17.5. Secure Shell

Objective

17.5.1. Secure Shell (SSH) is implemented correctly as an Approved Cryptographic Protocol.

Context

Scope

17.5.2. SSH is software based on the Secure Shell protocol and enables a connection to a remote system.

17.5.3. This section covers information on the conditions under which commercial and open-source implementations of SSH can be used as an approved cryptographic protocol. Additionally, secure copy and Secure File Transfer Protocol use SSH and are therefore also covered by this section.

17.5.4. When using a product that implements SSH, requirements for using approved cryptographic protocols will also need to be referenced from the Section 17. 3 - Approved Cryptographic Protocols.

References

17.5.5. Further references can be found at:

Reference	Title	Publisher	Source
	Further information on SSH can be found in the SSH specification	IETF	https://www.rfc-editor.org/rfc/rfc4252
	Further information on Open SSH	Open SSH	https://www.openssh.com/
	OpenSSH 7.3	Open SSH	http://www.openssh.com/txt/release-7.3

Rationale & Controls

Using SSH

17.5.6.R.01. **Rationale**

The configuration directives provided are based on the OpenSSH implementation of SSH. Agencies implementing SSH will need to adapt these settings to suit other SSH implementations.

17.5.6.R.02. **Rationale**

SSH version 1 is known to have vulnerabilities. In particular, it is susceptible to an adversary-in-the-middle attack, where an attacker who can intercept the protocol in each direction can make each node believe they are talking to the other. SSH version 2 does not have this vulnerability.

17.5.6.R.03. **Rationale**

SSH has the ability to forward connections and access privileges in a variety of ways. This means that an attacker who can exploit any of these features can gain unauthorised access to a potentially large amount of classified information.

17.5.6.R.04. **Rationale**

Host-based authentication requires no credentials (password, public key etc.) to authenticate although in some cases a host key can be used. This renders SSH vulnerable to an IP spoofing attack.

17.5.6.R.05. **Rationale**

An attacker who gains access to a system with system administrator privileges will have the ability to not only access classified information but to control that system completely. Given the clearly more serious consequences of this, system administrator login or administrator privilege

escalation SHOULD NOT be permitted.

17.5.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2647]

The table below outlines the settings that SHOULD be implemented when using SSH.

Configuration description	Configuration directive
Disallow the use of SSH version 1	Protocol 2
On machines with multiple interfaces, configure the SSH daemon to listen only on the required interfaces	ListenAddress xxx.xxx.xxx.xxx
Disable connection forwarding	AllowTCPForwarding no
Disable gateway ports	Gatewayports no
Disable the ability to login directly as root	PermitRootLogin no
Disable host-based authentication	HostbasedAuthentication no
Disable rhosts-based authentication	RhostsAuthentication no IgnoreRhosts yes
Do not allow empty passwords	PermitEmptyPasswords no
Configure a suitable login banner	Banner/directory/filename
Configure a login authentication timeout of no more than 60 seconds	LoginGraceTime xx
Disable X forwarding	X11Forwarding no

Authentication mechanisms

17.5.7.R.01. **Rationale**

Public key-based systems have greater potential for strong authentication, put simply, people are not able to remember particularly strong passwords. Password-based authentication schemes are also more susceptible to interception than public key-based authentication schemes.

17.5.7.R.02. **Rationale**

Passwords are more susceptible to guessing attacks, so if passwords are used in a system then countermeasures should be put into place to reduce the chance of a successful brute force attack.

17.5.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2672]

Agencies SHOULD use public key-based authentication before using password-based authentication.

17.5.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2673]

Agencies that allow password authentication SHOULD use techniques to block brute force attacks against the password.

Automated remote access

17.5.8.R.01. **Rationale**

If password-less authentication is enabled, allowing access from unknown IP addresses would allow untrusted parties to automatically authenticate to systems without needing to know the password.

17.5.8.R.02. **Rationale**

If port forwarding is not disabled or it is not configured securely, an attacker may be able to gain access to forwarded ports and thereby create a communication channel between the attacker and the host.

17.5.8.R.03. **Rationale**

If agent credential forwarding is enabled, an intruder could connect to the stored authentication credentials and then use them to connect to other trusted hosts or even intranet hosts, if port forwarding has been allowed as well.

17.5.8.R.04. **Rationale**

X11 is a computer software system and network protocol that provides a graphical user interface for networked computers. Failing to disable X11 display remoting could result in an attacker being able to gain control of the computer displays as well as keyboard and mouse control functions.

17.5.8.R.05. **Rationale**

Allowing console access permits every user who logs into the console to run programs that are normally restricted to the root user.

17.5.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2725]

Agencies SHOULD use parameter checking when using the 'forced command' option.

17.5.8.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2726]

Agencies that use logins without a password for automated purposes SHOULD disable:

- access from IP addresses that do not need access;
- port forwarding;
- agent credential forwarding;
- X11 display remoting; and
- console access.

17.5.8.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2727]

Agencies that use remote access without the use of a password SHOULD use the 'forced command' option to specify what command is executed.

SSH-agent

17.5.9.R.01. **Rationale**

SSH-agent or other similar key caching programs hold and manage private keys stored on workstations and respond to requests from remote systems to verify these keys. When an SSH-agent launches, it will request the user's password. This password is used to unlock the user's private key. Subsequent access to remote systems is performed by the agent and does not require the user to re-enter their password. Screenlocks and expiring key caches ensure that the user's private key is not left unlocked for long periods of time.

17.5.9.R.02. **Rationale**

Agent credential forwarding is required when multiple SSH connections are chained to allow each system in the chain to authenticate the user.

17.5.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2737]

Agencies that use SSH-agent or other similar key caching programs SHOULD:

- only use the software on workstation and servers with screenlocks;
- ensure that the key cache expires within four hours of inactivity; and
- ensure that agent credential forwarding is used when multiple SSH traversal is needed.

SSH-Versions

17.5.10.R.01. **Rationale**

Older versions contain known vulnerabilities which are regularly addressed or corrected by newer versions.

17.5.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2740]

Agencies SHOULD ensure that the latest implementation of SSH software is being used. Older versions contain known vulnerabilities.