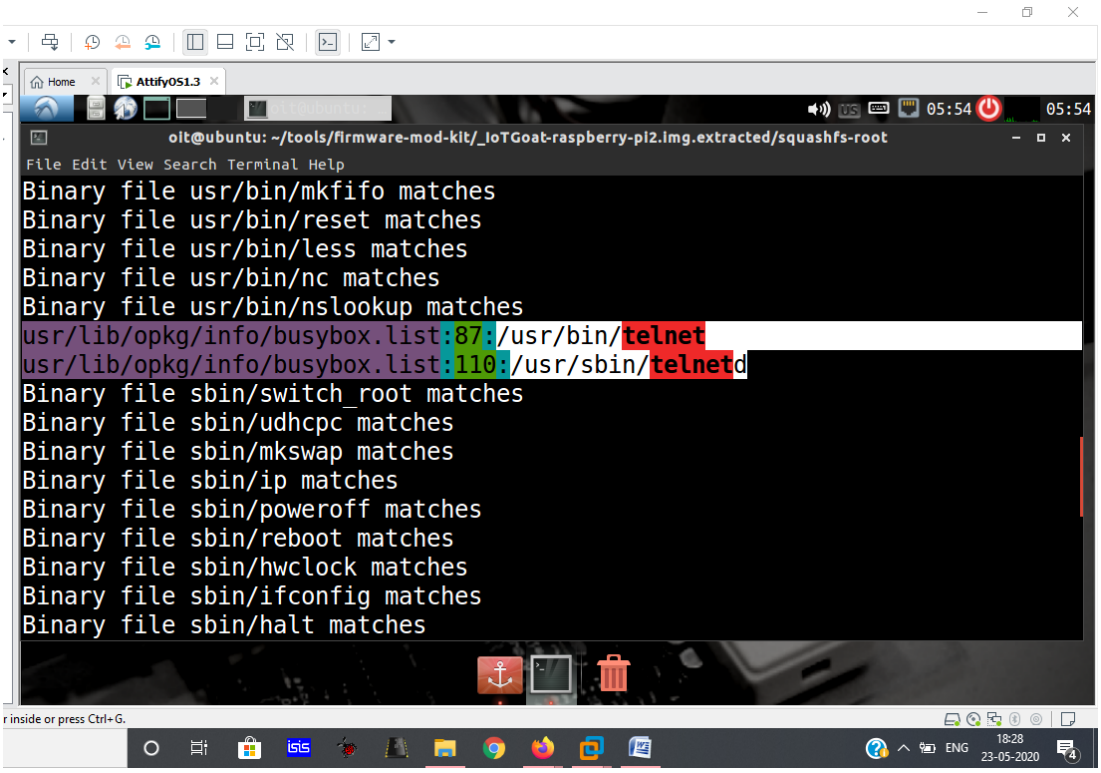
14)Go to */usr/lib/lua/luci/view/iotgoat*

We can directly access them on web UI of iotgoat



15) Grep telnet files we see telnet and telnetd in the following directories listed below

