Pi_labs_hostkeys

In this lab you will connect to your pi 8 machine, or work together with a colleague.
On the other vm (so not your current vm) you will remove the ssh host keys, and create new keys.

Then you will try to connect to that machine and fail.
To reconnect you will modify the known_hosts file.

1. Remove host keys

```
[root@pi159 ssh]# cd /etc/ssh
[root@pi159 ssh]# rm ssh_host_*
```

2. Generate new keys

```
[root@pi159 ssh]# ssh-keygen -A
ssh-keygen: generating new host keys: RSA DSA ECDSA ED25519
```

3. On you original vm try and connect

```
ssh pi@pi159
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    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:hpNcBPxesDFaVOMn9IenT0nw53I+r2dgcsZG6PrAmYM.
Please contact your system administrator.
Add correct host key in /Users/petervanderweerd/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /Users/petervanderweerd/.ssh/known_hosts:24
ECDSA host key for pi159 has changed and you have requested strict checking.
Host key verification failed.
```

4. Either modify known_hosts or delete it.

```
ssh-keygen -R "pi159"
```

5. Now reconnect

```
ssh pi@pi159
The authenticity of host 'pi159 (192.168.4.152)' can't be
established.
ECDSA key fingerprint is
SHA256:hpNcBPxesDFaVOMn9IenT0nw53I+r2dgcsZG6PrAmYM.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
y
```

6. On your remote machine, check the fingerprint!

```
[root@pi159 ssh]# ssh-keygen -lf /etc/ssh/ssh_host_ecdsa_key.pub
256 SHA256:hpNcBPxesDFaVOMn9IenT0nw53I+r2dgcsZG6PrAmYM root@pi159
(ECDSA)
```