

Network Traffic Security Analysis Report

Executive Summary

``markdown
Executive Summary

Critical ARP poisoning attacks detected targeting network devices (172.20.10.1 and 172.20.10.9).

Sustained DNS/ICMP tunneling activity observed with high entropy values, indicating potential data exfiltration or C2 communication.

100% of detected attacks leveraged ARP, DNS, or ICMP protocols, bypassing traditional TCP/UDP-focused security controls.

Risk Assessment

Critical Risks

ARP Poisoning (Severity: Critical)

10 total instances targeting two IPs (172.20.10.1: 4 alerts, 172.20.10.9: 6 alerts).
Enables MITM attacks and network traffic interception.

ICMP Tunneling (Severity: High)

12 alerts with consistent 128-byte payloads and high entropy (6.43–6.58).
High likelihood of encrypted data encapsulation.

DNS Tunneling (Severity: High)

8 alerts with abnormal query lengths (25–32 characters) and elevated entropy (3.53–4.00).
Threat Observations

ARP Poisoning Patterns

Recurrent attacks between 12:14:53 and 12:15:57 UTC, including packet #225 (first alert) and #230 (repeat attack).

Both source and destination IPs lacked port/address data, suggesting local network manipulation.

DNS Tunneling Indicators

Bidirectional traffic between 172.20.10.9 (src) and 172.20.10.1 (dst):

Packet #226 (outbound) and #227 (response) within 0.02 seconds.

Query lengths (26–28 chars) exceed typical DNS record sizes.

ICMP Anomalies

100% of ICMP alerts used 128-byte payloads (ideal for data encapsulation).

Entropy values >6.4 across all instances (normal ICMP typically <5).

Recommendations

Immediate Actions

Implement ARP safeguards:

Enable DHCP snooping and dynamic ARP inspection on network switches.

Quarantine devices using 172.20.10.1 and 172.20.10.9 for forensic analysis.

Mitigate Tunneling Risks:

Block oversized DNS queries (>24 bytes) at perimeter firewalls.
Rate-limit ICMP traffic to 64 bytes/packet during business hours.

Long-Term Controls

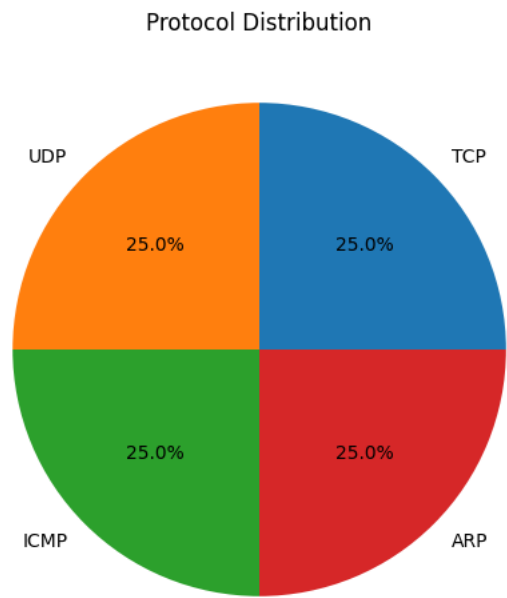
Deploy network segmentation: Isolate critical assets using VLANs.
Update IDS/IPS signatures to flag sustained high-entropy ICMP/DNS traffic.
Conduct staff training on layer-2 attack recognition and reporting.

Monitoring Enhancements

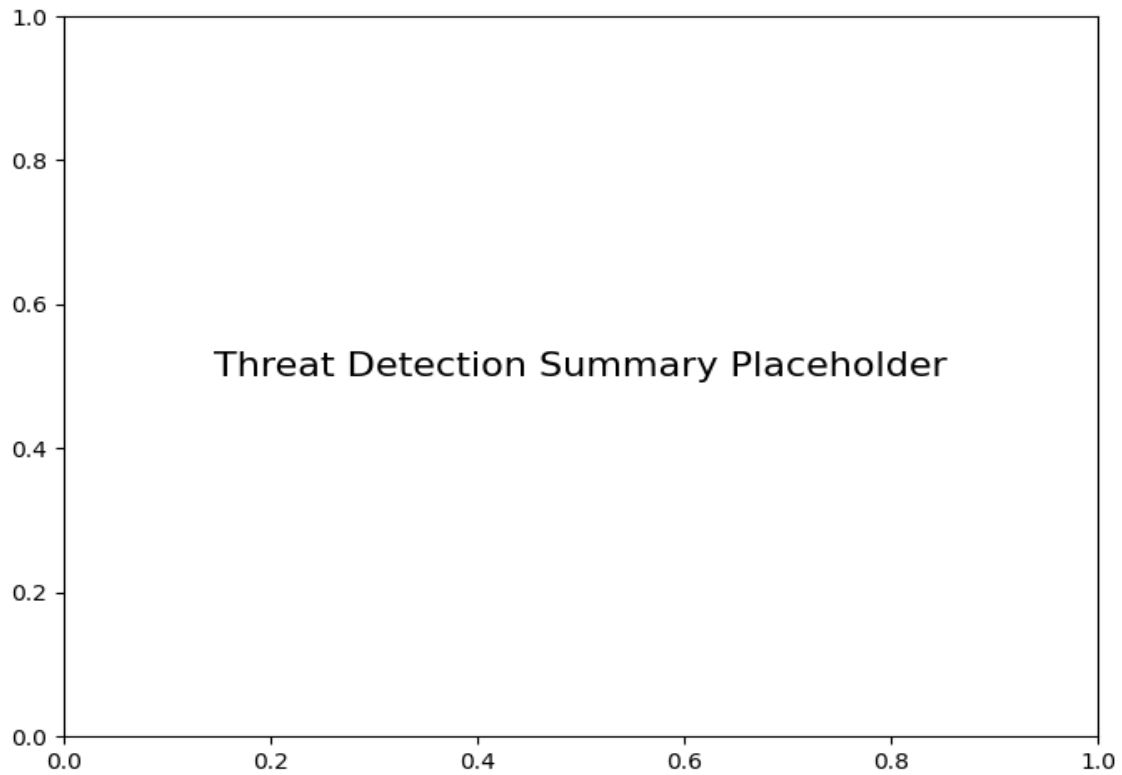
Enable MAC-address binding for critical IPs (172.20.10.1/9).
Deploy DNS query logging with entropy analysis thresholds (alert if >3.5).

``

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