Network Traffic Security Analysis Report

Overall Threat Assessment

Threat Level: 10/10

Table of Contents

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

DNS tunneling attempts dominate detected anomalies (195 instances across 14 variants), indicating potential data exfiltration or C2 activity
TCP connect scans detected at high volume (64 instances) suggesting network reconnaissance
ARP poisoning attacks actively occurring (26 instances) targeting gateway IP 192.168.1.1
Concentrated threat activity observed between 03:00-03:05 involving host 192.168.1.104
Risk Assessment

Critical Risk: DNS tunneling patterns (length 24-42, entropy 3.40-3.90) showing characteristics of **Domain Generation Algorithms (DGAs)**
Critical Risk: **ARP cache poisoning** affecting network gateway (192.168.1.1) enabling MITM attacks
High Risk: TCP SYN scans with abnormal window sizes (>1024) indicating **automated scanning tools**
Low Risk: Single UDP scan detection (packet length ≤8)
Threat ObservationsDNS Tunneling Patterns

Primary variant: length=24, entropy=3.66 (54 detections)
High-entropy outliers: length=30, entropy=3.90 (10) and length=26, entropy=3.87 (8)
Sustained activity from 192.168.1.104 to 192.168.1.1 across multiple sessions
Network Scanning Activity

64 TCP connect scans using non-standard window sizes (SYN flag + window >1024)
1 UDP scan packet matching known reconnaissance patterns
ARP Spoofing

Gateway IP 192.168.1.1 observed with **multiple MAC addresses**
26 poisoning attempts detected, compromising network layer integrity
Top Threat Patterns
Packet #	Timestamp	Source IP	Target IP	Threat Type
104-107	03:00:46	192.168.1.104	192.168.1.1	DNS tunneling (length=21)
331	03:05:10	192.168.1.104	192.168.1.1	DNS tunneling (length=24) |RecommendationsDNS Threat Mitigation

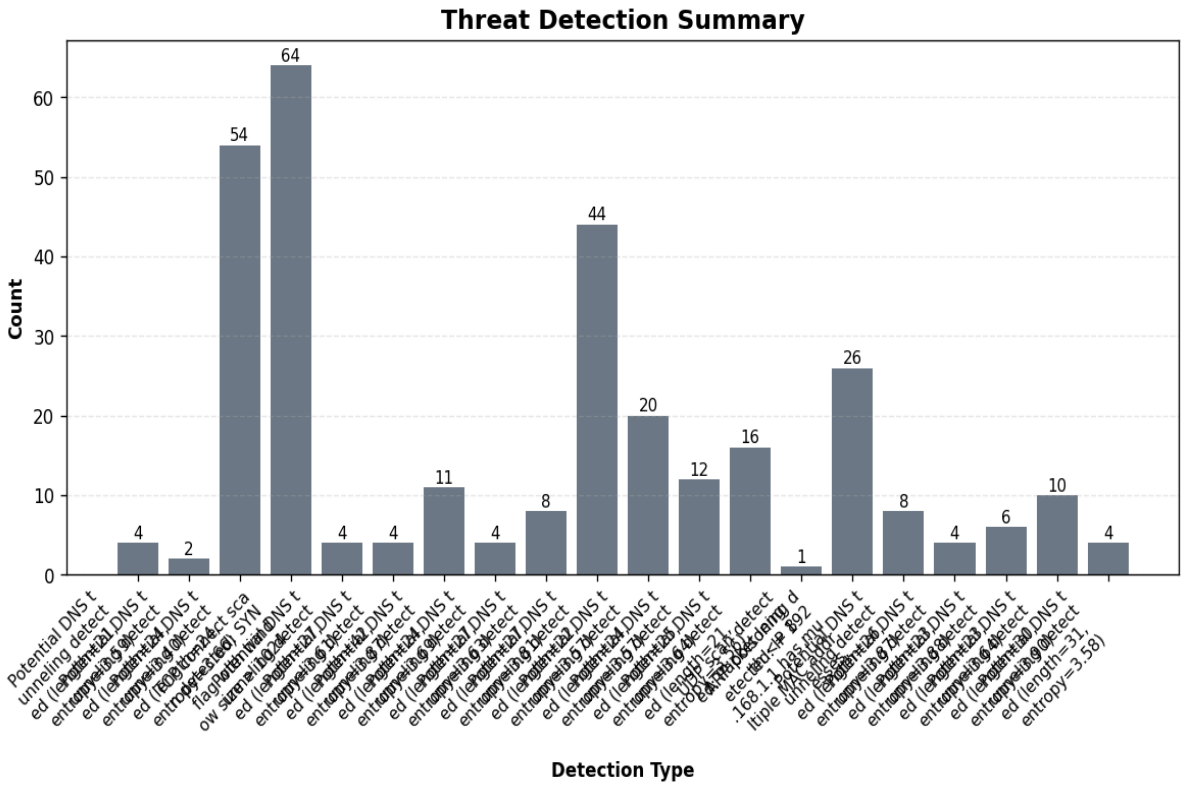
Implement DNS filtering solutions with DGA detection capabilities
Enforce **DNS query length restrictions** (block >32 character domains)
Establish baseline entropy thresholds (alert on >3.5)
Configure rate limiting for DNS queries per host
ARP Protection

