Network Device Interpretation # 201803

Testing SSH when password-based authentication is not supported

Status: ☒ *Active* ☐ *Inactive*

Date: *6-Jun-2018*

End of proposed Transition Period (to be updated after TR2TD process): *6-Jul-2018*

Type of Change: ☐ Immediate application ☒ Minor change ☐ Major change

Type of Document: ☐ *Technical Decision* ☒ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☐ *Network iTC*

Affected Document(s): *ND SD v2.0*

Affected Section(s): *FCS_SSHC_EXT.1.9*

Superseded Interpretation(s): *None*

Issue:

In the cNDPP v2.0 FCS_SSHC_EXT.1.9 Test 2 states:

"Test 2: The evaluator shall add an entry associating a host name with a public key into the TOE's local database. The evaluator shall replace, on the corresponding SSH server, the server's host key with a different host key. The evaluator shall initiate a connection from the TOE to the SSH server using password-based authentication, shall ensure that the TOE rejects the connection, and shall ensure that the password was not transmitted to the SSH server (for example, by instrumenting the SSH server with a debugging capability to output received passwords)."

However, password-based authentication is selection based and not mandatory for SSH clients in the cNDPP v2.0 FCS_SSHC_EXT.1.2 SFR, which states "The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: password-based, no other method]."

Because password-based authentication is not mandatory for SSH clients in this Protection Profile, when password-based authentication is not selected in FCS_SSHC_EXT.1.2, Test 2 in FCS_SSHC_EXT.1.9 should either be omitted or modified. A suggested modification would be to test a connection from the TOE to the SSH server using public key-based authentication after replacing the server's host key with a different host key and ensure that the TOE rejects the connection.

Please provide guidance on how to test a TOE that does not claim password-based authentication for SSH client.

Resolution:

The NIT proposes the following changes which shall be implemented if accepted by the Network iTC (sentence to be removed in case this recommendation is accepted).

The NIT acknowledges the issue described in the 'Issue' section above. In ND SD Test 2 for FCS_SSHC_EXT.1.9 shall therefore be modified as follows:

<*old*>"The evaluator shall add an entry associating a host name with a public key into the TOE's local database. The evaluator shall replace, on the corresponding SSH server, the server's host key with a different host key. The evaluator shall initiate a connection from the TOE to the SSH server using password-based authentication, shall ensure that the TOE rejects the connection, and shall ensure that the password was not transmitted to the SSH server (for example, by instrumenting the SSH server with a debugging capability to output received passwords)." </old>

shall be replaced by

<*new*>"The evaluator shall add an entry associating a host name with a public key into the TOE's local database. The evaluator shall replace, on the corresponding SSH server, the server's host key with a different host key. If 'password-based' is selected for the TOE in FCS_SSHC_EXT.1.2, the evaluator shall initiate a connection from the TOE to the SSH server using password-based authentication, shall ensure that the TOE rejects the connection, and shall ensure that the password was not transmitted to the SSH server (for example, by instrumenting the SSH server with a debugging capability to output received passwords). If 'password-based' is not selected for the TOE in FCS_SSHC_EXT.1.2, the evaluator shall initiate a connection from the TOE to the SSH server using public key-based authentication, and shall ensure that the TOE rejects the connection." </new>

Rationale:

see 'Issue' section.

Further Action:

None

Action by Network iTC:

None