How to spot differences in OpenSSH

Contributed by Michael Felt

There are ways to spot differences of ssh and sshd. Here are just a few.

And I hope you find the differences easy to spot and maybe even enlightening!

Using telnet - to see what demon you are connecting to:

```
root@x063:[/home/mamfelt]telnet localhost 22
Trying...
Connected to loopback.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.0

Connection closed.
root@x063:[/home/mamfelt]telnet x071 22
Trying...
Connected to x071.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.4
```

After installing the latest version from AIX WebPacks

```
root@x062:[/data/prj/IBM/OpenSSH_7.1.101.5000]telnet localhost 22
Trying...
Connected to loopback.
Escape character is '^]'.

SSH-2.0-OpenSSH_7.1
```

Executing the command - and request version

```
root@x063:[/home/mamfelt]ssh -V
OpenSSH_6.0p1, OpenSSL 1.0.1e 11 Feb 2013

michael@x071.home.local:[/home/michael/.ssh]ssh -V
OpenSSH_7.4p1, OpenSSL 1.0.2h  3 May 2016

root@x062:[/data/prj/IBM/OpenSSH_7.1.101.5000]ssh -V
OpenSSH_7.1p1, OpenSSL 1.0.1e 11 Feb 2013
```

Using a util such as ssh-keygen

```
michael@x071.home.local:[/home/michael/.ssh]/usr/bin/ssh-keygen -lf id_rsa.pub
1024 89:ad:16:cf:3a:f5:cd:fa:89:ab:49:17:2a:56:14:a5  michael@felt-1 (RSA)
michael@x071.home.local:[/home/michael/.ssh]/opt/bin/ssh-keygen -lf id_rsa.pub
1024 SHA256:AzHSpmLb8H+VU3/c8AB9o7397YwZeN7dmvrApq+4AEU michael@felt-1 (RSA)
```

Using/getting debug information

From openssh-7.4 to openssh-6.0

```
michael@x071.home.local:[/home/michael/.ssh]/opt/bin/ssh -v root@x063 date
OpenSSH_7.4p1, OpenSSL 1.0.2h  3 May 2016
debug1: Reading configuration data /var/openssh/etc/ssh_config
...
```

debug1: Enabling compatibility mode for protocol 2.0

debug1: Local version string SSH-2.0-OpenSSH_7.4

debug1: Remote protocol version 2.0, remote software version OpenSSH_6.0

...

debug1: kex: host key algorithm: ssh-rsa

debug1: kex: server->client cipher: aes128-ctr MAC: umac-64@openssh.com compression: none

debug1: kex: client->server cipher: aes128-ctr MAC: umac-64@openssh.com compression: none

...

debug1: Server host key: ssh-rsa SHA256:u7o8Qy+Q7Kh+ml4Y+GcCitYjBeZunJkMjU06nNvpCuc

From openssh-6.0 to openssh-7.4

root@x063:[/home/mamfelt]ssh -v michael@x071

OpenSSH_6.0p1, OpenSSL 1.0.1e 11 Feb 2013

debug1: Reading configuration data /etc/ssh/ssh_config

...

debug1: Remote protocol version 2.0, remote software version OpenSSH_7.4

debug1: match: OpenSSH_7.4 pat OpenSSH*

debug1: Enabling compatibility mode for protocol 2.0

debug1: Local version string SSH-2.0-OpenSSH_6.0

...

debug1: Server host key: RSA 7b:89:b4:a1:1a:dd:f1:04:59:8f:69:35:5e:3b:dd:4a

debug1: checking without port identifier

The authenticity of host '[x071]:22 ([192.168.XX.YY]:22)' can't be established.

RSA key fingerprint is 7b:89:b4:a1:1a:dd:f1:04:59:8f:69:35:5e:3b:dd:4a.

Are you sure you want to continue connecting (yes/no)?