CHALLENGE DESCRIPTION

In the dust and sand surrounding the vault, you unearth a rusty PCB... You try to read the etched print, it says Open..W...RT, a router! You hand it over to the hardware gurus and to their surprise the ROM Chip is intact! They manage to read the data off the tarnished silicon and they give you back a firmware image. It's now your job to examine the firmware and maybe recover some useful information that will be important for unlocking and bypassing some of the vault's countermeasures!

Once we download the .zip file from hackthebox we must unzip it with the given password in hackthebox.

Its .bin file ,that's mean it's a firmware image .

Lets try binwalk -e <filename> to extract files within the firmware image , and there is the result .

```
—$ ls
18168C  18168C.7z  42C2C8.squashfs  70000  7C0000.jffs2  jffs2-root  squashfs-root  squashfs-root-0
```

Now lets connect to the address given by hackthebox :

$ nc ip address port

First question : What version of OpenWRT runs on the router (ex: 21.02.0)

The OpenWRT is a linux based operating system , generally used for embedded device, particularly routers.

The version of OpenWRT can be found in " /etc/openwrt_release " file .

Let's move to the squashfs-root folder .

I found the etc directory , so I open it and I found the openwrt_release file .

```
DISTRIB_ID='OpenWrt'
DISTRIB_RELEASE='23.05.0'
DISTRIB_REVISION='r23497-6637af95aa'
DISTRIB_TARGET='ramips/mt7621'
DISTRIB_ARCH='mipsel_24kc'
DISTRIB_DESCRIPTION='OpenWrt 23.05.0 r23497-6637af95aa'
DISTRIB_TAINTS=''
```

The version is 23.05.0

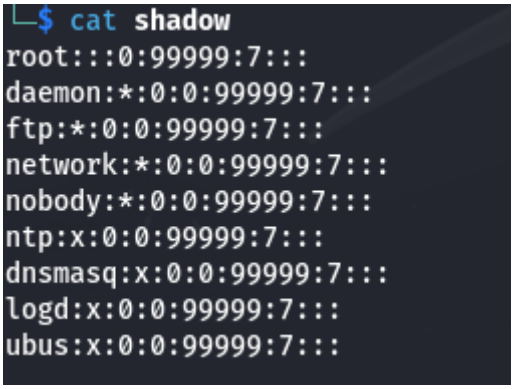
Next question : What is the Linux kernel version (ex: 5.4.143)

I found it when with strings command applied on chal_router_dump.bin , it is "5.15.134"

Next question : What's the hash of the root account's password, enter the whole line (ex: root:2JgiaOAai....)

Generally , this information can be found in the etc/shadow file .

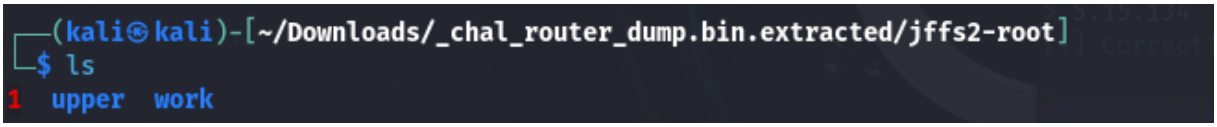
So let's open this file :



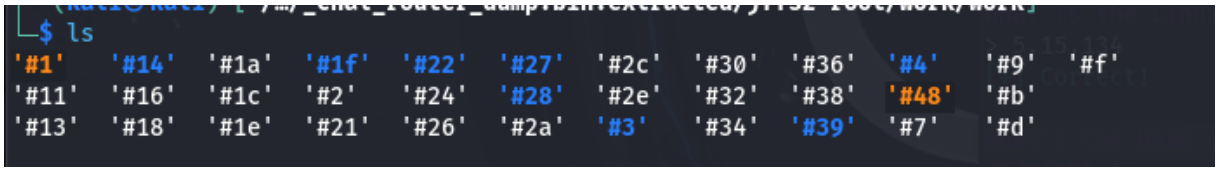
There is something wrong , there is no password for the root user , anyway lets try it .

Haha expected , its wrong answer .

When we extract the firmware file we found also jfss2-root directory , lets investigate it .



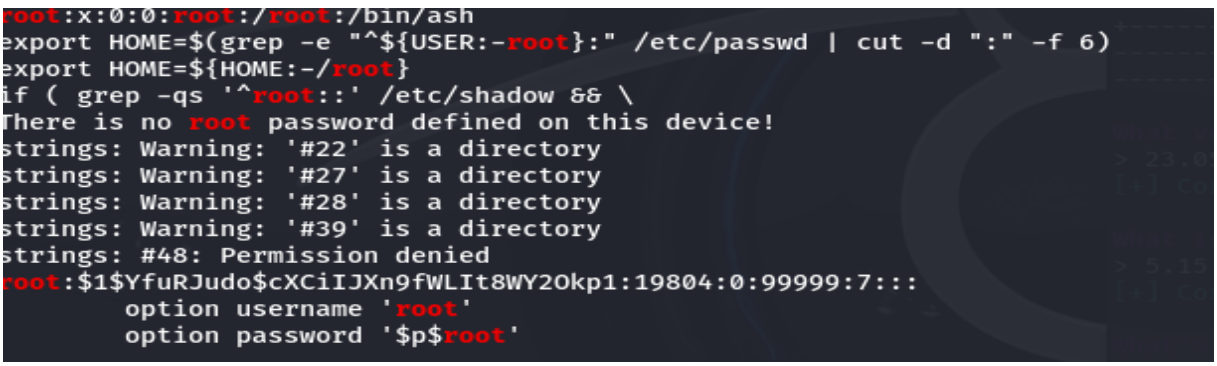
Change directory to work .



There is a huge number of files and folders .

The first thing that comes to my mind is "strings * | grep root " and searching if there is something readable .

There is something guys 😉, I think it's the correct answer .



Next question : What is the PPPoE username

PPPoE (Point-to-Point Protocol over Ethernet) in OpenWRT is a network protocol that encapsulates PPP frames inside Ethernet frames.

The information about PPPoE can be found in etc/config/network .

Lets look at upper directory .

There is a .gzip file ,unzip it , another .tar file comes, unzip it (tar -xvf filename.tar)

Cat etc/config/ network :

```
config interface 'wan'
        option device 'wan'
        option proto 'pppoe'
        option username 'yohZ5ah'
        option password 'ae-h+i$i^Ngohroorie!bieng6kee7oh'
        option ipv6 'auto'

config interface 'wan6'
```

Username : yohZ5ah

Next question : the password :

In the screenshot above

Next question : What is the WiFi SSID :

I found it in etc/config/wireless file :

```
config wifi-iface 'default_radio1'
        option device 'radio1'
        option network 'lan'
        option mode 'ap'
        option ssid 'VLT-AP01'
        option encryption 'sae-mixed'
        option key 'french-halves-vehicular-favorable'
        option ieee80211r '1'
        option ft_over_ds '0'
        option wpa_disable_eapol_key_retries '1'
```

“VLT-AP01”

Next question : the password:

In the screenshot above

Next question : What are the 3 WAN ports that redirect traffic from WAN -> LAN (numerically sorted, comma sperated: 1488,8441,19990)

We can find This information in etc/config/firewall file .

1778,2289,8088

And we get the flag .