Detection of Non-Application Layer Protocols for C2, Detection Strategy DET0457

Archived: 2026-04-05 17:37:29 UTC

AN1254

Anomalous use of ICMP or UDP by non-network service processes for data exfiltration or remote control, especially if traffic bypasses proxy infrastructure or shows unusual flow patterns.

Log Sources

Mutable Elements

Field	Description
ProcessContextAllowList	Processes normally allowed to use ICMP/UDP (e.g., ping.exe, DNS resolver).
ByteTransferAnomalyThreshold	Suspicion if client sends much more data than it receives (e.g., >90%).
ProtocolUsageBaseline	Baseline which protocols are normal per host or segment (ICMP, UDP, etc.).

AN1255

ICMP or raw socket traffic generated by user-mode processes like bash, Python, or nc, typically using `ping`, `hping3`, or crafted packets via libpcap or scapy.

Log Sources

Mutable Elements

Field	Description
RawSocketExecutionPath	Uncommon programs using raw sockets (e.g., netcat, Python, nmap).
TimeWindow	Tunable window for correlating execution with network events (e.g., 2m).

AN1256

Unsigned binaries or interpreted scripts initiating non-standard protocols (ICMP, UDP, SOCKS) outside of baseline network behavior.

Log Sources

Mutable Elements

Field	Description
UnsignedBinaryNetworkUsage	Detection threshold for unsigned or transient binaries making ICMP/UDP calls.

AN1257

VMCI (Virtual Machine Communication Interface) traffic between guest and host, or between VMs, originating from non-management tools or unauthorized binaries.

Log Sources

Mutable Elements

Field	Description
VMCIBackdoorProcess	Monitor for non-vSphere or VMware-native processes using VMCI.
GuestToHostCommPattern	Baseline pattern of guest-to-host traffic vs anomaly (unexpected port, volume).

AN1258

Non-standard port/protocol pairings or low-entropy ICMP traffic resembling tunneling patterns (e.g., fixed-size pings with delays).

Log Sources

Mutable Elements

Field	Description
ProtocolEntropyThreshold	ICMP/UDP packet content entropy filter to identify encoded payloads.
SessionDurationThreshold	Long ICMP/UDP sessions beyond expected limits (e.g., >5min).
