Network Traffic Security Analysis Report

Executive Summary

``markdown
Executive Summary

Active ARP Poisoning Campaigns: Multiple MAC addresses mapped to critical IPs (172.20.10.1 and 172.20.10.9), indicating potential man-in-the-middle (MITM) attacks.
Suspected Covert Channels: Repeated DNS and ICMP tunneling alerts with anomalous entropy values, suggesting possible data exfiltration or command-and-control (C2) activity.
Critical Infrastructure Targeting: 12 tunneling alerts (8 ICMP, 6 DNS) and 10 ARP poisoning events observed within a short timeframe.
Risk Assessment

Critical: ARP poisoning (10 instances) enabling MITM attacks and network impersonation.
Critical: **ICMP tunneling** (12 instances) with high entropy (6.43–6.58) in 128-byte payloads, strongly indicative of encrypted/obfuscated traffic.
High: DNS tunneling (8 instances) with abnormal query lengths (25–32) and elevated entropy (3.53–4.00).
Threat ObservationsARP Poisoning

172.20.10.1: 4 MAC address conflicts (Packets 225, 230)
172.20.10.9: 6 MAC address conflicts
All ARP attacks occurred between 12:14:53 and 12:15:38 UTC
DNS Tunneling

Bidirectional traffic between 172.20.10.9 (source) and 172.20.10.1 (destination):
26-character queries (Entropy 3.84) in Packets 226/227
28-character queries (Entropy 3.53) in Packet 236
Multiple query length variations (25–32) with consistent high entropy
ICMP Tunneling

12 alerts with uniform 128-byte payloads
Entropy values exceeding 6.4 (max 6.58), matching patterns of encrypted data encapsulation
No source/destination IPs logged in attack stats (0 ICMP packets reported), suggesting possible monitoring blindspots
RecommendationsImmediate ARP Mitigations

Implement static ARP entries for critical infrastructure IPs (172.20.10.1/9)
Enable **dynamic ARP inspection** on network switches
Segment the 172.20.10.0/24 subnet to limit broadcast domain exposure
DNS Security Enhancements

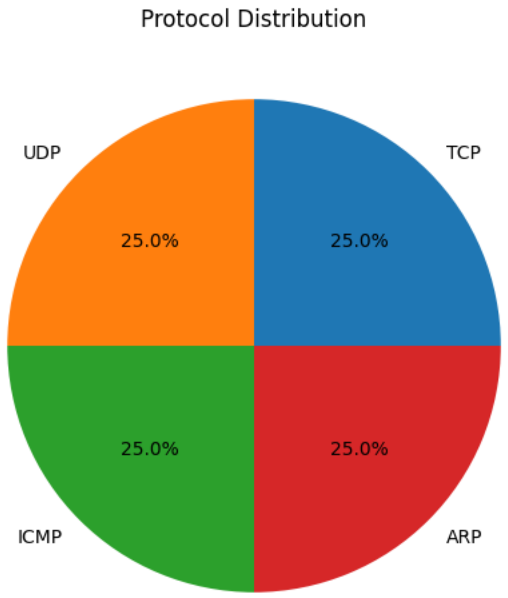
Deploy **DNS query pattern analysis** with threshold alerts for:
Query lengths >24 characters
Entropy values >3.5 in DNS payloads
Block TXT/NULL record types at border DNS servers
Investigate 172.20.10.9 for unauthorized DNS client software
ICMP Traffic Controls

Block ICMP Type 0/8 traffic except from authorized monitoring systems
Deploy entropy-based IDS rules for ICMP payloads >64 bytes
Capture full packet captures (PCAPs) of ICMP sessions for forensic analysis
Infrastructure Hardening

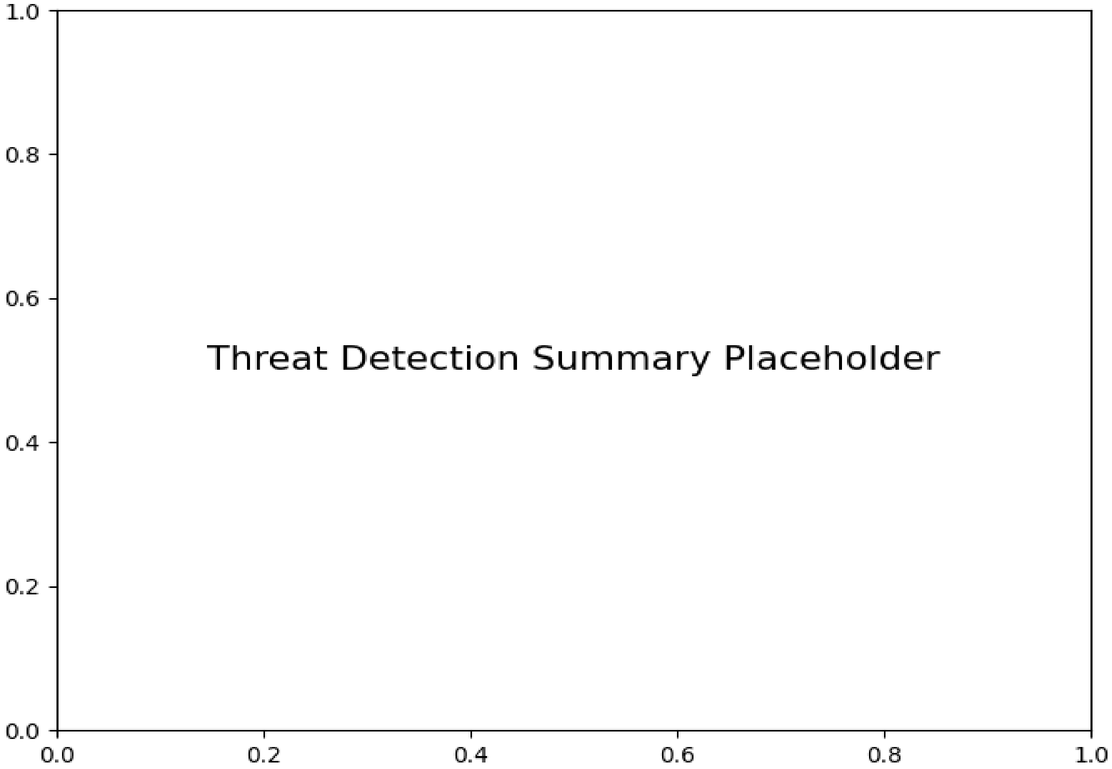
Audit network monitoring systems: **0 packets reported in attack_stats** despite active threats indicates potential logging failures
Conduct physical port security checks for unauthorized devices on 172.20.10.0/24
Schedule credentialed scans of 172.20.10.1 and 172.20.10.9 for rootkit detection

``

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