Network Traffic Security Analysis Report

Overall Threat Assessment

Threat Level: 10/10

Table of Contents

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Covert channel activity detected through DNS and ICMP tunneling attempts
12 DNS tunneling events and **8 ICMP tunneling events** identified across multiple internal hosts
Primary communication between internal IPs 172.20.10.9, 172.20.10.1, and 172.20.10.2
No traditional TCP/UDP attack patterns observed in packet statistics
Risk Assessment

Critical: ICMP Tunneling Cluster

8 repeated ICMP payloads with high entropy (6.46-6.62) indicating potential encrypted data exfiltration
Fixed payload length of 134 bytes across all ICMP events suggests structured malicious content

High: DNS Tunneling Patterns

Multiple DNS queries with abnormal characteristics:

26-32 character domain lengths
Elevated entropy values (3.53-4.00)

Bidirectional traffic between 172.20.10.9 and 172.20.10.1

Threat Observations

DNS Tunneling Indicators

Packet #226/227 and #236/237 show mirrored DNS traffic between 172.20.10.9 ↔ 172.20.10.1
Consistent UDP/DNS protocol pairing with null port values
Multiple query length variations (26,28,25,32 characters)

ICMP Tunneling Patterns

Packet #254 from 172.20.10.2 to 172.20.10.9 shows:

High-entropy payload (6.51 Shannon entropy)
Non-standard payload size (134 bytes)

7 additional ICMP events with nearly identical payload length

Internal Network Focus

All suspicious activity between RFC 1918 addresses
No observed external communication attempts

Recommendations

Immediate Actions

Quarantine 172.20.10.9 and 172.20.10.2 for forensic analysis
Block ICMP payloads > 64 bytes at network perimeter
Implement DNS query length restrictions (max 15 characters)

Technical Controls

Deploy entropy-based anomaly detection for DNS and ICMP
Enable DNS logging with mandatory query type filtering
Configure ICMP type/code whitelisting for internal traffic

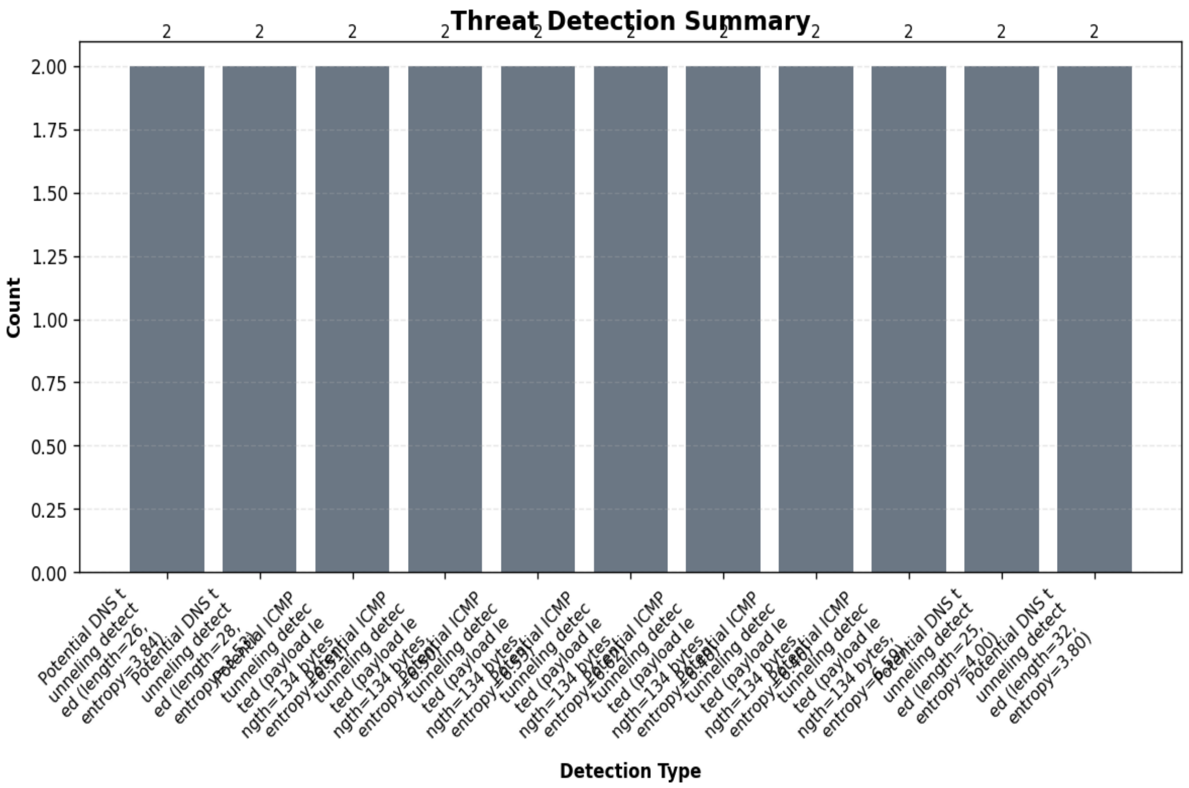
Architectural Improvements

Segment 172.20.10.0/24 network using micro-segmentation
Deploy network traffic analysis (NTA) tools with protocol conformance checking
Implement strict egress filtering for internal-to-internal unusual protocols