Enable DHCP snooping and dynamic ARP inspection on network switches
Implement static ARP entries for critical infrastructure IPs
Deploy network segmentation for sensitive subnets
Scanning Response

Review firewall rules for **SYN packet handling** and window size anomalies
Block source IP 192.168.1.104 pending investigation
Implement port scan detection rules in IDS/IPS systems
General hardening

Update network intrusion detection signatures for DNS tunneling patterns
Conduct packet capture analysis of 192.168.1.104's full traffic history
Schedule security awareness training covering network reconnaissance tactics

Threat Detection Summary



Detection Details

Detection Type	Count
Potential DNS tunneling detected (length=21, entropy=3.59)	4
Potential DNS tunneling detected (length=24, entropy=3.40)	2
Potential DNS tunneling detected (length=24, entropy=3.66)	54
TCP connect scan detected: SYN flag with window size > 1024	64
Potential DNS tunneling detected (length=27, entropy=3.61)	4
Potential DNS tunneling detected (length=42, entropy=3.87)	4
Potential DNS tunneling detected (length=24, entropy=3.69)	11
Potential DNS tunneling detected (length=27, entropy=3.63)	4

Potential DNS tunneling detected (length=27, entropy=3.81)	8
Potential DNS tunneling detected (length=22, entropy=3.57)	44
Potential DNS tunneling detected (length=24, entropy=3.57)	20
Potential DNS tunneling detected (length=25, entropy=3.64)	12
Potential DNS tunneling detected (length=21, entropy=3.56)	16
UDP scan detected: Packet length <= 8	1
ARP poisoning detected: IP 192.168.1.1 has multiple MAC addresses.	26
Potential DNS tunneling detected (length=26, entropy=3.87)	8
Potential DNS tunneling detected (length=23, entropy=3.88)	4
Potential DNS tunneling detected (length=23, entropy=3.64)	6
Potential DNS tunneling detected (length=30, entropy=3.90)	10
Potential DNS tunneling detected (length=31, entropy=3.58)	4

Source/Destination Analysis

IP Address	As Source	As Destination	Total
192.168.1.104	3	2	5
192.168.1.1	2	3	5

Event Timeline

Time	Packet #	Protocol	Detection
03:00:46.589	104	UDP, DNS	Potential DNS tunneling detect ed (length=21, entropy=3.59)
03:00:46.589	105	UDP, DNS	Potential DNS tunneling detect ed (length=21, entropy=3.59)
03:00:46.590	106	UDP, DNS	Potential DNS tunneling detect ed (length=21, entropy=3.59)
03:00:46.590	107	UDP, DNS	Potential DNS tunneling detect ed (length=21, entropy=3.59)
03:05:10.113	331	UDP, DNS	Potential DNS tunneling detect ed (length=24, entropy=3.40)

