ssh known_hosts

The `ssh` program keeps track of all servers you connect to using `ssh` hostkeys. When the hostkey changes `ssh` warns you and asks if this is a legitimate change, or you are connecting to a malicious server which is impersonating the real one. If the change is expected you can simply remove the conflicting line from your `~/.ssh/known_hosts` file and reconnect. To make things easy `ssh` shows which line doesn't match the new host key.

Here "`Offending key for IP in /Users/pepper/.ssh/known_hosts:634`" and "`Offending ECDSA key in /Users/pepper/.ssh/known_hosts:478`" meant that lines 634 and 478 of known_hosts on my Mac contained a different (old) hostkeys, and could be removed to clear this warning and re-enable access to lilac.

```
pepper@RSKI0050:~$ ssh lilac
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@       WARNING: POSSIBLE DNS SPOOFING DETECTED!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
The ECDSA host key for lilac has changed,
and the key for the corresponding IP address 140.163.188.123
is unchanged. 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 /Users/pepper/.ssh/known_hosts:634
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    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:kkBACKn07y86mn48F1Zlhtsvn5mAEt2POLNcSLbEW/4.
Please contact your system administrator.
Add correct host key in /Users/pepper/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /Users/pepper/.ssh/known_hosts:478
ECDSA host key for lilac has changed and you have requested strict checking.
Host key verification failed.
```

If you use `vi`, the command "`vi +634 /Users/pepper/.ssh/known_hosts`" will open the file to line 634 for editing.

Then you can `ssh` into the server again, accept the new key (just type 'yes' at the prompt), and continue normally.

The last time this happened to many users was March 25th, 2021. We replaced the old lilac-ln01 login server with the backup lilac-ln02 login server, which had a different hostkey and generated an alert for each lilac user when they connected to the new server.

https://mskcchpc.slack.com/archives/C16D1339U/p1616694952026300

Some users will see the warning again when we return lilac-ln01 to service.