



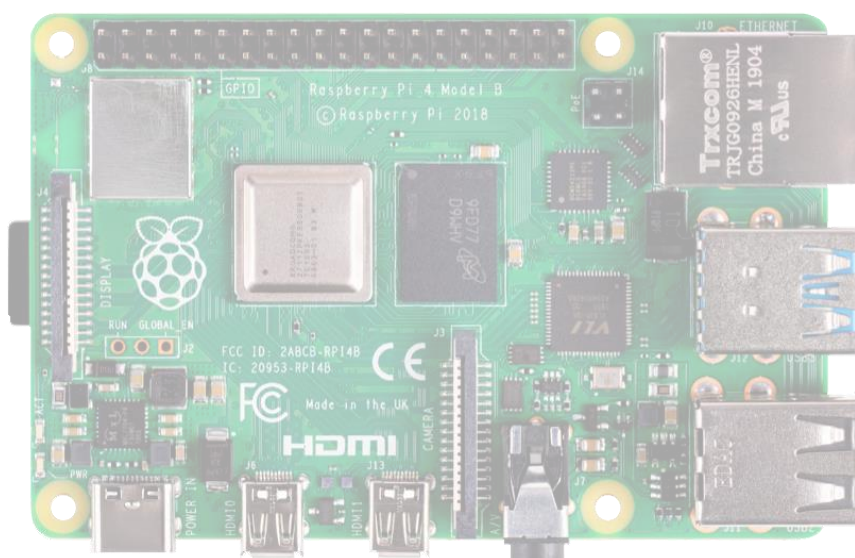
Synthèse de manipulation RPI.

Par Jean Staffe,

Bachelier 1 Sécurité Systèmes.

Table des matières

1. Changer le hostname	3
2. Trouver l'IP du Raspberry	3
3. Configuration Wi-Fi	3
Méthode non sécurisée :	4
Méthode sécurisée :	4
4. Sécurisation SSH	4
Changer le mot de passe	4
Changer le port SSH.....	4
5. Utilisations de clés SSH.....	5
Cas Windows.	5
Connexion avec la clé publique.	6
Désactiver la connexion par password.....	7
Cas Linux.....	7
6. Xming.....	8



1. Changer le hostname

`sudo raspi-config`

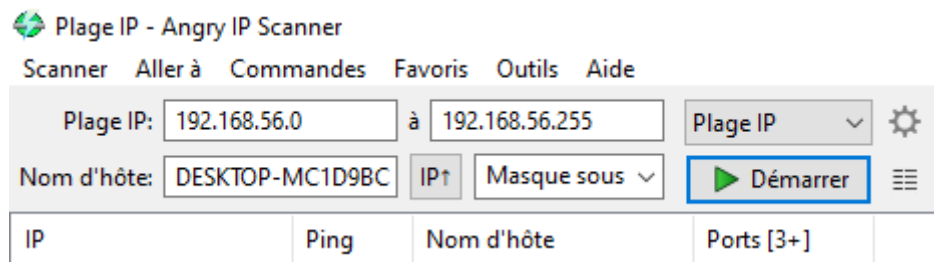
ou

`/etc/sysconfig/network => changer HOSTNAME`

+ `/etc/hosts + hostname « NOM »`

2. Trouver l'IP du Raspberry

Ouvrir angry ip scanner, changer les valeurs si nécessaire dans plage ip



Pour trouver la plage IP à scanner, ouvrez un CMD et faites « ipconfig » pour récupérer votre masque de sous réseau et IP d'ordinateur.

```
Carte Ethernet Eth PC :

Suffixe DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . . : fe80::4d2d:aaf2:8f30:42ba%18
Adresse IPv4. . . . . : 192.168.1.235
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.1
```

Chez moi, ma plage IP sera 192.168.1.0 à 192.168.1.255 car mon masque de sous réseau est 255.255.255.0 soit /24

Si la plage à un masque 255.255.0.0 par exemple la plage sera 10.1.0.0 à 10.1.255.255

3. Configuration Wi-Fi

Fichier à modifier : `/etc/wpa_supplicant/wpa_supplicant.conf`

Il faut d'abord setup la région sur raspi-config. Faites la configuration wifi uniquement pour la région. Vous pouvez utiliser le wizzard pour le setup wifi mais je ne peux assurer que vous aurez autant de points qu'une personne qui passe par nano/vim.