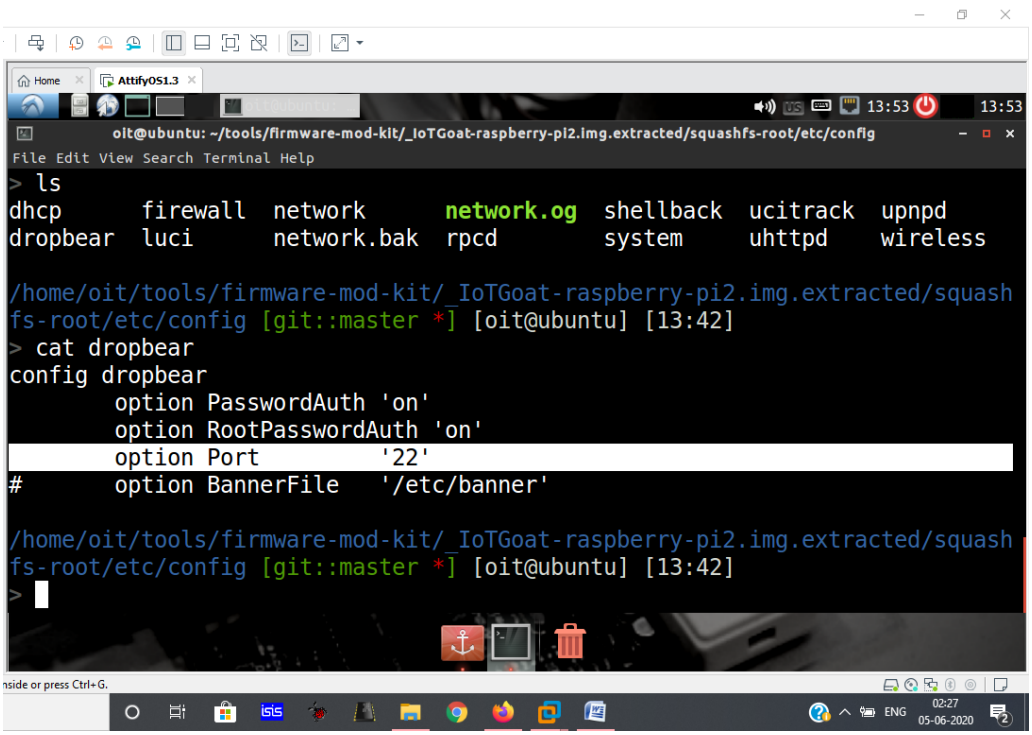




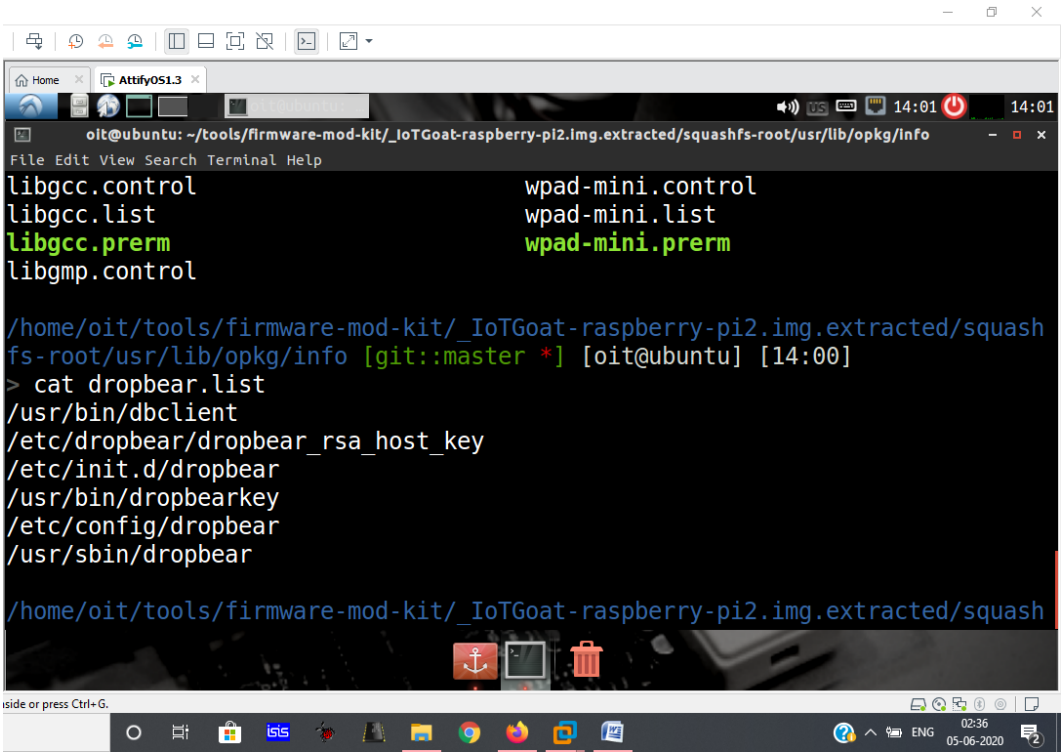
16)we also have dropbear port at 22

Drobear files are located at

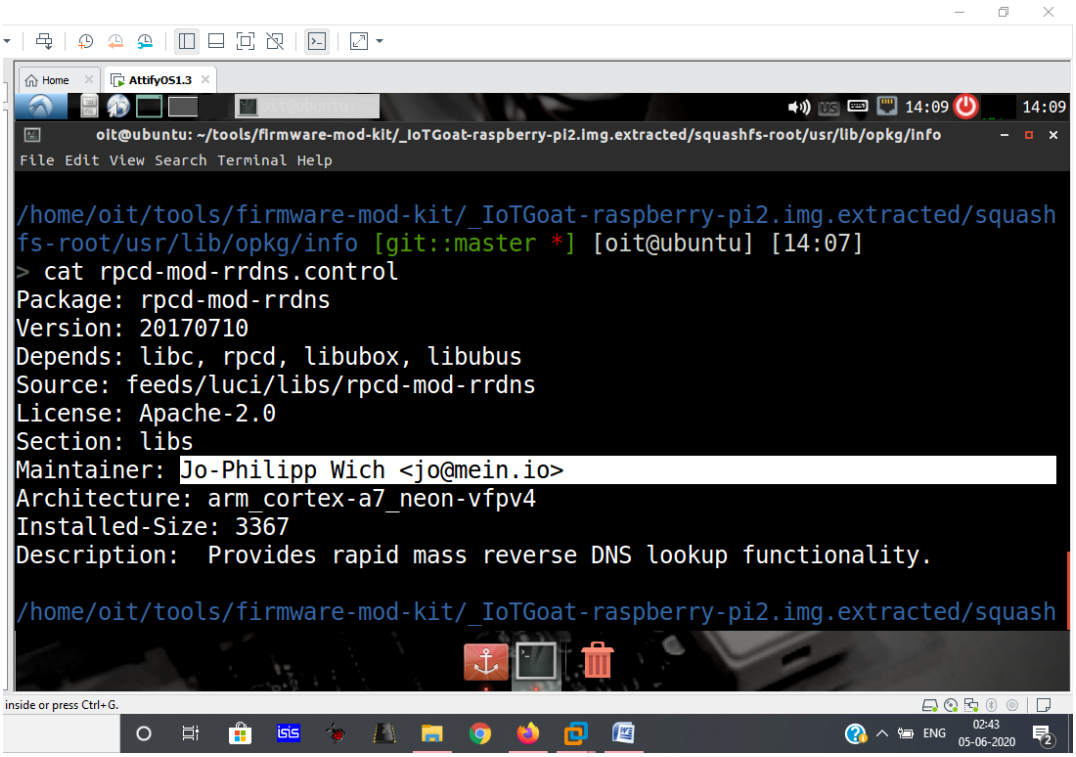
/usr/sbin/dropbear
/etc/config/dropbear
/etc/init.d/dropbear

