

Problème de changement de clés d'authentification sur le serveur SSH

SOMMAIRE :

1. PROBLÉMATIQUE.	2
2. COMMENT FAIRE SOUS « WINDOWS » ?	2
3. COMMENT FAIRE SOUS « MAC OS X » OU « LINUX » ?	2

1. Problématique.

Si on change le serveur SSH « marion.szpieg.fr » pour en mettre un neuf, et que quelqu'un s'était déjà connecté à l'ancien alors le client SSH détecte le changement. Le client SSH refuse de se connecter car il a un doute sur l'authenticité du serveur.

Résultat de la connexion sur « Windows » :

```
PS C:\Users\Marion> ssh lfcltx@marion.szpieg.fr
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@           WARNING: POSSIBLE DNS SPOOFING DETECTED!           @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
The ECDSA host key for marion.szpieg.fr has changed,
and the key for the corresponding IP address 176.128.12.22
has a different value. This could either mean that
DNS SPOOFING is happening or the IP address for the host
and its host key have changed at the same time.
Offending key for IP in C:\Users\Marion\.ssh\known_hosts:6
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@           WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!   @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:1jgtzpNoBQ3ZS3MSWajhpi7v8FnCUN23Vr3gpS27h8c.
Please contact your system administrator.
Add correct host key in C:\Users\Marion\.ssh\known_hosts to get rid of this message.
Offending ECDSA key in C:\Users\Marion\.ssh\known_hosts:5
ECDSA host key for marion.szpieg.fr has changed and you have requested strict checking.
Host key verification failed.
PS C:\Users\Marion>
```

« Host key verification failed » →

Résultat de la connexion sous MAC OS X :

```
Mini-de-mini22:~ marion$ ssh marion@marion.szpieg.fr
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@           WARNING: POSSIBLE DNS SPOOFING DETECTED!           @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
The ECDSA host key for marion.szpieg.fr has changed,
and the key for the corresponding IP address 176.128.12.22
is unknown. This could either mean that
DNS SPOOFING is happening or the IP address for the host
and its host key have changed at the same time.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@           WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!   @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:1jgtzpNoBQ3ZS3MSWajhpi7v8FnCUN23Vr3gpS27h8c.
Please contact your system administrator.
Add correct host key in /Users/marion/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /Users/marion/.ssh/known_hosts:1
ECDSA host key for marion.szpieg.fr has changed and you have requested strict checking.
Host key verification failed.
```

« Host key verification failed » →

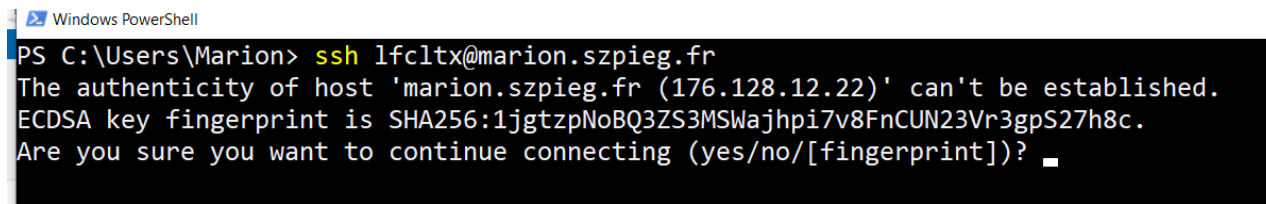
2. Comment faire sous « Windows » ?

Lancer l'interpréteur de commandes « PowerShell » puis taper les deux lignes ci-contre →

```
PS C:\Users\Marion> cd .ssh
PS C:\Users\Marion> rm .\known_hosts
```

Attention, il y a bien le caractère « . » devant « ssh » sur la première ligne donc « .ssh » !!!

Puis lancer la connexion

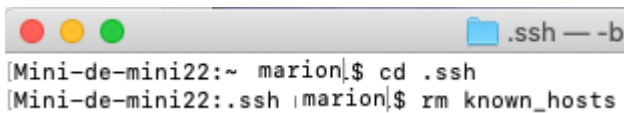


```
Windows PowerShell
PS C:\Users\Marion> ssh lfcltx@marion.szpieg.fr
The authenticity of host 'marion.szpieg.fr (176.128.12.22)' can't be established.
ECDSA key fingerprint is SHA256:1jgtzpNoBQ3ZS3MSWajhpi7v8FnCUN23Vr3gpS27h8c.
Are you sure you want to continue connecting (yes/no/[fingerprint])? █
```

Répondre « yes » et taper votre mot de passe, la connexion doit fonctionner !!

3. Comment faire sous « Mac OS X » ou « Linux » ?

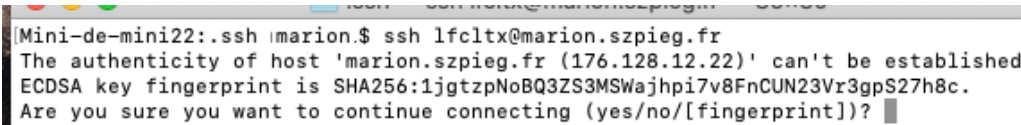
Lancer un terminal et taper les deux lignes ci-contre :



```
Mini-de-mini22:~ marion|$ cd .ssh
Mini-de-mini22:~ marion|$ rm known_hosts
```

Attention, il y a bien le caractère « . » devant « ssh » sur la première ligne donc « .ssh » !!!

Puis lancer la connexion :



```
Mini-de-mini22:~ marion|$ ssh lfcltx@marion.szpieg.fr
The authenticity of host 'marion.szpieg.fr (176.128.12.22)' can't be established.
ECDSA key fingerprint is SHA256:1jgtzpNoBQ3ZS3MSWajhpi7v8FnCUN23Vr3gpS27h8c.
Are you sure you want to continue connecting (yes/no/[fingerprint])? █
```

Répondre « yes » et taper votre mot de passe, la connexion doit fonctionner !!