HOME NETWORK SECURITY

Edmond Lascaris - Creative Commons - 9 March 2021

OVERVIEW

Running a Raspberry Pi computer on your home network can be done securely.

There are many ways to improve and maintain security.

LEARNING OBJECTIVES

- Updating and Upgrading your Raspberry Pi
- Changing the default password for user pi
- Make directories and files in the Terminal
- Install fail2ban
- Install a firewall

WEEK 3: LESSON 3: PART 1: HOME NETWORK SECURITY

KEEPING YOU PI UPDATED

When you update your computer, not only do you get updates to the latest features, but you also get fixes to software bugs and security issues. You can do this process manually and you can also automate this procedure.

There are two commands we need to enter in the Terminal

- sudo apt-get update
- sudo apt-get full-upgrade (or sudo apt full-upgrade)
- sudo apt-get clean (or sudo apt clean)

Notes:
sudo apt-get update - updates software libraries on the Raspberry Pi
sudo apt-get full-upgrade - downloads and installs all the new software upgrades
sudo apt-get - clean removes downloaded files kept in the archive directory (/var/cache/apt/archives)

1. **Update Raspberry Pi Software**

- Open the Terminal on the Pi and enter sudo apt-get update

```
pi@raspberrypi: ~
File  Edit  Tabs  Help
pi@raspberrypi:~ $ sudo apt-get update
```

- The update takes approximately 30 seconds to one minute.
- This is the typical output.

```
pi@raspberrypi: ~
File  Edit  Tabs  Help
pi@raspberrypi:~ $ sudo apt-get update
Get:1 http://archive.raspberrypi.org/debian stretch InRelease [25.4 kB]
Get:2 http://raspbian.raspberrypi.org/raspbian stretch InRelease [15.0 kB]
Get:3 http://raspbian.raspberrypi.org/raspbian stretch/main armhf Packages [11.7
 MB]
Get:4 http://archive.raspberrypi.org/debian stretch/main armhf Packages [220 kB]
Fetched 11.9 MB in 20s (574 kB/s)
Reading package lists... Done
pi@raspberrypi:~ $
```

2. **Upgrade Raspberry Pi Software**

- Now enter the command sudo apt-get full-upgrade

```
pi@raspberrypi:~ $ sudo apt full-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  gconf-service gconf2-common libexiv2-14 libgconf-2-4 libgfortran3
  libgmime-2.6-0 libmicrodns0 libncurses5 libssl1.0.2 lxplug-volume
  rpi-eeprom-images uuid-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
pi@raspberrypi:~ $
```

- The Pi will tell you what software upgrades are required and ask for permission.
- It will also tell you how much additional disk space will be required.

```
pi@raspberrypi: ~
File  Edit  Tabs  Help
The following packages have been kept back:
  chromium-browser libavcodec-dev libavcodec57 libavfilter6 libavformat-dev
  libavformat57 libavresample3 libavutil-dev libavutil55 libpostproc54
  libswresample-dev libswresample2 libswscale-dev libswscale4 mu nodejs
  nodered omxplayer python-gpiozero python3-gpiozero python3-thonny
  rpi-chromium-mods sense-emu-tools wolfram-engine
The following packages will be upgraded:
  cups-bsd cups-client cups-common curl evince evince-common git git-man
  icu-devtools libcups2 libcupsimage2 libcurl3 libcurl3-gnutls
  libcurl4-openssl-dev libevdocument3-4 libevview3-3 libexif-dev libexif12
  libfreetype6 libfreetype6-dev libglib2.0-0 libglib2.0-bin libglib2.0-data
  libglib2.0-dev libicu-dev libicu57 libidn11 libmariadbclient18 libopenjp2-7
  libopenjp2-7-dev libperl5.24 libqt5concurrent5 libqt5core5a libqt5dbus5
  libqt5gui5 libqt5network5 libqt5opengl5 libqt5printsupport5 libqt5sql5
  libqt5sql5-sqlite libqt5test5 libqt5widgets5 libqt5xml5 libservlet3.1-java
  libssl1.0.2 libtimedate-perl libxslt1.1 mariadb-client-10.1
  mariadb-client-core-10.1 mariadb-common mariadb-server-10.1
  mariadb-server-core-10.1 perl perl-base perl-modules-5.24 php7.0-common
  php7.0-mysql python-cryptography python-pil python-werkzeug
  python3-cryptography python3-pil python3-werkzeug qt5-gtk-platformtheme sudo
65 upgraded, 0 newly installed, 0 to remove and 24 not upgraded.
Need to get 89.6 MB of archives.
After this operation, 383 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

- The first time you do an upgrade it could take several minutes.
- Sometimes you need to check how much additional disk space you have available.
- If too much space is occupied by the operating system and associated software it can compromise

PROTECTING THE RASPBERRY PI FROM MALICIOUS ATTACKS ON THE INTERNET

Fail2ban is a tool used to detect brute-force attacks and block them. If an attack is sustained for many months it is possible for an attacker to gain access to your computer system. Fail2ban aims to protect your computer from repeat attacks. It does this by blocking attackers for an re-occurring IP address if they fail to login more than a certain number of times You can configure the number of tries before a ban is put in place and how long the ban will remain.

1. **Install Fail2ban software**

- Enter the following Terminal commands to install Fail2ban on your Raspberry Pi: sudo apt-get install fail2ban

