Network Traffic Security Analysis Report

Executive Summary

Network Traffic Security Analysis Report1. Executive Summary

Multiple high-risk threats detected, including ARP poisoning (10 instances) and tunneling activities (12 instances).
ARP spoofing targets critical IPs (172.20.10.1 and 172.20.10.9), indicating potential MITM (Man-in-the-Middle) attacks.
DNS/ICMP tunneling detected with anomalous payload characteristics (high entropy, unusual lengths), suggesting data exfiltration or C2 communication.
Zero TCP/UDP/ICMP/ARP attack packets reported in attack_stats, but **suspicious activity persists in protocol-specific detections**.
2. Risk Assessment
Critical Vulnerabilities

ARP Poisoning (Severity: Critical)
IPs **172.20.10.1** (4 detections) and **172.20.10.9** (6 detections) mapped to multiple MAC addresses, enabling traffic interception.
DNS Tunneling (Severity: High)
8 detections with abnormal query lengths (25–32) and high entropy (3.53–4.00), indicative of covert data channels.
ICMP Tunneling (Severity: High)
12 detections of 128-byte payloads with entropy >6.4, consistent with encrypted/obfuscated traffic.
3. Threat Observations
ARP Poisoning

IP 172.20.10.9 exhibited the highest frequency (6 detections), suggesting persistent attacker focus.
Packets #225 and #230 targeted IP 172.20.10.1 (ARP protocol), occurring within 45 seconds (12:14:53 to 12:15:38).
DNS Tunneling

Bidirectional traffic between **172.20.10.9 (source)** and **172.20.10.1 (destination)** (e.g., Packets #226, #227, #236).
Entropy values (3.53–4.00) exceed typical DNS query randomness thresholds (normal: <3.0).
ICMP Tunneling

Uniform payload length (128 bytes) and consistently high entropy (6.43–6.58), aligning with tunneling tools like ICMPTX or Ptunnel.
Top Threat Examples

Packet #225: ARP poisoning targeting 172.20.10.1.
Packet #226/227: DNS tunneling with length=26, entropy=3.84.
Packet #236: DNS tunneling with length=28, entropy=3.53.
4. Recommendations
Immediate Actions

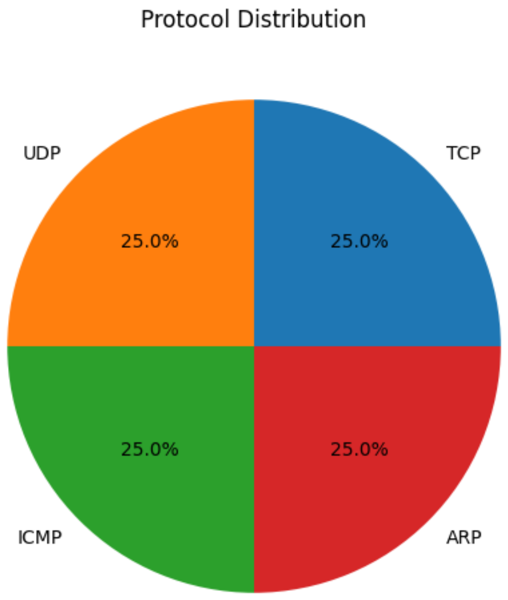
Isolate IPs 172.20.10.1 and 172.20.10.9 for forensic analysis and MAC address validation.
Implement ARP inspection via DHCP snooping or static ARP entries to mitigate spoofing.
Block ICMP payloads >64 bytes and monitor ICMP traffic for entropy anomalies.
DNS Hardening

Enforce DNS query length limits (e.g., reject queries >32 bytes) and inspect high-entropy requests.
Deploy DNS filtering solutions (e.g., DNSFirewall) to detect/block tunneling tools.
Network Monitoring Enhancements

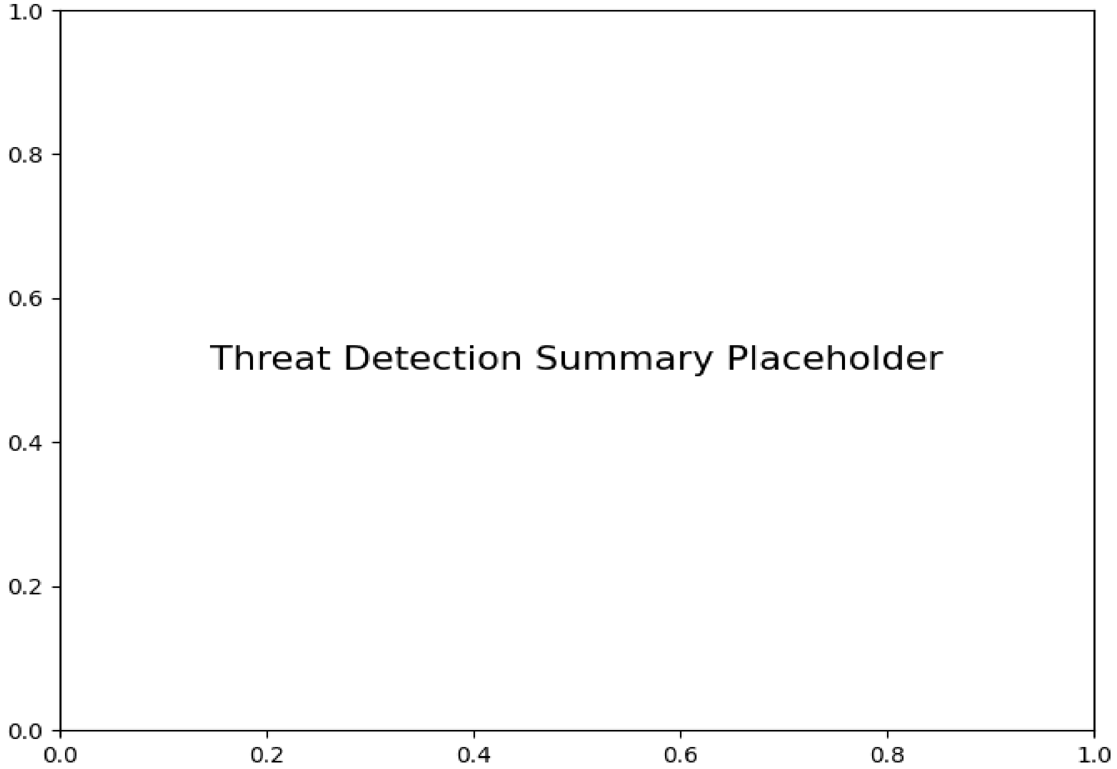
Enable deep packet inspection (DPI) for ICMP and DNS protocols.
Deploy anomaly detection tools to flag entropy deviations in payloads.
Long-Term Strategies

Segment the network to limit lateral movement post-ARP spoofing.
Conduct red-team exercises to test defenses against tunneling attacks.
Update incident response playbooks to include entropy-based detection workflows.

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