Méthode non sécurisée :

```
network={
    ssid="<le ssid du wifi auquel vous voulez vous connecter>"
    psk="<le mot de passe>"
}
```

Méthode sécurisée :

Générer une clé avec wpa_passphrase

Commande : **wpa_passphrase "SSID" "MOT DE PASSE"**

```
network={
    ssid="<le ssid du wifi auquel vous voulez vous connecter>"
    psk="<la clé générée>"
}
```

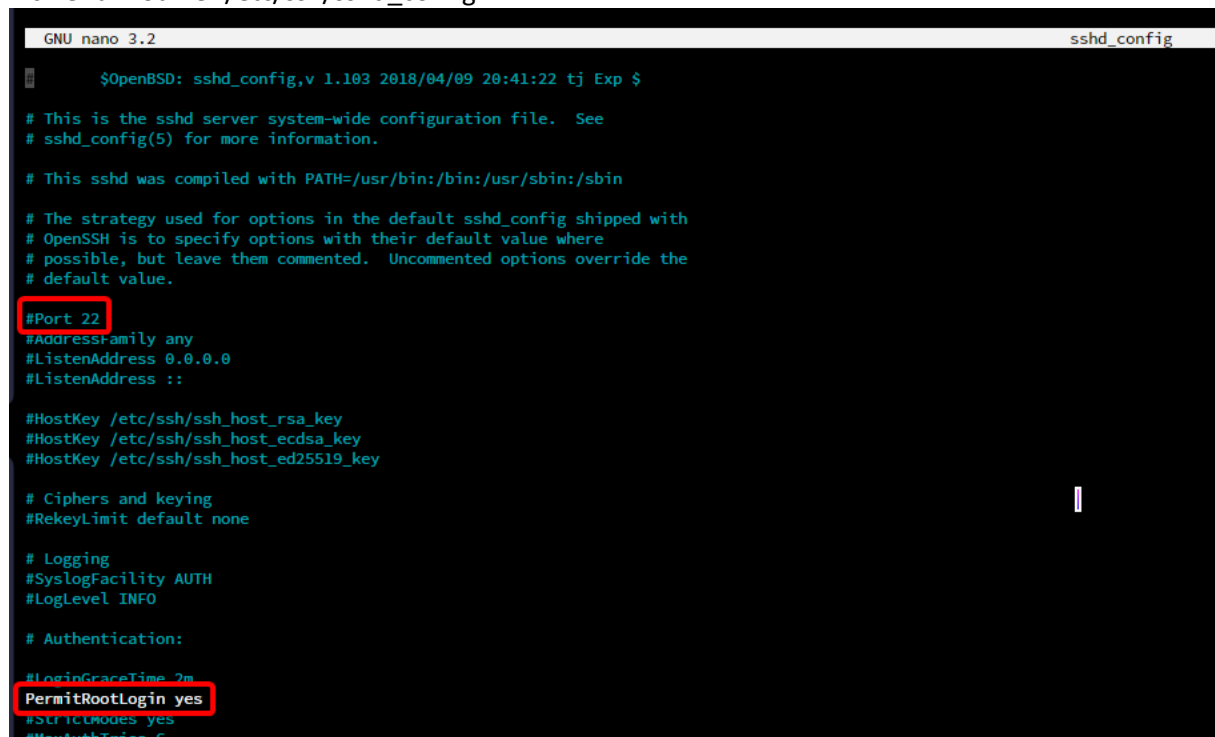
4. Sécurisation SSH

Changer le mot de passe

Commande : **passwd <nom d'utilisateur>**

Changer le port SSH

Fichier à modifier /etc/ssh/sshd_config



```
GNU nano 3.2 sshd_config
$OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

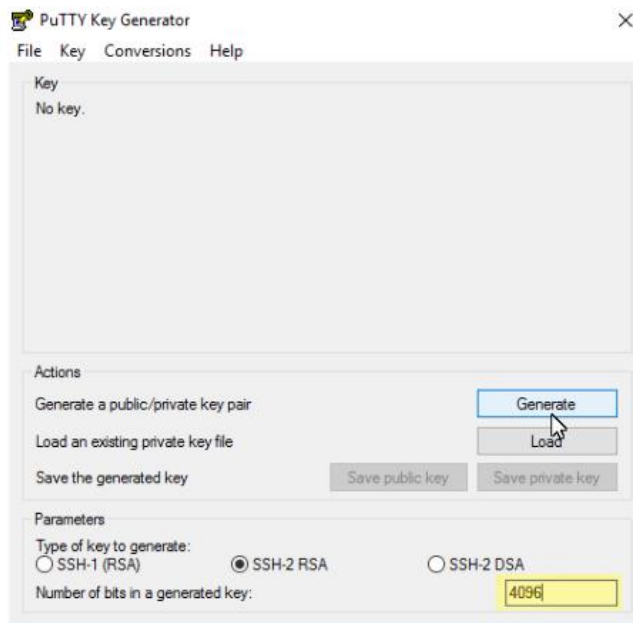
# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
```

