Detection of Remote Service Session Hijacking, Detection Strategy DET0079

Archived: 2026-04-05 18:33:16 UTC

AN0216

Detection of anomalous RDP or remote service session activity where a logon session is hijacked rather than newly created. Indicators include mismatched user credentials vs. active session tokens, service session takeovers without corresponding successful logon events, or RDP shadowing activity without user consent.

Log Sources

Mutable Elements

Field	Description
ExpectedUserSessionMap	Mapping of users to hosts they are expected to access; deviations indicate possible hijacking.
TimeWindow	Threshold for detecting rapid pivoting via hijacked sessions.

AN0217

Detection of SSH/Telnet session hijacking via discrepancies between authentication logs and active session tables. Adversary behavior includes reusing or stealing active PTY sessions, attaching to screen/tmux, or issuing commands without corresponding login events.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	auditd:SYSCALL	execve: Commands executed within an SSH session where no matching logon/authentication event exists
Logon Session Creation (DC0067)	NSM:Connections	Mismatch between recorded user logon and active sessions (e.g., wtmp/utmp entries without corresponding authentication in auth.log)
Network Traffic Flow (DC0078)	NSM:Flow	Long-lived or hijacked SSH sessions maintained with no active user activity

Mutable Elements

Field	Description
MonitoredServicePorts	Ports for SSH/Telnet/RDP monitored for session hijacking; may vary by environment.

AN0218

Detection of hijacked VNC or SSH sessions on macOS where adversaries take over an existing session rather than authenticating directly. Indicators include process execution from active sessions without new logon events, manipulation of TTY sessions, or anomalous network activity tied to dormant sessions.

Log Sources

Mutable Elements

Field	Description
SessionIdleThreshold	Time threshold for inactive sessions flagged as suspicious when commands suddenly resume.
