Port-knock → rule/daemon change → first successful connect (T1205.001), Detection Strategy DET0302

Archived: 2026-04-05 15:42:49 UTC

AN0842

A remote source rapidly touches a short sequence of closed ports (SYN→RST/S0) on a Windows host. Within a short window the host changes firewall state (WFP rule added/modified or service starts listening) and then the same source completes the first successful handshake to the newly opened port.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Seconds to correlate knock sequence → rule change → successful connect (60–300s typical).
MinSequenceLen	Minimum number of distinct destination ports in the sequence (≥3 by default).
RuleChangeAllowList	Accounts/processes allowed to adjust Windows Firewall (e.g., update agents).
WatchedPorts	Ports of interest to flag when opened (e.g., 22,23,2323,8022,3389,8080).

AN0843

A source performs a short closed-port sequence; the host then modifies iptables/nftables/ufw rules or starts a daemon binding a new socket, followed by a successful connection from the same source.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve: Commands that alter firewall or start listeners: iptables|nft|ufw|firewall-cmd|pfctl|systemctl start sshd/telnet/dropbear; raw-socket/libpcap tools (tcpdump, tshark, nmap --raw).
Network Connection Creation (DC0082)	auditd:SYSCALL	socket/bind: New bind() to a previously closed port shortly after the sequence.

Data Component	Name	Channel
Network Traffic Flow (DC0078)	NSM:Flow	Knock pattern: repeated REJ/S0 across ≥MinSequenceLen ports from same src_ip then SF success.

Mutable Elements

Field	Description
ServicePort	Candidate port expected to open after knock (e.g., 22/2323).
KnockTolerance	Max seconds between hits inside the sequence.
MgmtAllowList	Automation allowed to change firewall/daemon state (config mgmt, orchestration).

AN0844

A source performs a closed-port sequence; the endpoint enables a PF/socketfilterfw rule or a background process binds a port; then a successful connection completes from the same source.

Log Sources

Mutable Elements

Field	Description
PFAnchorPaths	Anchors/confs to monitor (/etc/pf.conf, /etc/pf.anchors/*).
DevMode	Suppress expected PF testing on developer devices.

AN0845

Router/switch receives a knock pattern (same src touches device unicast, broadcast, and network-address on same or stepped ports) followed by ACL/line-vty/service enable and the first mgmt session success.

Log Sources

Data Component	Name	Channel
Network Traffic Flow (DC0078)	networkdevice:syslog	Config/ACL changes, line vty transport input changes, telnet/ssh/http(s) enable, image/feature module changes.
Network Connection Creation (DC0082)	NSM:Flow	Series of denied/closed flows to distinct ports then success to mgmt port from same src_ip within TimeWindow.

Mutable Elements

Field	Description
MgmtPortSet	Mgmt ports to focus on: 22,23,2323,80,443,161,4786.
DeviceRole	Tighten thresholds on edge/internet-facing devices.

Source: https://attack.mitre.org/detectionstrategies/DET0302#AN0843