Mirai walkthrough

Index

List of pictures

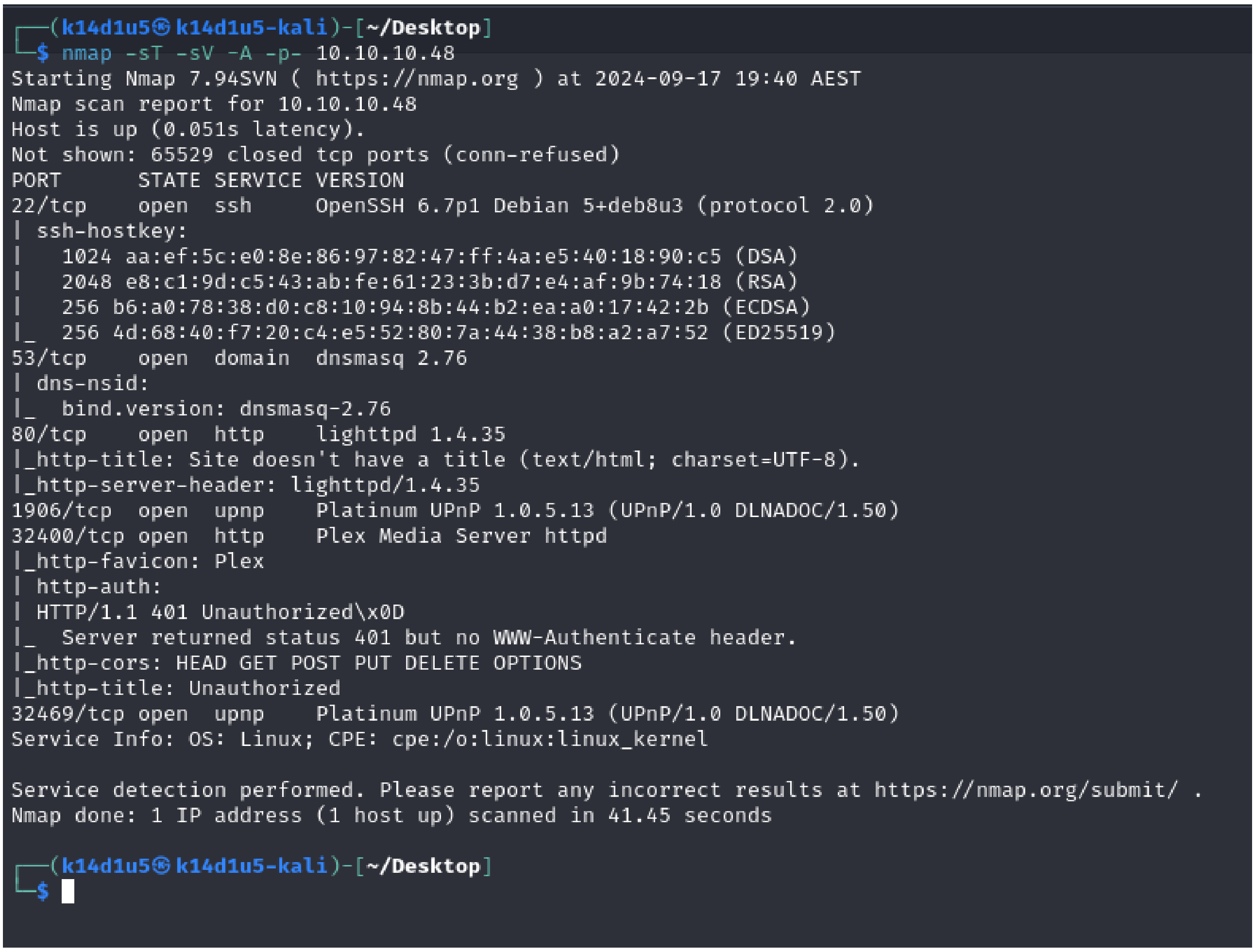
Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who're willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Just as note: I am not an English native person, so sorry if I did some grammatical and syntax mistakes.

