Network Traffic Security Analysis Report

Executive Summary

``markdown
Executive Summary

Multiple high-risk threats detected across the network, including ARP poisoning and DNS tunneling attempts.
ARP spoofing campaigns targeting critical IPs (172.20.10.1 and 172.20.10.9) observed with 10 total incidents.
DNS tunneling activity detected in 8 instances, suggesting potential data exfiltration or C2 communication.
No TCP/ICMP attack traffic recorded; threats focused on ARP/UDP-DNS layers.
Risk Assessment
Critical Risks

ARP Poisoning (Severity: Critical)
IP 172.20.10.1: 4 MAC address conflicts
IP 172.20.10.9: 6 MAC address conflicts
Enables MITM attacks, session hijacking, and network disruption.

DNS Tunneling (Severity: High)
8 suspicious DNS queries with abnormal characteristics:
High entropy values (3.53–4.00)
Long payloads (25–32 characters)
Indicates potential covert data channels.
Attack Vector Statistics

ARP: 0 packets (normal traffic) but 10 malicious ARP events detected
DNS-over-UDP: All tunneling attempts used UDP transport
Threat Observations
ARP Poisoning Patterns

Recurring spoofing events between packets #225–230:
Packet #225: First poisoning attempt against 172.20.10.1 (12:14:53 UTC)
Packet #230: Repeat attack on same IP 45 seconds later
No IP-layer data in ARP packets, suggesting protocol-level spoofing.
DNS Tunneling Indicators

Bidirectional traffic between 172.20.10.9 (source) and 172.20.10.1 (destination):
Packet #226: Outbound DNS query (length=26, entropy=3.84)
Packet #227: Inbound response matching same metrics
Packet #236: Follow-up query with modified parameters (length=28)
Entropy thresholds exceeded: Normal DNS typically has entropy ≤3.2.
Recommendations
ARP Mitigation

Implement dynamic ARP inspection on network switches to validate MAC/IP bindings.
Deploy **ARPwatch** or similar monitoring for real-time poisoning alerts.

Segment critical devices (172.20.10.1/172.20.10.9) into separate VLANs.
DNS Security Enhancements

Block oversized DNS queries (>24 characters) via firewall rules.
Deploy **DNS filtering solutions** (Cisco Umbrella, DNSFilter) to detect tunneling patterns.
Enable DNS logging and analyze for:
High-entropy domain names
Uncommon record types (TXT, NULL)
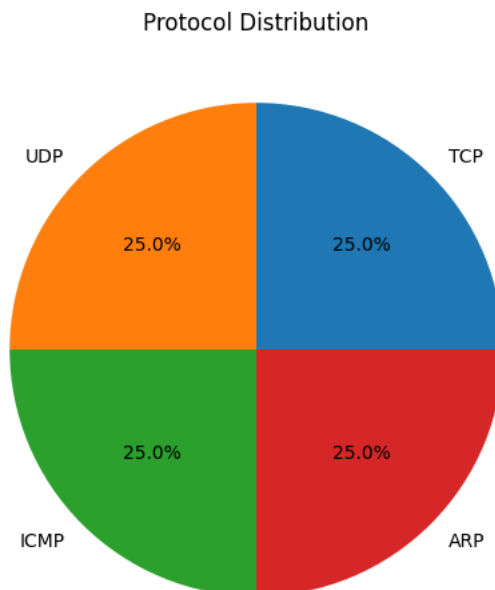Frequent requests to non-business domains
Network Hardening

Enable port security to limit MAC address changes per switch port.
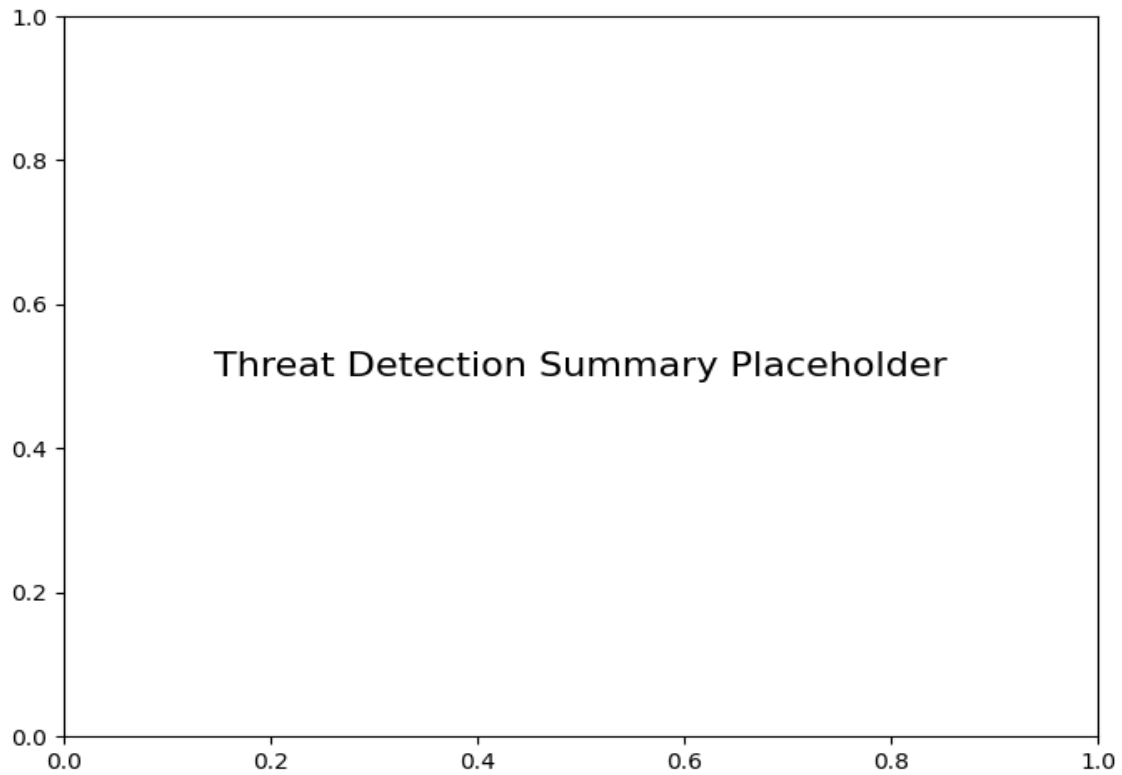**Enforce DNSSEC** to prevent DNS cache poisoning and tunneling abuse.
Isolate suspicious endpoints: Quarantine 172.20.10.9 for forensic analysis.

``

Protocol Distribution

Protocol Distribution

Threat Detection Summary

Threat Detection Summary Placeholder

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