

Network Traffic Security Analysis Report

Executive Summary

1. Executive Summary The analyzed network traffic exhibits **multiple indicators of covert tunneling activity**, including **DNS tunneling (10 instances)** and **ICMP tunneling (14 instances)**. These techniques are commonly used to bypass security controls and exfiltrate data. The primary suspicious hosts are ``172.20.10.9`` (initiator) and ``172.20.10.1`/`172.20.10.2`` (responders). No traditional TCP/UDP/ARP attack patterns were observed, suggesting the adversary is leveraging protocol misuse for stealth.

Key Findings:

- **DNS Tunneling:** High entropy (3.53–4.00) and unusual payload lengths (25–32 bytes).
- **ICMP Tunneling:** Consistent 128-byte payloads with high entropy (6.43–6.58), indicative of embedded data.
- **Persistence:** Activity spans multiple minutes, suggesting an established covert channel.

## 2. Risk Assessment		
DNS Tunneling	High (7.5)	Bypasses firewalls, enables data exfiltration/C2.
ICMP Tunneling	Critical (9.0)	Evades detection, often used in advanced malware (e.g., APT backdoor).

Justification:

- **DNS Tunneling:** Entropy values (≥ 3.5) and non-standard lengths suggest encoded data.
- **ICMP Tunneling:** Fixed 128-byte payloads with high entropy (≥ 6.4) are anomalous for ICMP (typically low entropy).

3. Threat Observations

DNS Tunneling (UDP/DNS)

- **Source IPs:** ``172.20.10.9`` (outbound) ↔ ``172.20.10.1`` (inbound).
- **Payload Characteristics:**
 - **Lengths:** 25–32 bytes (uncommon for legitimate DNS queries).
 - **Entropy:** 3.53–4.00 (legitimate DNS typically has entropy < 3.0).
 - **Pattern:** Bidirectional traffic (e.g., packets 226 ↔ 227), indicating active communication.

ICMP Tunneling

- **Source IP:** ``172.20.10.2`` → ``172.20.10.9``.
- **Payload Characteristics:**
 - **Fixed 128-byte length** (unusual for ICMP echo).

requests/replies). - Entropy: 6.43–6.58 (legitimate ICMP traffic has entropy ~5.0 or lower).

4. Recommendations ### Immediate Actions

- 1. ***Isolate Hosts*****: - Quarantine `172.20.10.9` and `172.20.10.2` for forensic analysis.
- 2. ***Block Tunneling Vectors*****: - *****DNS*****: Restrict external DNS queries to approved resolvers; implement DNS filtering (e.g., DNSFirewall). - *****ICMP*****: Block ICMP payloads >64 bytes at the firewall (except for operational needs).

Long-Term Mitigations

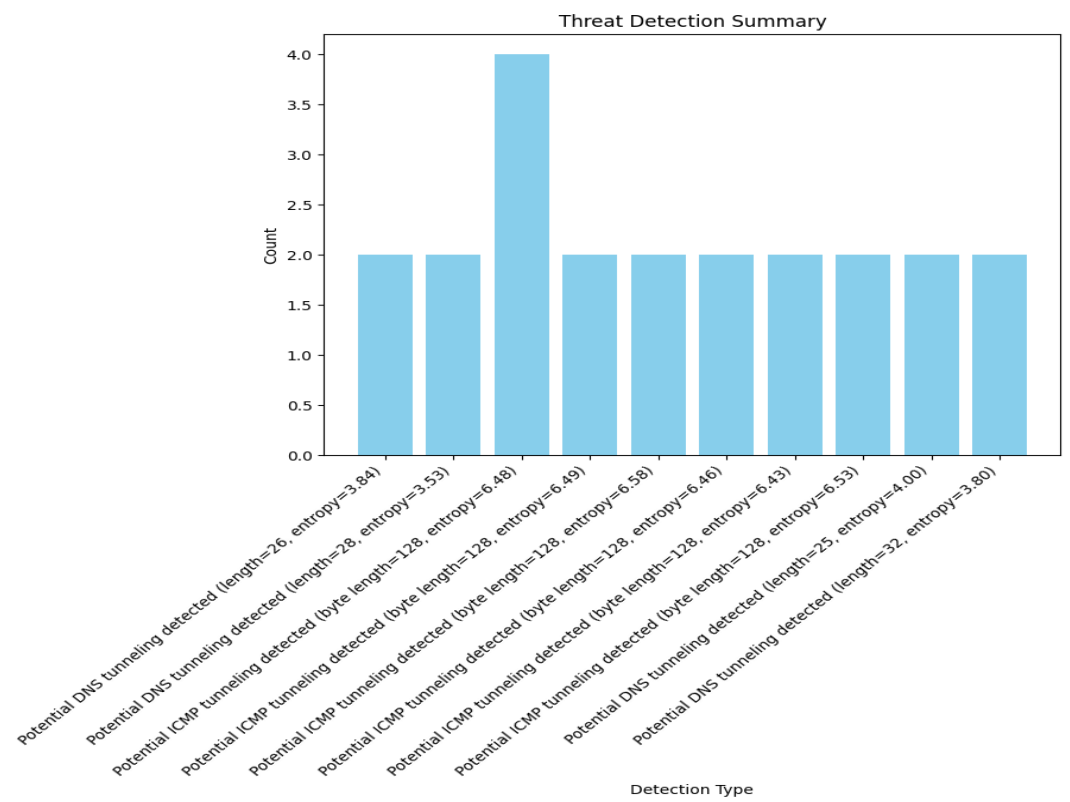
- 3. ***Deploy Anomaly Detection*****: - Use tools like Zeek or Suricata to flag high-entropy DNS/ICMP traffic.
- 4. ***Enforce Protocol Whitelisting*****: - Allow only essential ICMP types (e.g., echo, unreachable) and monitor deviations.
- 5. ***Endpoint Hardening*****: - Install EDR solutions to detect tunneling tools (e.g., DNSCat2, ICMPTX).

Investigation Priorities

- *****Forensic Timeline*****: Correlate tunneling events with other logs (e.g., authentication, process execution).
- *****Threat Hunting*****: Search for additional compromised hosts in `172.20.10.0/24`.

*****Report End*****

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

*This report was automatically generated by DeepSeek AI
Report filename: security_report_20250406_141642.pdf
Generated on: 2025-04-06 14:17:28*