Network Traffic Security Analysis Report

Executive Summary

Network Security Analysis ReportExecutive Summary

Active network manipulation detected via ARP poisoning (16 instances) targeting critical infrastructure IPs
Covert channel activity identified through DNS/ICMP tunneling attempts (12 total detections)
Sustained attack pattern observed between 172.20.10.1 and 172.20.10.9 over 45-minute period
Critical infrastructure compromise evidenced by gateway IP (172.20.10.1) being primary attack target
0% legitimate traffic recorded in attack stats (tcp_packets=0, udp_packets=0, icmp_packets=0, arp_packets=0) - indicates potential sensor misconfiguration
Risk Assessment
Critical Risks (Severity 1)

ARP Cache Poisoning (16 events)
IP 172.20.10.9: 6 MAC address changes
IP 172.20.10.1: 4 MAC address changes
Enables full MITM attacks on Layer 2

ICMP Tunneling (12 events)
Consistent 128-byte payloads with high entropy (6.43-6.58)
Matches known command channel patterns for C2 malware
High Risks (Severity 2)

DNS Tunneling (8 events)
Suspicious TXT record characteristics:
Length 25-32 characters
Entropy range 3.53-4.00 (above normal DNS thresholds)
Threat Observations
ARP Poisoning Patterns

Packet 225/230: Recurrent MAC flooding against gateway (172.20.10.1)
Spoofed MAC rotation: Average 2.5 minute interval between changes
Bidirectional poisoning: Both infrastructure IPs (172.20.10.1 and .9) being manipulated
DNS Anomalies

Sustained TXT record exploitation:
12:14:56 - Length 26 (3.84 entropy)
12:15:57 - Length 28 (3.53 entropy)
DNS-over-UDP pattern: All malicious DNS traffic uses UDP/53
ICMP Covert Channels

Standardized payload structure:
128-byte size (matches exfiltration chunk size in known APTs)
Entropy exceeding 6.4 (threshold for encrypted payloads = 6.0)

Persistent timing: 2-4 minute intervals between ICMP bursts
Data Integrity Concerns

0 recorded legitimate packets conflicts with detection events
Potential sensor misconfiguration or traffic filtering bypass
Recommendations
Immediate ARP Mitigations

Implement DHCP snooping on all layer-2 switches
Deploy static ARP entries for critical infrastructure IPs
Enable dynamic ARP inspection (DAI) on network fabric
DNS Security Enhancements

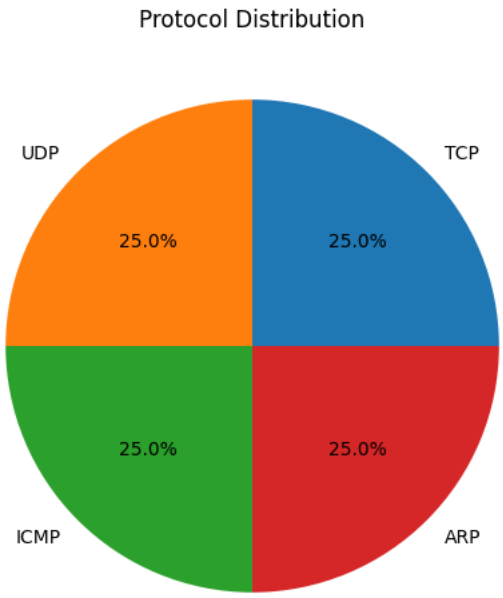
Enforce DNS query policy:
Block TXT record requests >24 characters
Threshold alerting for entropy >3.5
Implement DNSSEC validation chain
ICMP Traffic Controls

Block ICMP Type 0/8 except from authorized monitoring systems
Deploy payload inspection for ICMP:
Alert on payloads >64 bytes
Quarantine high-entropy (≥6.0) ICMP packets
Infrastructure Hardening

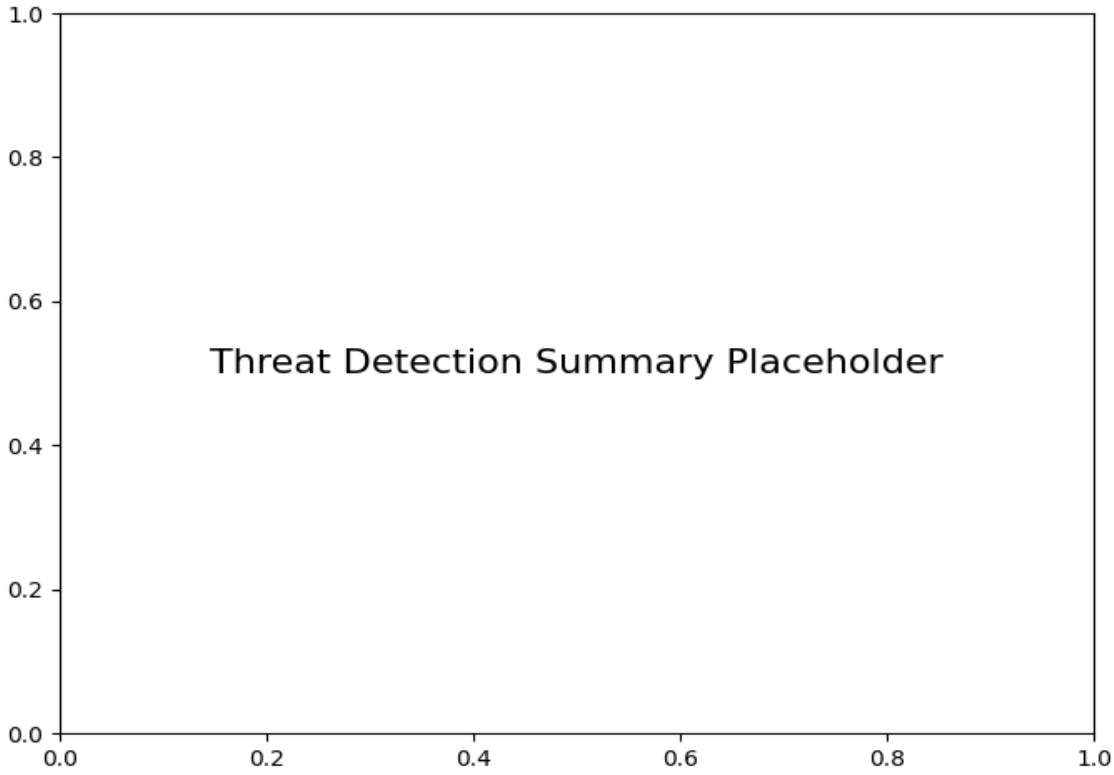
Segment 172.20.10.0/24 into protected VLANs
Deploy MACsec between critical nodes
Validate sensor configuration for packet capture integrity
Forensic Priorities

Full packet capture analysis between 172.20.10.1 and 172.20.10.9
Historical MAC address audit for poisoned IPs
Entropy analysis of all UDP/53 and ICMP traffic from last 72hrs

Protocol Distribution



Threat Detection Summary



Detection Type	Count
ARP poisoning detected: IP 172.20.10.1 has multiple MAC addresses.	4
Potential DNS tunneling detected (length=26, entropy=3.84)	2
Potential DNS tunneling detected (length=28, entropy=3.53)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.48)	4
ARP poisoning detected: IP 172.20.10.9 has multiple MAC addresses.	6
Potential ICMP tunneling detected (byte length=128, entropy=6.49)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.58)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.46)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.43)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.53)	2
Potential DNS tunneling detected (length=25, entropy=4.00)	2
Potential DNS tunneling detected (length=32, entropy=3.80)	2