

# Network Traffic Security Analysis Report

## Executive Summary

Network Traffic Security Analysis Report1. Executive Summary

**Primary Threats Detected:** ARP poisoning attacks and DNS tunneling attempts.

**Key Statistics:**

**4 ARP poisoning alerts** targeting IP 172.20.10.1 and **6 alerts** for IP 172.20.10.9.

**8 DNS tunneling alerts** with anomalous payload characteristics (lengths 25–32, entropy 3.53–4.00).

**Attack Vectors:** No TCP/UDP/ICMP-based attacks observed; threats focused on ARP/DNS protocol abuse.

2. Risk Assessment

**Critical Risks:**

**ARP Poisoning (Severity: Critical):** Multiple MAC addresses mapped to critical IPs (172.20.10.1 and 172.20.10.9), enabling MITM attacks.

**DNS Tunneling (Severity: High):** High entropy and long payloads suggest covert data exfiltration/C2 activity.

**Other Observations:**

ARP packets dominate attack traffic (0 TCP/UDP/ICMP attack packets reported).

3. Threat Observations

ARP Poisoning

**IP 172.20.10.1:** 4 instances of MAC address spoofing (e.g., Packet #225, #230).

**IP 172.20.10.9:** 6 instances of MAC address spoofing, indicating persistent attacker focus.

**Traffic Pattern:** ARP packets lack source/destination IPs (typical of layer-2 attacks).

DNS Tunneling

**Anomalous DNS Queries:**

Bidirectional traffic between 172.20.10.9 (client) and 172.20.10.1 (server) (Packets #226, #227, #236).

Payload characteristics:

Lengths 25–32 (unusually long for standard DNS).

High entropy (3.53–4.00), suggesting encrypted/compressed data.

4. Recommendations

ARP Poisoning Mitigation

**Implement Dynamic ARP Inspection (DAI):** Enforce valid MAC-IP bindings on network switches.

**Deploy Static ARP Entries:** For critical devices (e.g., 172.20.10.1 and 172.20.10.9).

**Segment Network:** Isolate sensitive subnets to limit ARP spoofing impact.

DNS Tunneling Mitigation

**Enforce DNS Query Monitoring:** Flag/block queries with:

Payloads > 20 characters.

Entropy thresholds > 3.5.

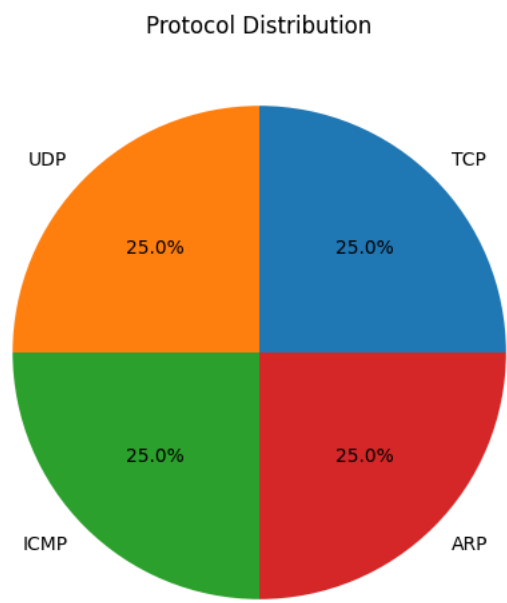
**Restrict External DNS Resolvers:** Allow only authorized DNS servers.

**Enable DNSSEC:** Validate DNS response integrity.

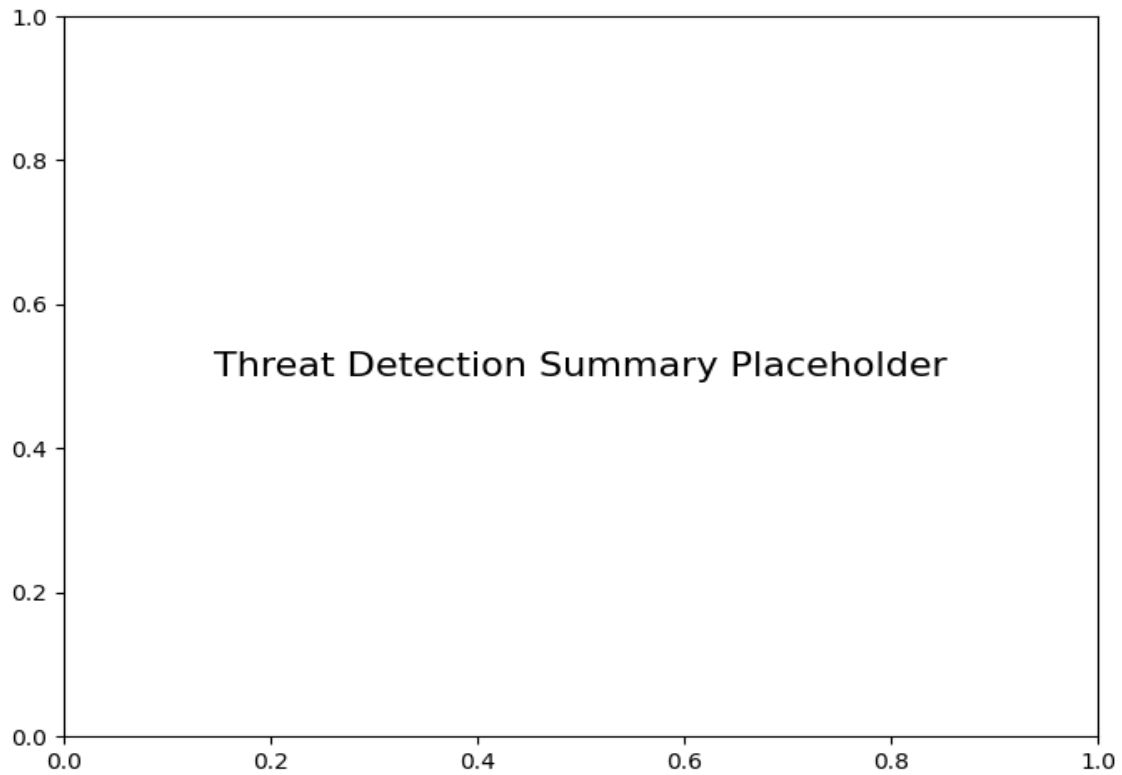
General Actions

**Enhance Network Monitoring:** Deploy IDS/IPS with ARP/DNS anomaly detection rules.  
**Conduct Forensic Analysis:** Inspect 172.20.10.9 for malware/unauthorized tools.  
**Staff Training:** Educate teams on layer-2 attack indicators and DNS abuse tactics.

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
ARP poisoning detected: IP 172.20.10.9 has multiple MAC addresses.	6
Potential DNS tunneling detected (length=25, entropy=4.00)	2
Potential DNS tunneling detected (length=32, entropy=3.80)	2