Reconnaissance

The results of an initial nMap scan are the following:



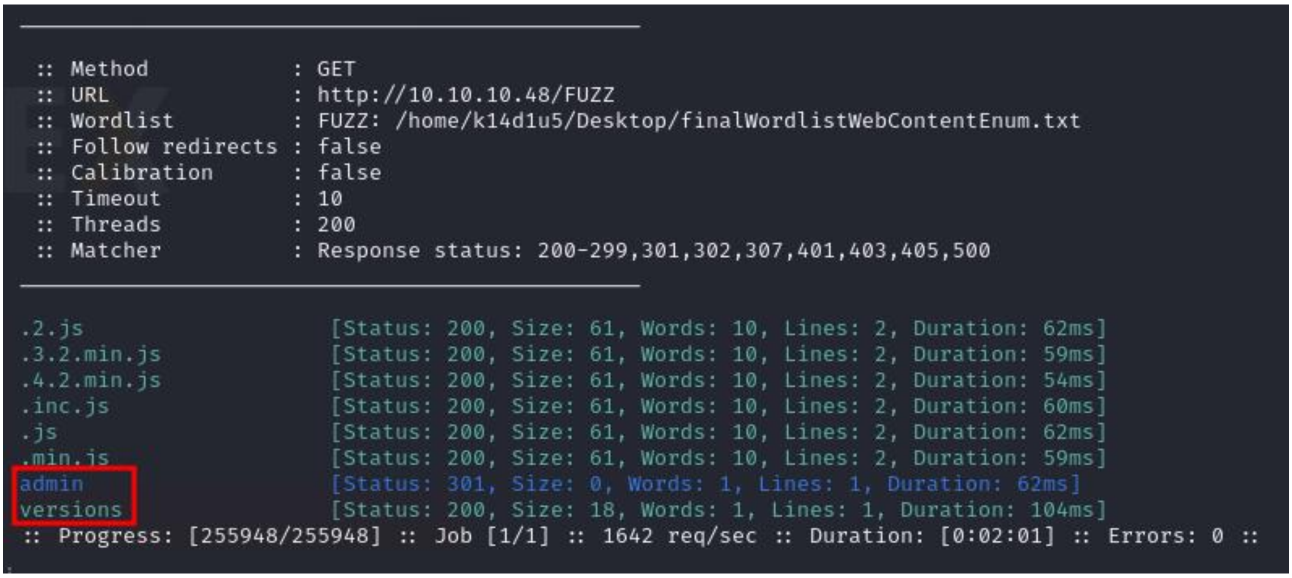
```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ nmap -sT -sV -A -p- 10.10.10.48
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 19:40 AEST
Nmap scan report for 10.10.10.48
Host is up (0.051s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 aa:ef:5c:e0:8e:86:97:82:47:ff:4a:e5:40:18:90:c5 (DSA)
|   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
|   256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
|_  256 4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (ED25519)
53/tcp    open  domain  dnsmasq 2.76
| dns-nsid:
|_  bind.version: dnsmasq-2.76
80/tcp    open  http    lighttpd 1.4.35
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: lighttpd/1.4.35
1906/tcp  open  upnp    Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
32400/tcp open  http    Plex Media Server httpd
|_http-favicon: Plex
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
|_http-cors: HEAD GET POST PUT DELETE OPTIONS
|_http-title: Unauthorized
32469/tcp open  upnp    Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.45 seconds

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ 
```

Figure 1 - nMap scan results

Open ports are 22, 53, 80, 1906, 32400 and 32469. NMap identified SSH service on port 22, DNS service on port 53, a web application server on port 80, Platinum UPnP service on ports 1906 and 32469 and Plex media server service on port 32400. Also, nMap identified Linux as system operating, but it didn't provide more details about it.

Initial foothold

The first thing I did was trying to access to web application server and Plex Media Server services I found via browser. The web application running on port 80 has a blank page. The Plex service required credentials to log in. At this point I started to search some hidden content on web application running on port 80, using ffuf tool:



