Detection of System Network Connections Discovery Across Platforms, Detection Strategy DET0320

Archived: 2026-04-05 15:36:03 UTC

AN0903

Detects usage of commands or binaries (e.g., netstat, PowerShell Get-NetTCPConnection) and WMI or API calls to enumerate local or remote network connections.

Log Sources

Mutable Elements

Field	Description
SuspiciousParentProcesses	Non-standard binaries launching PowerShell or netstat (e.g., winword.exe spawning powershell.exe).
TimeWindow	Correlates discovery behavior before lateral movement or credential access.
CommandPatternList	Regex or keyword patterns to match discovery utilities (e.g., `netstat`, `Get-NetTCPConnection`).

AN0904

Detects use of netstat, ss, lsof, or custom shell scripts to list current network connections. Often paired with privilege escalation or staging.

Log Sources

Mutable Elements

Field	Description
UtilityNameList	List of binaries used for discovery (e.g., netstat, ss, lsof).
UserContextScope	Limit detection to non-administrative or service accounts performing enumeration.
ExecutionFrequencyThreshold	Unusual number of executions within a short time window.

AN0905

Detects shell-based enumeration of active connections using `netstat`, `lsof -i`, or AppleScript-based system discovery.

Log Sources

Mutable Elements

Field	Description
ShellCommandWatchlist	Matches terminal commands like `lsof -i`, `netstat`, or scripts issued via Automator or AppleScript.
TerminalBinaryDenylist	Tracks execution of networking discovery tools by apps outside Terminal.app or iTerm.

AN0906

Detects shell or API usage of `esxcli network ip connection list` or `netstat` to enumerate ESXi host connections.

Log Sources

Mutable Elements

Field	Description
ExecutionOriginCheck	Detect commands executed outside normal management interfaces (e.g., SSH or root shell).
ExpectedAdminAccessWindow	Timeframe when host connection audits are expected (e.g., maintenance windows).

AN0907

Detects interactive or automated use of CLI commands like `show ip sockets`, `show tcp brief`, or SNMP queries for active sessions on routers/switches.

Log Sources

Mutable Elements

Field	Description
CommandPatternList	Monitors for known socket/session query strings.
PrivilegedUserCheck	Restrict detections to non-admin roles executing advanced queries.

AN0908

Detects enumeration of cloud network interfaces, VPCs, subnets, or peer connections using CLI or SDKs (e.g., AWS CLI, Azure CLI, GCloud CLI).

Log Sources

Mutable Elements

Field	Description
ServicePrincipalAllowlist	Allow certain automation roles to perform discovery during provisioning.
BurstQueryThreshold	Unusual number of Describe* or List* network API calls in a short timeframe.