```
pi@raspberrypi:~ $ sudo apt-get install fail2ban
```

- Enter y (yes) to proceed with installation.

  - The installation only takes a few seconds to complete.
  - By default fail2ban will ban attacker for 10 minutes after 5 failed attempts.
  - This will be fine for our system

```
pi@raspberrypi:~ $ sudo apt-get install fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  lxkeymap python-cairo python-gobject python-gobject-2 python-gtk2
  python-xklavier python3-appdirs python3-ipykernel python3-jupyter-client
  python3-jupyter-core python3-pycodestyle python3-pyqt5.qtsvg
  python3-qtconsole python3-semver python3-zmq realpath
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  python3-systemd whois
Suggested packages:
  mailx monit
The following NEW packages will be installed:
  fail2ban python3-systemd whois
0 upgraded, 3 newly installed, 0 to remove and 24 not upgraded.
Need to get 387 kB of archives.
After this operation, 1,717 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

  - If you need to change the configuration file you can find it in /etc/fail2ban
  - The main configuration file is jail.conf

2. Access the configuration file

- To have a look at the configuration file jail.conf first navigate using cd /etc/fail2ban

```
pi@raspberrypi:~ $ cd /etc/fail2ban
pi@raspberrypi:/etc/fail2ban $ ls
action.d        fail2ban.d  jail.conf  paths-arch.conf    paths-debian.conf
fail2ban.conf   filter.d    jail.d     paths-common.conf  paths-opensuse.conf
pi@raspberrypi:/etc/fail2ban $
```

- To look inside the jail.conf file you can enter less jail.conf

```
pi@raspberrypi:/etc/fail2ban $ less jail.conf
```

  - This will allow you to scoll down the jail.conf file one line at a time using the arrow keys.
  - To exit less, enter q.

```
pi@raspberrypi: /etc/fail2ban
File  Edit  Tabs  Help
#
# WARNING: heavily refactored in 0.9.0 release.  Please review and
#          customize settings for your setup.
#
# Changes:  in most of the cases you should not modify this
#           file, but provide customizations in jail.local file,
#           or separate .conf files under jail.d/ directory, e.g.:
#
# HOW TO ACTIVATE JAILS:
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local file.
# See man 5 jail.conf for details.
#
# [DEFAULT]
# bantime = 1h
jail.conf
```

- If you make any changes to the configuration file you need to restart the service with the command sudo service fail2ban restart

INSTALL A FIREWALL

A firewall allows you to block all ports except the ones you need and also filter access by IP address. We are going to install ufw (Uncomplicated FireWall), which is very straightforward to use and configure according to our needs. A basic administration configuration page can be accessed using the Terminal.

