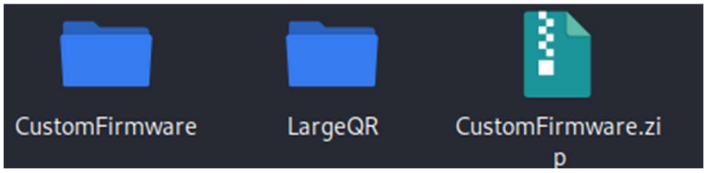
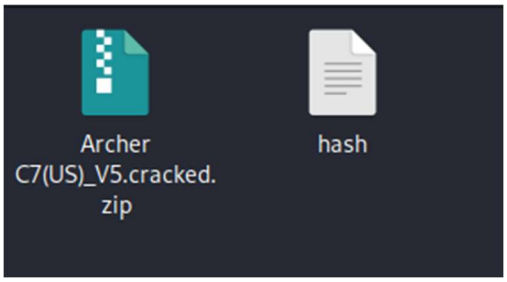
For this challenge you are given supposed cracked firmware from the dark web. This firmware is for the Archer C7 TP link router. Unzip the main firmware file:



Inside there is a hash and the actually firmware zip.



Inside that zip file there is the instructions to install the firmware, the .bin.tgz and a License.

```
'c7v5_us-up-ver1-2-1-P1[20220715-rel19099]_2022-07-15_17.44.43.bin.tgz'
'GPL License Terms.pdf'
'How to upgrade TP-Link Wireless Router.pdf'
```

Gunzip the main binary:

```
└─$ ls
13409.7z  5B00.7z  EFCA47  filesystem.squashfs
```

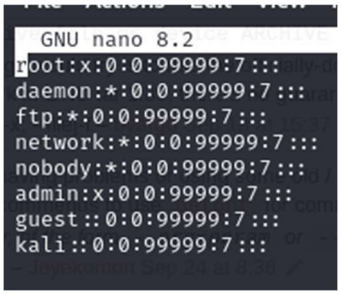
There is a couple binary 7zip files, a binary file, and the squash filesystem. The Squash FS is what was messed with and changed. In a real cracked firmware, they might also edit and change the binaries. So to proceed unsquash the filesystem.

```
┌──(andrew㉿kali)-[~/Documents/Malasia CTF/CustomFirmware/Archer C7(US)_V5.0_220715/_c7v5_us-up-ver1-2-1-P
1[20220715-rel19099]_2022-07-15_17.44.43.bin.extracted]
└─$ unsquashfs filesystem.squashfs
Parallel unsquashfs: Using 8 processors
2395 inodes (2302 blocks) to write

[==========================================================================================] 4697/4697 100%

created 2091 files
created 209 directories
created 304 symlinks
created 0 devices
created 0 fifos
created 0 sockets
created 0 hardlinks

┌──(andrew㉿kali)-[~/Documents/Malasia CTF/CustomFirmware/Archer C7(US)_V5.0_220715/_c7v5_us-up-ver1-2-1-P
1[20220715-rel19099]_2022-07-15_17.44.43.bin.extracted]
└─$ ls
13409.7z  5B00.7z  EFCA47  filesystem.squashfs  squashfs-root
```

As you can see it is a full filesystem for the Linux kernel:

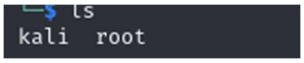
```
┌──(andrew㉿kali)-[~/Documents/Malasia CTF/CustomFirmware/Archer C7(US)_V5.0_220715/_c
1[20220715-rel19099]_2022-07-15_17.44.43.bin.extracted/squashfs-root]
└─$ ls
bin  dev  etc  lib  mnt  overlay  proc  rom  root  sbin  sys  tmp  usr  var  www
```

Etc, bin, var, and www are the most important areas to investigate. These are easy to tamper with and corrupt. If you go into etc and look at passwd and shadow, you see a user kali was added.



It was also given the same privilege as root which is suggestive of a malicious user. Next, I file that is good to check is crontab. This can be used for the attacker to gain persistence when the router is restarted.

Ther are two crontabs. Root and kali:



The root crontab is empty but kali has a malicious cron job.

This is the IP for the first flag. Some other things that could be edited are etc/hosts and etc/banner. That is out of scope of this ctf though. If we look in the www directory, we can find the webpage that launches when you setup the router.

If you look into the index.html you can see that there is a malicious website redirection.

Those should be the three flags in the CTF