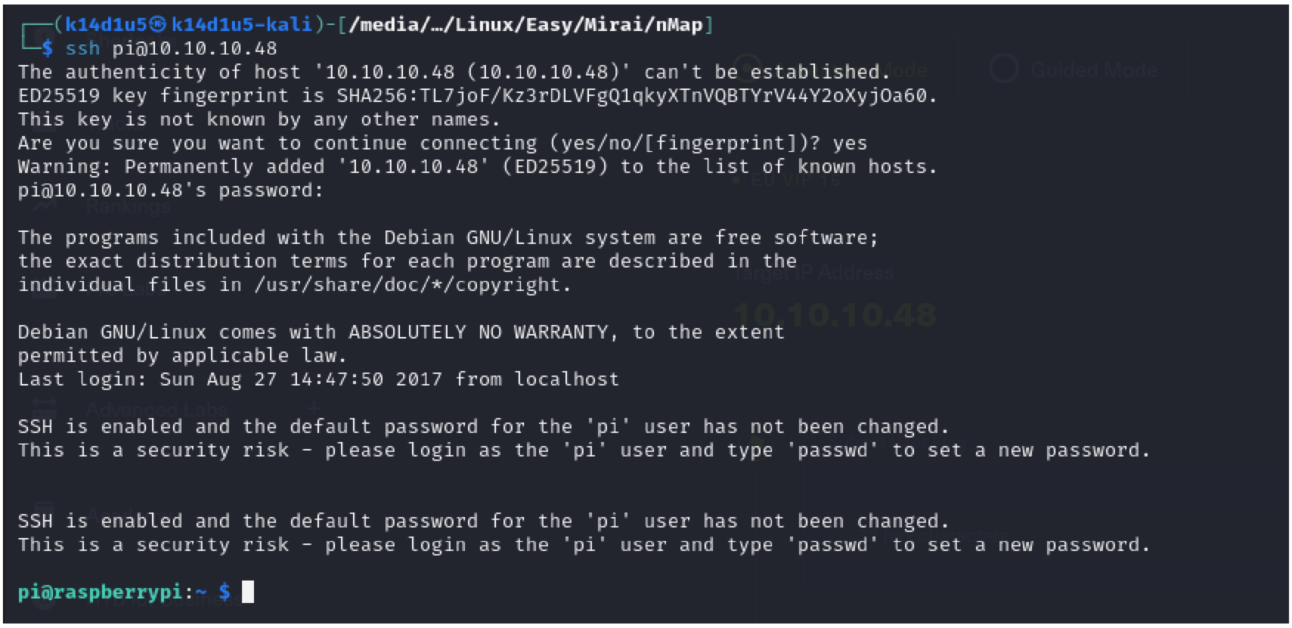
```
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.48/FUZZ
 :: Wordlist         : FUZZ: /home/k14d1u5/Desktop/finalWordlistWebContentEnum.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.2.js                   [Status: 200, Size: 61, Words: 10, Lines: 2, Duration: 62ms]
.3.2.min.js             [Status: 200, Size: 61, Words: 10, Lines: 2, Duration: 59ms]
.4.2.min.js             [Status: 200, Size: 61, Words: 10, Lines: 2, Duration: 54ms]
.inc.js                 [Status: 200, Size: 61, Words: 10, Lines: 2, Duration: 60ms]
.js                     [Status: 200, Size: 61, Words: 10, Lines: 2, Duration: 62ms]
.min.js                 [Status: 200, Size: 61, Words: 10, Lines: 2, Duration: 59ms]
admin                   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 62ms]
versions                [Status: 200, Size: 18, Words: 1, Lines: 1, Duration: 104ms]
:: Progress: [255948/255948] :: Job [1/1] :: 1642 req/sec :: Duration: [0:02:01] :: Errors: 0 ::
```

Figure 2 - ffuf scan results

I founded the admin and versions path. The latter one allowed me to download a file which contains versions numbers. The former one allowed me to access to a new dashboard.

User flag

On the admin dashboard I found out that the application running there was **Pi-hole**. Looking for it on the Internet, I learnt this application has a distribution for Raspberry devices. At this point, I kept to search some interesting information on the target. For example, I tried to analyzing the DNS service. It let me to find a new domain. I added this domain to the $/etc/hosts$ file on my Kali and I browsed to it. However, it informed me that the navigation is blocked. Also, I found some interesting CVEs, but any of them fitted to this box scenario, at this stage at least. After a lot of time, I tried to use the Raspberry default credential on the login pages. However, them doesn't work. So, my last chance and idea was to try these credentials to log in via SSH:



