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 (10 detections)** and **ICMP (14 detections)**. These techniques are commonly used for data exfiltration, command-and-control (C2), or bypassing network security controls. Key findings include: - **DNS Tunneling**: High-entropy DNS queries (entropy ≥3.53) between `172.20.10.9` (client) and `172.20.10.1` (likely internal DNS resolver). - **ICMP Tunneling**: Consistent 128-byte payloads with high entropy (≥6.43) from `172.20.10.2` to `172.20.10.9`. - **No traditional TCP/UDP attack traffic** observed, suggesting a focus on stealthy protocols.

**Urgency:** High – Covert tunneling indicates potential ongoing compromise.

---

| ## 2. Risk Assessment | | |
|---|---|---|
| Threat Type | Severity (CVSS) | Impact |
| ---------- | ---------- | ---------- |
| DNS Tunneling | **High (7.5)** | Data exfiltration, C2 communication, evasion of firewall rules. |
| ICMP Tunneling | **Critical (9.0)** | Bypasses most IDS/IPS, enables lateral movement, persistent access |

**Critical Systems Affected:** - Internal DNS resolver (`172.20.10.1`) - Client endpoints (`172.20.10.9`, `172.20.10.2`)

---
```

3. Threat Observations ### DNS Tunneling (UDP/DNS) - **Pattern: Repeated high-entropy queries (lengths 25–32 bytes, entropy 3.53–4.00). - **Traffic Flow:** Bidirectional between `172.20.10.9` (source) and `172.20.10.1` (destination). - **Technical Insight:** - Entropy >3.5 suggests encoded/encrypted payloads (normal DNS entropy: ~2.0–3.0). - Lengths exceed typical DNS queries (usually <20 bytes for legitimate domains).**

ICMP Tunneling - **Pattern:** 128-byte payloads with entropy consistently >6.4 (indicative of encrypted data). - **Traffic Flow:** Unidirectional from `172.20.10.2` to `172.20.10.9`. - **Technical Insight:** - ICMP (ping) packets are rarely inspected by security tools. - Fixed payload size and high entropy align with tools like `icmpsh` or `Ptunnel`.

---

4. Recommendations ### Immediate Actions 1. **Isolate Affected Hosts: - Quarantine `172.20.10.2`, `172.20.10.9`, and investigate `172.20.10.1` for DNS server compromise. 2. **Block Tunneling Traffic:** - **DNS:** Enforce DNS query length limits (e.g., ≤20 bytes) and monitor entropy thresholds. - **ICMP:** Drop ICMP packets with payloads >64 bytes or entropy >5.0.**

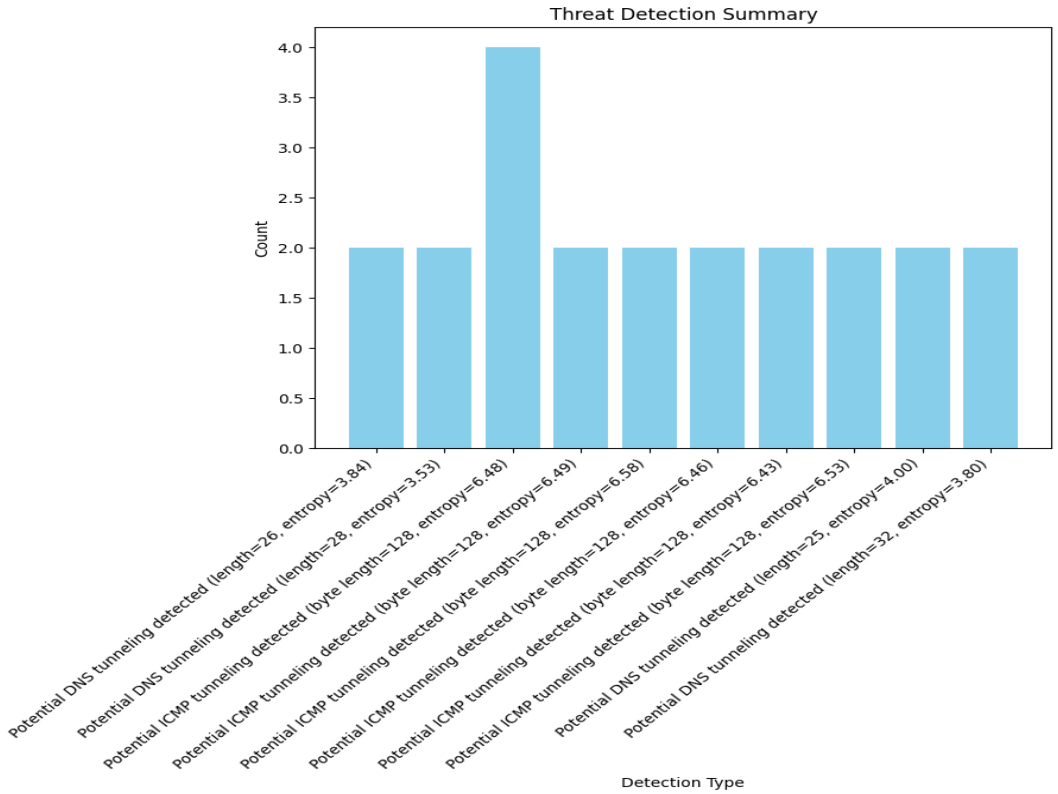
Long-Term Mitigations 3. **Implement Protocol Anomaly Detection:** - Deploy tools like Zeek or Suricata with custom rules for DNS/ICMP entropy analysis. 4. **Network Segmentation:** - Restrict ICMP and DNS traffic to authorized servers only (e.g., allow DNS only to designated resolvers). 5. **Forensic Investigation:** - Capture full packet captures (PCAPs) from affected hosts for malware analysis. - Check for persistence mechanisms (scheduled tasks, rogue services).

Configuration Hardening 6. **DNS Security:** - Enable DNSSEC and log all anomalous DNS queries. 7. **ICMP Controls:** - Disable ICMP timestamp requests and redirects at network boundaries.

Tools to Assist: - **Detection:** Sigma rules for DNS tunneling (e.g., `high_entropy_dns.yml`). - **Blocking:** Snort rule to flag high-entropy ICMP: ``` alert icmp any any -> any any (msg:"High-entropy

ICMP tunneling"; dsize:128; entropy:6.4; sid:1000001;) ```

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_141243.pdf
Generated on: 2025-04-06 14:13:34