Appendix: Raw Traffic Analysis Data


```
{
  "detection_counts": {
    "Potential DNS tunneling detected (length=21, entropy=3.59)": 4,
    "Potential DNS tunneling detected (length=24, entropy=3.40)": 2,
    "Potential DNS tunneling detected (length=24, entropy=3.66)": 54,
    "TCP connect scan detected: SYN flag with window size > 1024": 64,
    "Potential DNS tunneling detected (length=27, entropy=3.61)": 4,
    "Potential DNS tunneling detected (length=42, entropy=3.87)": 4,
    "Potential DNS tunneling detected (length=24, entropy=3.69)": 11,
    "Potential DNS tunneling detected (length=27, entropy=3.63)": 4,
    "Potential DNS tunneling detected (length=27, entropy=3.81)": 8,
    "Potential DNS tunneling detected (length=22, entropy=3.57)": 44,
    "Potential DNS tunneling detected (length=24, entropy=3.57)": 20,
    "Potential DNS tunneling detected (length=25, entropy=3.64)": 12,
    "Potential DNS tunneling detected (length=21, entropy=3.56)": 16,
    "UDP scan detected: Packet length <= 8": 1,
    "ARP poisoning detected: IP 192.168.1.1 has multiple MAC addresses.": 26,
    "Potential DNS tunneling detected (length=26, entropy=3.87)": 8,
    "Potential DNS tunneling detected (length=23, entropy=3.88)": 4,
    "Potential DNS tunneling detected (length=23, entropy=3.64)": 6,
    "Potential DNS tunneling detected (length=30, entropy=3.90)": 10,
    "Potential DNS tunneling detected (length=31, entropy=3.58)": 4
  },
  "attack_stats": {
    "tcp_packets": 0,
    "udp_packets": 0,
    "icmp_packets": 0,
    "arp_packets": 0
  },
  "top_threats": [
    {
      "packet_number": 104,
      "timestamp": "1970-01-01T03:00:46.589267",
      "minute": "1970-01-01 03:00",
      "protocols": [
        "UDP",
        "DNS"
      ],
      "src_ip": "192.168.1.104",
      "dst_ip": "192.168.1.1",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential DNS tunneling detected (length=21, entropy=3.59)"
      ]
    },
    {
      "packet_number": 105,
      "timestamp": "1970-01-01T03:00:46.589608",
      "minute": "1970-01-01 03:00",
      "protocols": [
        "UDP",
        "DNS"
      ],
      "src_ip": "192.168.1.104",
      "dst_ip": "192.168.1.1",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential DNS tunneling detected (length=21, entropy=3.59)"
```

```
      ]
    },
    {
      "packet_number": 106,
      "timestamp": "1970-01-01T03:00:46.590367",
      "minute": "1970-01-01 03:00",
      "protocols": [
        "UDP",
        "DNS"
      ],
      "src_ip": "192.168.1.1",
      "dst_ip": "192.168.1.104",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential DNS tunneling detected (length=21, entropy=3.59)"
      ]
    },
    {
      "packet_number": 107,
      "timestamp": "1970-01-01T03:00:46.590578",
      "minute": "1970-01-01 03:00",
      "protocols": [
        "UDP",
        "DNS"
      ],
      "src_ip": "192.168.1.1",
      "dst_ip": "192.168.1.104",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential DNS tunneling detected (length=21, entropy=3.59)"
      ]
    },
    {
      "packet_number": 331,
      "timestamp": "1970-01-01T03:05:10.113583",
      "minute": "1970-01-01 03:05",
      "protocols": [
        "UDP",
        "DNS"
      ],
      "src_ip": "192.168.1.104",
      "dst_ip": "192.168.1.1",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "Potential DNS tunneling detected (length=24, entropy=3.40)"
      ]
    }
  ]
}
```