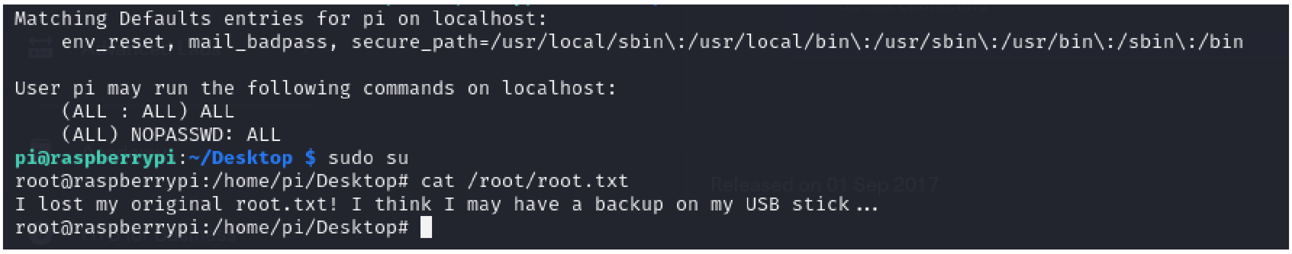
```
┌──(k14d1u5㉿k14d1u5-kali)-[/media/…/Linux/Easy/Mirai/nMap]
└─$ ssh pi@10.10.10.48
The authenticity of host '10.10.10.48 (10.10.10.48)' can't be established.
ED25519 key fingerprint is SHA256:TL7joF/Kz3rDLVFgQ1qkyXTnVQBTYrV44Y2oXyjOa60.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.48' (ED25519) to the list of known hosts.
pi@10.10.10.48's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 27 14:47:50 2017 from localhost

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.


SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi:~ $ 
```

Figure 3 - SSH login

I was very surprised that them worked. Anyway, I am on the target machine and more surprising, this user has the user flag I retrieved (I forgot a screenshot about the user flag).

Privilege escalation

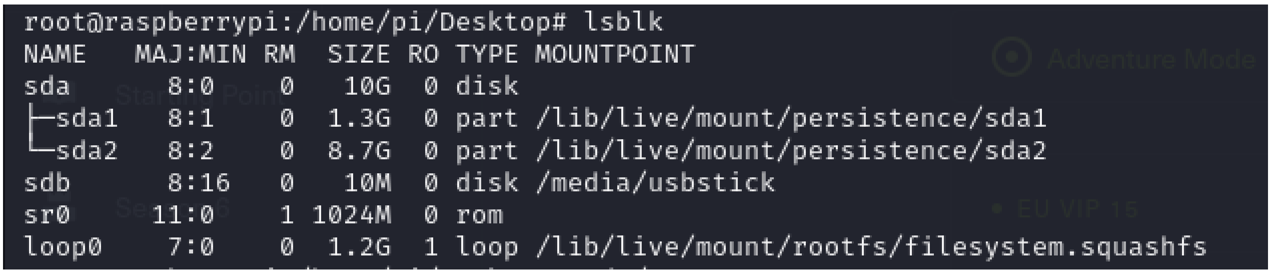
At this point I need to escalate my privileges. The first thing I usually check are the sudoers. It was incredible that this was the right way to escalate privileges. In fact, the pi user had the following configuration:



```
Matching Defaults entries for pi on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User pi may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
pi@raspberrypi:~/Desktop $ sudo su
root@raspberrypi:/home/pi/Desktop# cat /root/root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
root@raspberrypi:/home/pi/Desktop# 
```

Figure 4 - Privilege escalation

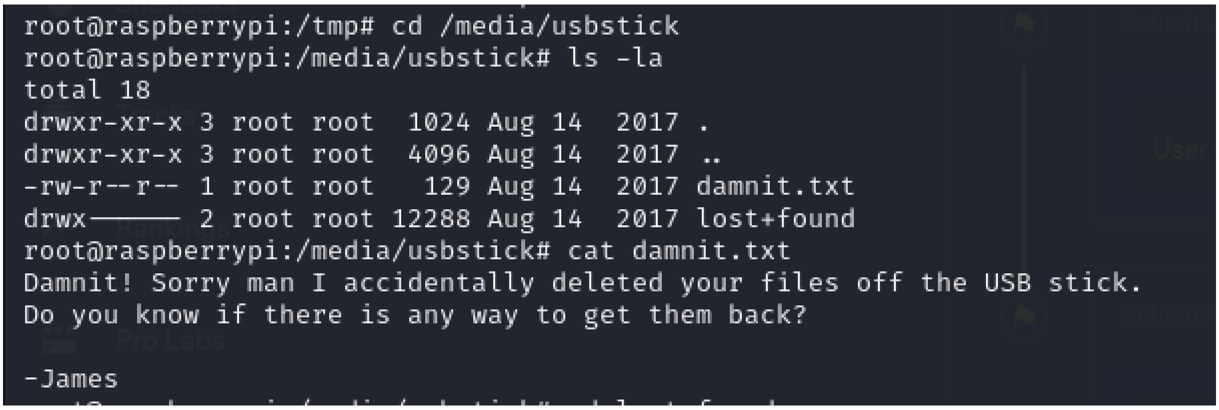
As you can see in the previous picture, I just needed to run the *sudo su* command to became root. However, I was not able to retrieve the root flag yet. The root.txt existed, but it informed me that the file was deleted and can exist a copy on a USB stick. Due to this clue, I checked the devices mounted:



```
root@raspberrypi:/home/pi/Desktop# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   10G  0 disk
├─sda1   8:1    0  1.3G  0 part /lib/live/mount/persistence/sda1
└─sda2   8:2    0  8.7G  0 part /lib/live/mount/persistence/sda2
sdb      8:16   0   10M  0 disk /media/usbstick
sr0     11:0    1 1024M  0 rom
loop0    7:0    0  1.2G  1 loop /lib/live/mount/rootfs/filesystem.squashfs
```