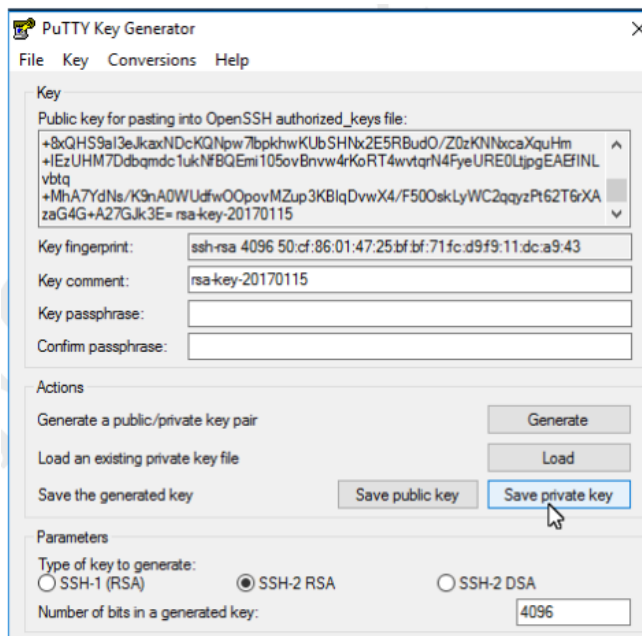
Décommentez la ligne #Port 22 et changez la valeur par celle du port que vous souhaitez utiliser. La ligne PermitRootLogin permet d'autoriser la connexion en root à la machine. Reboot ssh après

5. Utilisations de clés SSH.

Cas Windows.



Ouvrez puttygen et générez une clé



Sauvegardez la clé privée, vous pouvez lui définir un mot de passe comme conseillé.

ATTENTION ! Votre clé privée ne doit en aucun cas être partagée.

Commandes :

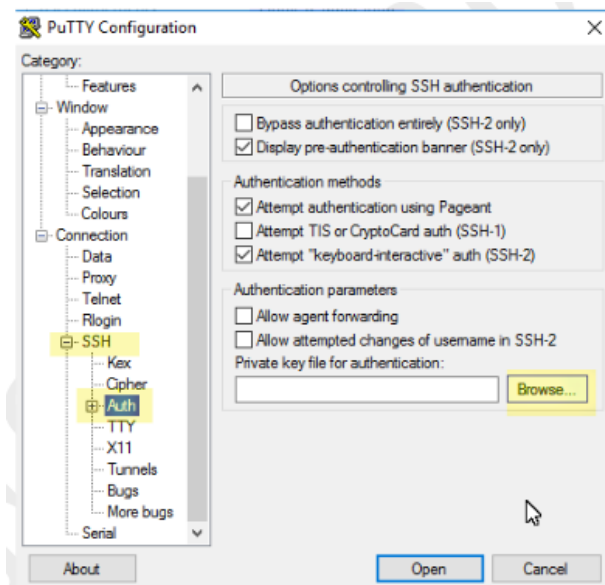
```
cd ~/.ssh
```

```
nano authorized_keys
```

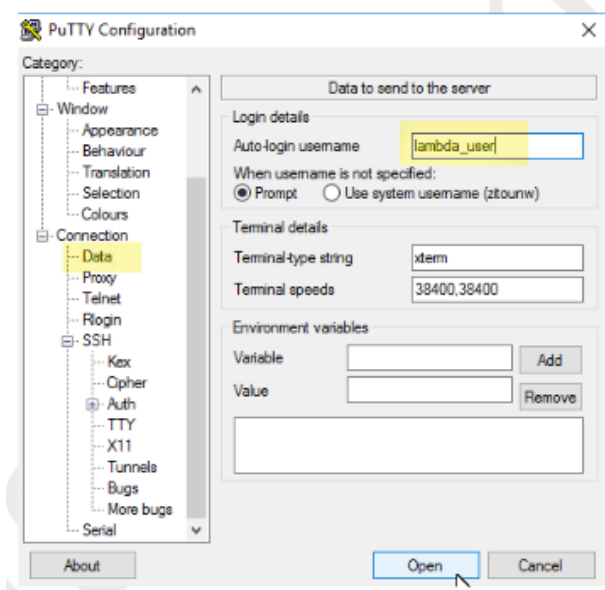
Collez la clé SSH publique.

Connexion avec la clé publique.

Lancer putty et ajouter la clé SSH :



Ouvrez la clé privée puis lancez la connexion :



Désactiver la connexion par password.

```
sudo nano /etc/ssh/sshd_config
```

```
PasswordAuthentication no
```

```
PubkeyAuthentication yes
```

```
sudo service ssh restart
```

Cas Linux.

```
cd /home/pi/.ssh
```

```
ssh-keygen -b 4096 -t rsa
```

```
cd /home/pi/.ssh
```

```
touch authorized_keys
```

```
chmod 600 authorized_keys
```

```
cd ~/.ssh
```

```
cat id_ras.pub | ssh -p 22 pi@<ip de votre Rasp> 'cat >> .ssh/authorized_keys
```

VERIFIER LA CONNEXION

Sécurité :

```
sudo nano /etc/ssh/sshd_config
```

```
PasswordAuthentication no
```

```
PubkeyAuthentication yes
```

```
sudo service ssh restart
```

6. Xming

Activer “x11 forwarding” dans Putty » SSH > Auth > X11