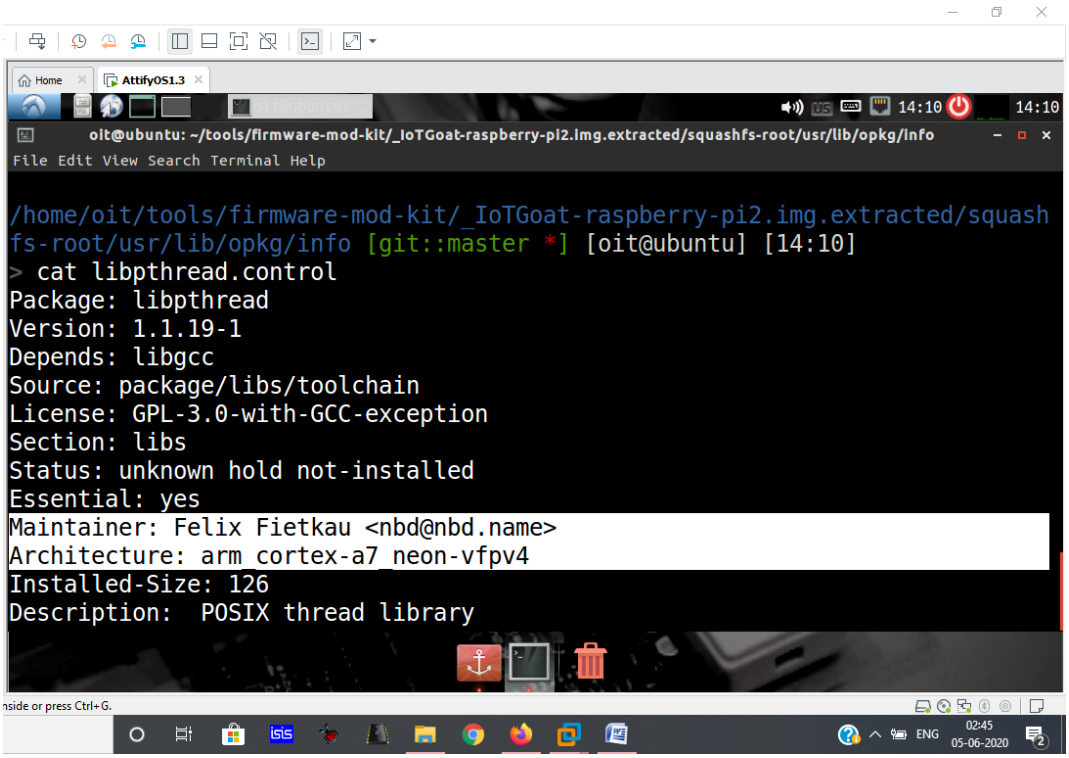


17)we can also get dropbear related files from dropbear.list



18)There were many files with email ID too, few are





There was so much of more information present in the firmware we can traverse through.