Figure 5 - Devices mounted

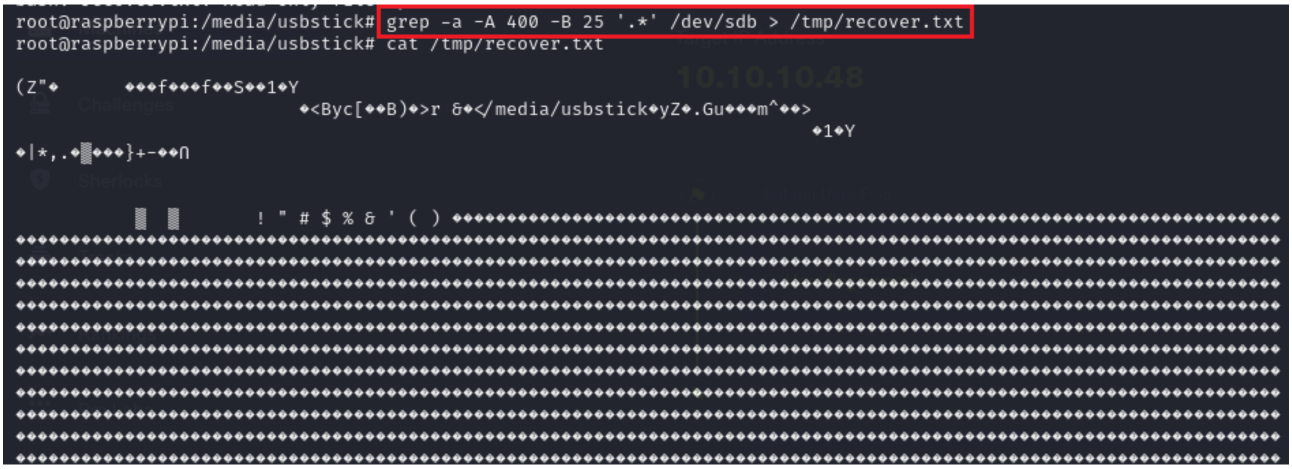
As I expected, one of these devices is a USB stick. So, I simply checked in it. However, it didn't contain the root flag, but I found a new note:



```
root@raspberrypi:/tmp# cd /media/usbstick
root@raspberrypi:/media/usbstick# ls -la
total 18
drwxr-xr-x 3 root root  1024 Aug 14  2017 .
drwxr-xr-x 3 root root  4096 Aug 14  2017 ..
-rw-r--r-- 1 root root   129 Aug 14  2017 damnit.txt
drwx------ 2 root root 12288 Aug 14  2017 lost+found
root@raspberrypi:/media/usbstick# cat damnit.txt
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?

-James
```

