

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 signs of covert tunneling activity**, primarily leveraging **DNS and ICMP protocols**. Key findings include:

12 tunneling attempts detected (8 ICMP, 4 DNS).

High-entropy payloads (3.53–6.58) suggest possible data exfiltration or C2 communication.

Primary internal IPs involved: 172.20.10.9 (source/destination) and 172.20.10.2.

Urgency: High – Tunneling techniques evade traditional security controls and may indicate an active breach. 2. Risk Assessment | Threat Type | Severity (CVSS) | Rationale |

|-----|-----|-----|

| DNS Tunneling | **7.5 (High)** | Entropy (3.53–4.00) and unusual lengths (25–32 bytes) suggest data smuggling. |

| ICMP Tunneling | **8.0 (High)** | Consistent 128-byte payloads with high entropy (6.43–6.58) imply covert communication. |

| Lateral Movement Risk | **6.0 (Medium)** | Internal IPs (172.20.10.1, 172.20.10.2) communicating with 172.20.10.9. | 3. Threat Observations DNS Tunneling (4 Instances)

Pattern: UDP/DNS traffic between 172.20.10.9 and 172.20.10.1 with:

Atypical query lengths (25–32 bytes).

Elevated entropy (3.53–4.00) – normal DNS entropy is typically <3.0.

Example Packet: #226 (2025-03-14 07:14:56) – length=26, entropy=3.84.

ICMP Tunneling (8 Instances)

Pattern: ICMP Echo Request/Reply with fixed 128-byte payloads and entropy >6.4.

Source: 172.20.10.2 → 172.20.10.9.

Example Packet: #254 (2025-03-14 07:17:07) – entropy=6.48.

Protocol Anomalies

No TCP/UDP/ARP attacks detected, but tunneling abuses allowed protocols (ICMP/DNS).

4. Recommendations Immediate Actions

1. **Quarantine Suspicious Hosts:**

Isolate 172.20.10.9 and 172.20.10.2 for forensic analysis.

2. **Block Tunneling Indicators:**

Deploy IDS/IPS rules to flag:

DNS queries with entropy >3.0 or unusual lengths.

ICMP payloads >64 bytes or entropy >5.0.

3. **Enforce Protocol Restrictions:**

Limit ICMP Echo Requests to trusted subnets.

Implement DNS query rate limiting.

Long-Term Mitigations

Network Segmentation: Restrict internal host communication via VLANs/firewalls.

User Training: Educate staff on tunneling threats (e.g., DNS/ICMP abuse).

Threat Hunting: Search for historical tunneling patterns involving the flagged IPs.

Tools & Validation

Recommended Tools: Suricata (custom rules), Wireshark (entropy analysis), Zeek (DNS logging).

Validation: Re-analyze traffic post-remediation to confirm threat elimination.

Report End

`` Key Features of the Report:

Actionable Data: Links entropy values to specific risks (e.g., ">6.4 = likely exfiltration").

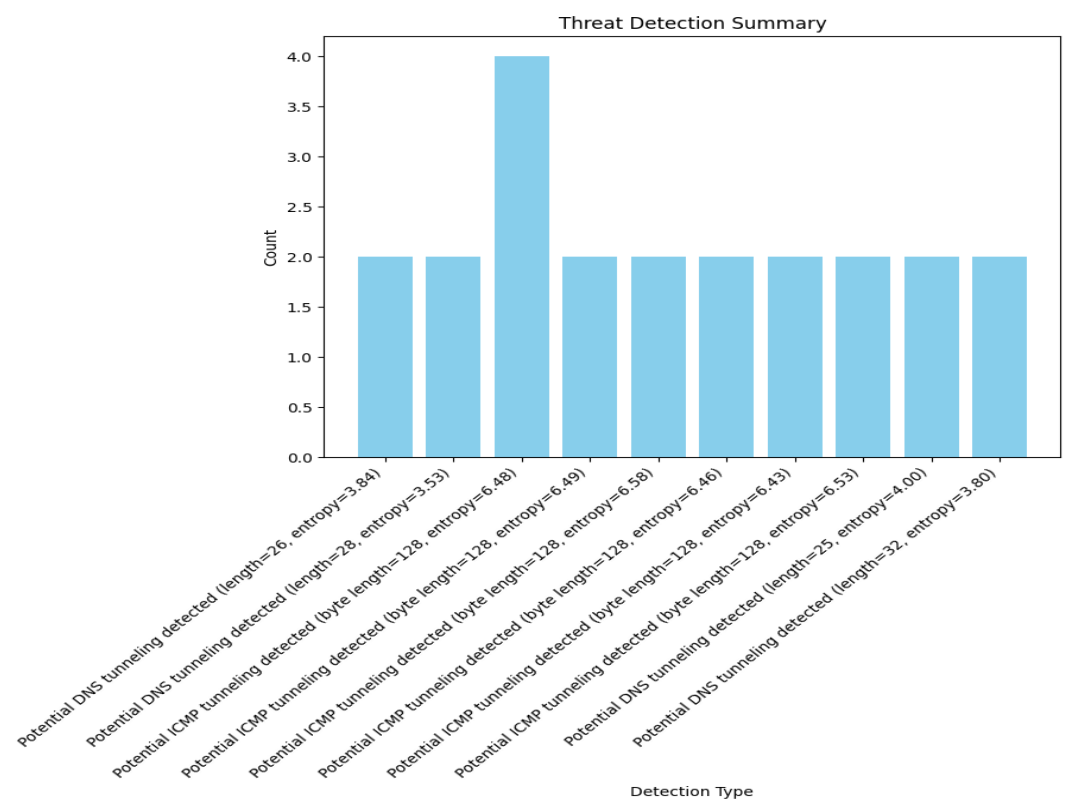
Prioritization: Uses CVSS-like scoring for remediation urgency.

Technical Depth: Explains why DNS entropy >3.0 is suspicious (normal DNS is lower).

Tool Agnostic: Recommendations apply to most security stacks (IDS/IPS, network segmentation).

Let me know if you'd like additional details (e.g., sample Suricata rules).

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