Monitoring Enhancements

Create baselines for normal DNS query lengths and ICMP payload sizes
Enable full packet capture for all host-to-host ICMP communications
Deploy certificate pinning for DNS resolvers to prevent unauthorized delegation

Threat Detection Summary



Detection Details

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 (payload length=134 bytes, entropy=6.51)	2
Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.50)	2
Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.53)	2
Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.62)	2
Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.48)	2
Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.46)	2

Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.59)	2
Potential DNS tunneling detected (length=25, entropy=4.00)	2
Potential DNS tunneling detected (length=32, entropy=3.80)	2

Source/Destination Analysis

IP Address	As Source	As Destination	Total
172.20.10.9	2	3	5
172.20.10.1	2	2	4
172.20.10.2	1	0	1

Event Timeline

Time	Packet #	Protocol	Detection
07:14:56.113	226	UDP, DNS	Potential DNS tunneling detect<br/>ed (length=26, entropy=3.84)
07:14:56.137	227	UDP, DNS	Potential DNS tunneling detect<br/>ed (length=26, entropy=3.84)
07:15:57.855	236	UDP, DNS	Potential DNS tunneling detect<br/>ed (length=28, entropy=3.53)
07:15:57.957	237	UDP, DNS	Potential DNS tunneling detect<br/>ed (length=28, entropy=3.53)
07:17:07.470	254	ICMP	Potential ICMP tunneling detec<br/>ted (payload length=134 bytes,<br/> entropy=6.51)

Appendix: Raw Traffic Analysis Data

```
{
  "detection_counts": {
    "Potential DNS tunneling detected (length=26, entropy=3.84)": 2,
    "Potential DNS tunneling detected (length=28, entropy=3.53)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.51)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.50)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.53)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.62)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.48)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.46)": 2,
    "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.59)": 2,
    "Potential DNS tunneling detected (length=25, entropy=4.00)": 2,
    "Potential DNS tunneling detected (length=32, entropy=3.80)": 2
  },
  "attack_stats": {
    "tcp_packets": 0,
    "udp_packets": 0,
    "icmp_packets": 0,
    "arp_packets": 0
  },
  "top_threats": [
    {
      "packet_number": 226,
      "timestamp": "2025-03-14T07:14:56.113791",
      "minute": "2025-03-14 07:14",
      "protocols": [
        "UDP",
        "DNS"
      ],
      "src_ip": "172.20.10.9",
      "dst_ip": "172.20.10.1",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential DNS tunneling detected (length=26, entropy=3.84)"
      ]
    },
    {
      "packet_number": 227,
      "timestamp": "2025-03-14T07:14:56.137435",
      "minute": "2025-03-14 07:14",
      "protocols": [
        "UDP",
        "DNS"
      ],
      "src_ip": "172.20.10.1",
      "dst_ip": "172.20.10.9",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential DNS tunneling detected (length=26, entropy=3.84)"
      ]
    },
    {
      "packet_number": 236,
      "timestamp": "2025-03-14T07:15:57.855561",
      "minute": "2025-03-14 07:15",
      "protocols": [
        "UDP",
        "DNS"
      ],
      "src_ip": "172.20.10.9",
      "dst_ip": "172.20.10.1",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential DNS tunneling detected (length=28, entropy=3.53)"
      ]
    },
    {
      "packet_number": 237,
      "timestamp": "2025-03-14T07:15:57.957007",
      "minute": "2025-03-14 07:15",
      "protocols": [
        "UDP",
        "DNS"
      ],
      "src_ip": "172.20.10.1",
      "dst_ip": "172.20.10.9",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential DNS tunneling detected (length=28, entropy=3.53)"
      ]
    },
    {
      "packet_number": 254,
      "timestamp": "2025-03-14T07:17:07.470886",
      "minute": "2025-03-14 07:17",
      "protocols": [
        "ICMP"
      ],
      "src_ip": "172.20.10.2",
      "dst_ip": "172.20.10.9",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential ICMP tunneling detected (payload length=134 bytes, entropy=6.51)"
      ]
    }
  ]
}
```

This report was automatically generated by DeepSeek AI
Filename: security_report_20250410_181359.pdf
SHA-256 Hash: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Generated on: 2025-04-10 18:15:09