Figure 6 - Note about file deleting

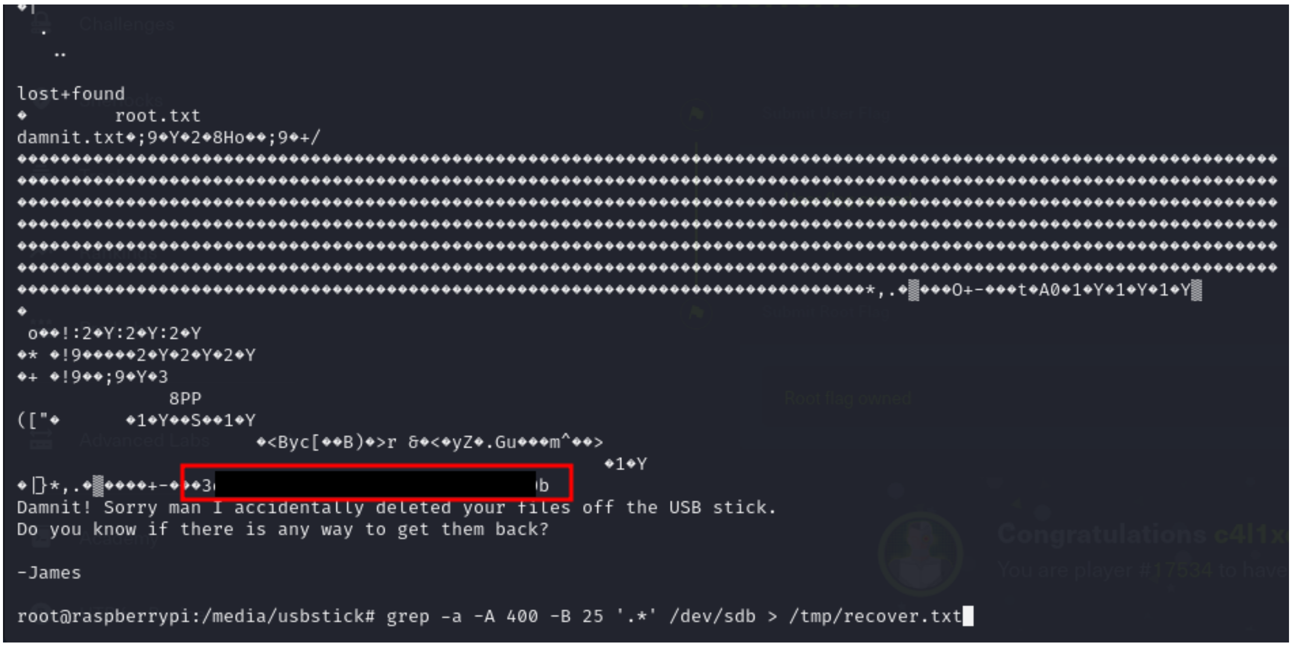
I didn't still find the root flag. The last note I found made me think about I have to recover the root flag from the USB stick. I looked on the Internet some way to do it and several of them require a no built-in tool. So, this searching took a bit of time. Finally, I found a rough way to do it:



```
root@raspberrypi:/media/usbstick# grep -a -A 400 -B 25 '.*' /dev/sdb > /tmp/recover.txt
root@raspberrypi:/media/usbstick# cat /tmp/recover.txt

(Z"◆      ◆◆◆f◆◆◆f◆◆S◆◆1◆Y
                          ◆<Byc[◆◆B)◆>r &◆</media/usbstick◆yZ◆.Gu◆◆◆m^◆◆>
                                                                               ◆1◆Y
◆|*,.◆▒◆◆◆}+-◆◆∩


           ▒  ▒       ! " # $ % & ' ( ) ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
```

Figure 7 - Rough file recover

So, looking for the flag in all output, I finally found the root flag:



```
◆|
 .
    ..

lost+found
◆        root.txt
damnit.txt◆;9◆Y◆2◆8Ho◆◆;9◆+/
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆*,.◆▒◆◆◆O+-◆◆◆t◆A0◆1◆Y◆1◆Y◆1◆Y▒
◆
 o◆◆!:2◆Y:2◆Y:2◆Y
◆* ◆!9◆◆◆◆◆2◆Y◆2◆Y◆2◆Y
◆+ ◆!9◆◆;9◆Y◆3
              8PP
(["◆      ◆1◆Y◆◆S◆◆1◆Y
                      ◆<Byc[◆◆B)◆>r &◆<◆yZ◆.Gu◆◆◆m^◆◆>
                                                      ◆1◆Y
◆[]*,.◆▒◆◆◆◆+-◆◆◆3[redacted]b
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?

-James

root@raspberrypi:/media/usbstick# grep -a -A 400 -B 25 '.*' /dev/sdb > /tmp/recover.txt
```

Figure 8 - Root flag

Personal comments

I consider this box very funny and basic. However, I liked the searching of the root flag, similar to a treasure hunting. However, since I can't install anything on a box, it was challenging to find the right command to use to recover files from the USB stick. Also, I understand the password reuse matter, but, at least in this case, it is not easy to think that the Raspberry default password can be used to log in via SSH. In fact, there is any clue to hypnotize that a user named pi, or relative to Pi-hole or Raspberry, exist. In conclusion, I rated this box as easy.