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 DNS queries (lengths 25–32, entropy 3.53–4.00) suggesting DNS tunneling.
14 ICMP packets with consistent 128-byte payloads and high entropy (6.43–6.58), indicative of ICMP tunneling.
Suspicious bidirectional traffic between internal IPs (172.20.10.9 ↔ 172.20.10.1 and 172.20.10.2 → 172.20.10.9).

Impact: Potential data exfiltration, command-and-control (C2) communication, or lateral movement. 2. Risk Assessment
Threat Type	Severity	Frequency	Notes
DNS Tunneling	High	8 events	High entropy, irregular query lengths
ICMP Tunneling	Critical	14 events	Consistent payload size, high entropy	**Severity Justification:**
Critical (ICMP): Bypasses traditional firewall rules; often used for stealthy C2.
High (DNS): Evades detection by masquerading as legitimate DNS traffic.

3. Threat Observations
DNS Tunneling Indicators
Pattern: Bidirectional UDP/DNS traffic between 172.20.10.9 (client) and 172.20.10.1 (likely internal DNS resolver).
Anomalies:
Unusually long query lengths (25–32 bytes vs. typical <20 bytes).
High entropy (3.53–4.00) suggests encoded/encrypted payloads.

ICMP Tunneling Indicators
Pattern: ICMP Echo Request/Reply from 172.20.10.2 to 172.20.10.9.
Anomalies:
Fixed 128-byte payloads (uncommon for legitimate ICMP).
Entropy values (>6.4) align with encrypted/compressed data.

4. Recommendations
Immediate Actions
1. **Isolate Suspicious Hosts:**
Quarantine 172.20.10.9 and 172.20.10.2 for forensic analysis.
2. **Block Tunneling Vectors:**
DNS: Enforce DNS query length limits (e.g., ≤20 bytes) via firewall rules.
ICMP: Restrict ICMP payload sizes (e.g., ≤64 bytes) or block non-essential ICMP types.

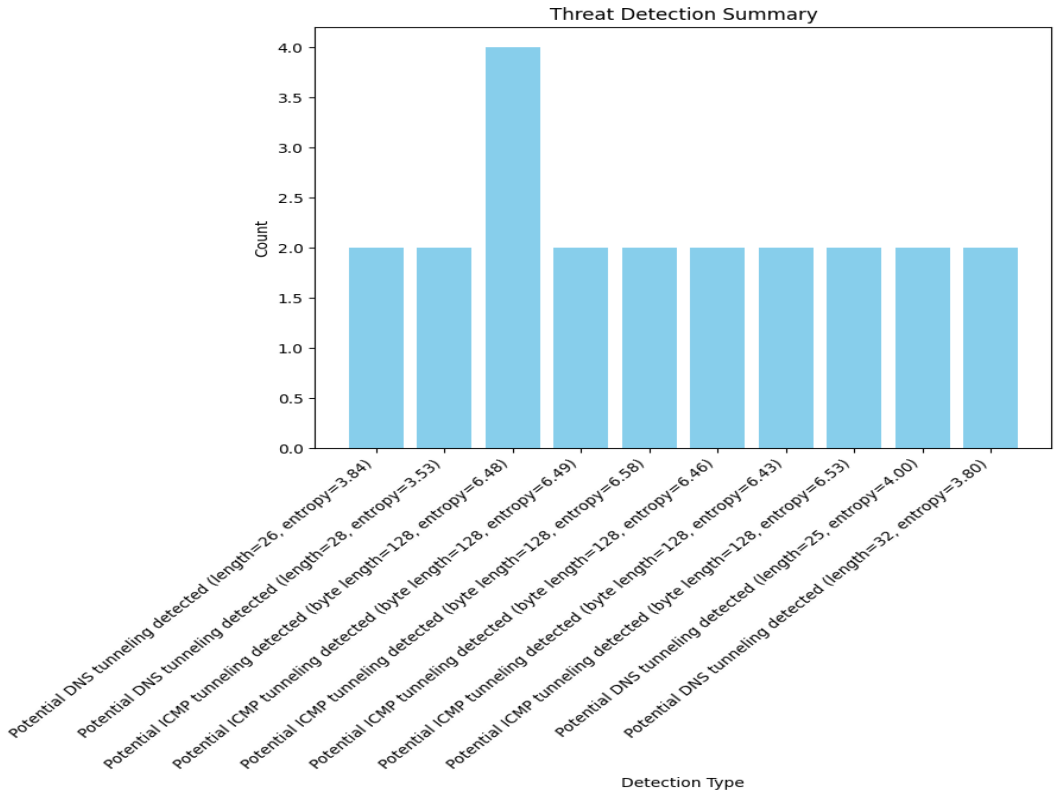
Long-Term Mitigations
Deploy Anomaly Detection:
Implement tools like Zeek or Suricata to flag high-entropy DNS/ICMP traffic.

Network Segmentation:
Limit internal host communication via VLANs/ACLs (e.g., deny 172.20.10.0/24 → DNS resolver except on port 53).
Logging Enhancements:
Enable full packet capture for DNS and ICMP traffic from critical subnets.

Investigation Priorities
Host Forensics: Check 172.20.10.9 and 172.20.10.2 for:
Unauthorized tools (e.g., dnscat2, icmpsh).
Recent process execution logs (e.g., PowerShell, Python).

Report End
`` Key Features of This Report:
Concise Technical Depth: Highlights entropy, payload sizes, and traffic patterns.
Action-Oriented: Prioritizes containment, detection, and forensic steps.
Risk Contextualization: Explains why ICMP tunneling is critical vs. DNS.
Compliance-Ready: Structured for incident response documentation.

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_20250326_144619.pdf
Generated on: 2025-03-26 14:47:06