Remote Service Session Hijacking: SSH Hijacking, Sub-technique T1563.001 - Enterprise

Archived: 2026-04-05 17:32:08 UTC

Adversaries may hijack a legitimate user's SSH session to move laterally within an environment. Secure Shell (SSH) is a standard means of remote access on Linux and macOS systems. It allows a user to connect to another system via an encrypted tunnel, commonly authenticating through a password, certificate or the use of an asymmetric encryption key pair.

In order to move laterally from a compromised host, adversaries may take advantage of trust relationships established with other systems via public key authentication in active SSH sessions by hijacking an existing connection to another system. This may occur through compromising the SSH agent itself or by having access to the agent's socket. If an adversary is able to obtain root access, then hijacking SSH sessions is likely trivial.[1][2][3][4]

SSH Hijacking differs from use of SSH because it hijacks an existing SSH session rather than creating a new session using Valid Accounts.

Source: https://attack.mitre.org/techniques/T1563/001