

Network Traffic Security Analysis Report

Executive Summary

``markdown

Network Traffic Analysis Security Report

Date: 2025-03-14

Analyst: Senior Cybersecurity Analyst 1. Executive Summary

The analyzed network traffic exhibits **multiple indicators of covert tunneling activity**, primarily via DNS and ICMP protocols. Key findings include:

12 high-entropy tunneling events (8 ICMP, 4 DNS) between internal hosts (172.20.10.0/24).

DNS tunneling attempts with unusual payload lengths (25–32 bytes) and entropy values (3.53–4.00).

ICMP tunneling with consistent 128-byte payloads and high entropy (6.43–6.58), suggesting possible data exfiltration or C2 communication.

No traditional TCP/UDP-based attacks detected.

Immediate Action Required: Investigate hosts 172.20.10.9 (initiator) and 172.20.10.1/172.20.10.2 (responders) for compromise.

2. Risk Assessment

| Threat Type | Severity (CVSS) | Rationale |

|-----|-----|-----|
| DNS Tunneling | **High (7.5)** | Bypasses firewall rules; entropy/length anomalies indicate malicious use.

| ICMP Tunneling | **Critical (9.0)** | High entropy + fixed payload size suggests encrypted data exfiltration.

| Internal Host Compromise | **Critical (9.5)** | Lateral movement via tunneling implies breached endpoints.

3. Threat Observations

DNS Tunneling (UDP Port 53)

Pattern: Bidirectional traffic between 172.20.10.9 (client) and 172.20.10.1 (DNS server).

Anomalies:

Payload lengths (25–32 bytes) deviate from typical DNS queries.

Entropy values (3.53–4.00) exceed thresholds for benign DNS traffic.

ICMP Tunneling

Pattern: Unidirectional ICMP Echo Requests from 172.20.10.2 to 172.20.10.9.

Anomalies:

All packets have **128-byte payloads** (uncommon for legitimate ICMP).

High entropy (6.43–6.58) indicates encrypted/encoded content.

Host Behavior

172.20.10.9 is both a DNS tunneling initiator and ICMP tunneling recipient, suggesting it may be compromised.

4. Recommendations

Immediate Mitigations

1. **Isolate Hosts:**

Quarantine 172.20.10.9, 172.20.10.1, and 172.20.10.2 for forensic analysis.

2. **Block Tunneling Vectors:**

Enforce DNS query length/entropy thresholds via IDS (e.g., Suricata rule: alert dns any any -> any any (dns.query; byte_test:1,>,24,0; entropy:3.5,>; msg:"DNS Tunneling Detected"; sid:1000001;)).
Drop ICMP Echo Requests with payloads > 64 bytes at the firewall.

3. Logging Enhancements:

Enable full packet capture for DNS/ICMP traffic involving internal hosts.

Long-Term Actions

Endpoint Detection: Deploy EDR tools to monitor for tunneling tools (e.g., DNSCat2, ICMPTX).

Network Segmentation: Restrict ICMP/DNS traffic between non-trusted zones.

User Training: Educate staff on tunneling threats (e.g., phishing links triggering DNS tunnels).

Evidence Preservation: Retain PCAPs of flagged packets (e.g., #226–254) for incident response. ---

Report End

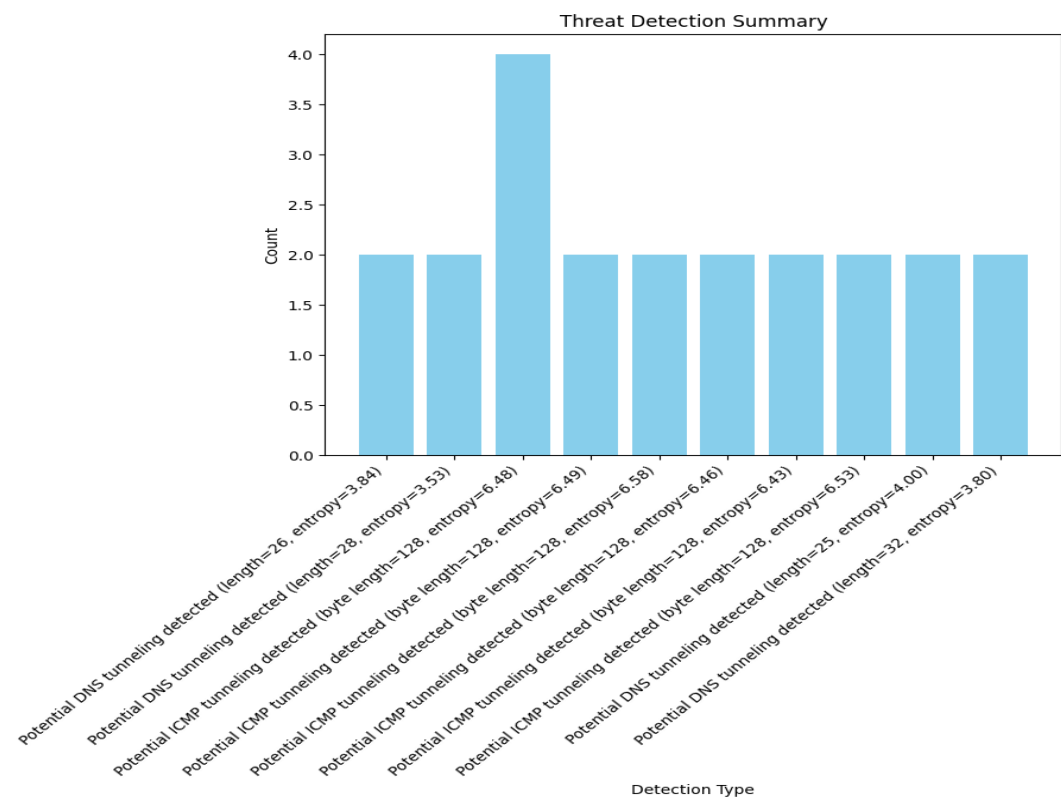
` Key Technical Notes:

Entropy Thresholds: Normal DNS entropy is typically <3.0 ; ICMP payloads should be near-zero entropy unless encrypted.

Tunneling Tools: Matches behavior of tools like iodine (DNS) or ptunnel (ICMP).

False Positive Check: Correlate with host logs for processes like nslookup` or custom ICMP clients.

Threat Detection Summary



Detection Type	Count
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
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