1. **Install Uncomplicated Firewall on your Raspberry Pi**

- Enter the following command to install the firewall package: sudo apt-get install ufw

```
pi@raspberrypi:~ $ sudo apt-get install ufw
```

- The installation takes a few seconds.

```
pi@raspberrypi: ~
File  Edit  Tabs  Help
After this operation, 848 kB of additional disk space will be used.
Get:1 http://raspbian.melbourneitmirror.net/raspbian stretch/main armhf ufw all
0.35-4 [164 kB]
Fetched 164 kB in 1s (95.2 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 167428 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.35-4_all.deb ...
Unpacking ufw (0.35-4) ...
Setting up ufw (0.35-4) ...

Creating config file /etc/ufw/before.rules with new version

Creating config file /etc/ufw/before6.rules with new version

Creating config file /etc/ufw/after.rules with new version

Creating config file /etc/ufw/after6.rules with new version
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /lib/s
ystemd/system/ufw.service.
Processing triggers for systemd (232-25+deb9u12) ...
Processing triggers for man-db (2.7.6.1-2) ...
Processing triggers for rsyslog (8.24.0-1) ...
pi@raspberrypi:~ $
```

- We can get help using ufw using the command sudo ufw help

```
pi@raspberrypi:~ $ sudo ufw help

Usage: ufw COMMAND

Commands:
 enable                          enables the firewall
 disable                         disables the firewall
 default ARG                     set default policy
 logging LEVEL                   set logging to LEVEL
 allow ARGS                      add allow rule
 deny ARGS                       add deny rule
 reject ARGS                     add reject rule
 limit ARGS                      add limit rule
 delete RULE|NUM                 delete RULE
 insert NUM RULE                 insert RULE at NUM
 route RULE                      add route RULE
 route delete RULE|NUM           delete route RULE
 route insert NUM RULE           insert route RULE at NUM
 reload                          reload firewall
 reset                           reset firewall
 status                          show firewall status
```

- All Linux software also comes with an electronic manual. To read the manual enter man ufw

```
File  Edit  Tabs  Help
UFW:(8)                         February 2016                         UFW:(8)

NAME
       ufw - program for managing a netfilter firewall

DESCRIPTION
       This  program  is  for managing a Linux firewall and aims to provide an
       easy to use interface for the user.

USAGE
       ufw [--dry-run] enable|disable|reload
```

2. Enable Uncomplicated firewall

When ufw is first installed all ports are blocked by default. To make these ports available we need to open them up. Ports are small channels used by different software on our computer. The more ports are open, the more vulnerable your computer is to hackers.

Port examples

- HTTP or web requests are on port 80

- VNC (Virtual Network Computer) is on port 5900

Note: To make any change to ufw you need to be a super user

- To enable the firewall enter the command: sudo ufw enable

```
pi@raspberrypi:~ $ sudo ufw enable
Firewall is active and enabled on system startup
pi@raspberrypi:~ $
```

- The ufw service will be enabled even on reboot.

3. Opening Selective ports (pigeon holes)

- To open up port 80 enter the command sudo ufw allow 80
- To open up port 5900 enter the command sudo ufw allow 5900

```
pi@raspberrypi:~ $ sudo ufw allow 80
Rules updated
Rules updated (v6)
pi@raspberrypi:~ $ sudo ufw allow 5900
Rules updated
Rules updated (v6)
pi@raspberrypi:~ $
```

4. Check the status of Uncomplicated Firewall

- To display the current rules that are being applied by the firewall enter: sudo ufw status verbose

```
pi@raspberrypi:~ $ sudo ufw enable
Firewall is active and enabled on system startup
pi@raspberrypi:~ $ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
80                         ALLOW IN    Anywhere
5900                       ALLOW IN    Anywhere
80 (v6)                    ALLOW IN    Anywhere (v6)
5900 (v6)                  ALLOW IN    Anywhere (v6)

pi@raspberrypi:~ $
```

Other commands that are useful with ufw include:

- sudo ufw disable - to turn the service off
- sudo ufw deny 80 - to deny access via port 80
- sudo ufw status numbered - to give each item a reference number
- sudo ufw delete 2 - to remove rule number 2 from the numbered list