Network Traffic Security Analysis Report

Overall Threat Assessment

Threat Level: 10/10

Table of Contents

Executive Summary

``markdown
Executive Summary

High-volume reconnaissance activity: 129 TCP connect scans detected from internal IP 192.168.153.154 to multiple external destinations
Persistent DNS anomalies: 28 instances of potential DNS tunneling with suspicious payload characteristics
Network layer compromise: 120 ARP poisoning events involving IP 192.168.153.2
Internal threat pattern: Bidirectional suspicious traffic between 192.168.153.154 (internal) and 192.168.153.2 (local network)
Risk Assessment

Critical Risk: ARP poisoning (120 events) enabling MITM attacks
High Risk: TCP scanning (129 events) indicating network reconnaissance
High Risk: DNS tunneling attempts (28 events) suggesting potential data exfiltration
Elevated Risk: Internal host (192.168.153.154) acting as attack source
Threat Observations
TCP Connect Scans

129 SYN packets with window size >1024 from 192.168.153.154
Targeted external IPs: 204.79.197.203 (Microsoft), 204.79.197.200 (Microsoft), 213.139.38.16 (DE-CIX)
Consistent use of TCP protocol with null port information
DNS Tunneling Indicators

Multiple suspicious DNS queries with high entropy (3.27-4.09):

14 distinct payload length variations (21-37 bytes)
Bidirectional traffic between 192.168.153.154 and 192.168.153.2
Entropy levels exceeding typical DNS payload norms (>3.0)

ARP Poisoning

IP 192.168.153.2 mapped to multiple MAC addresses
120 detection events indicating sustained spoofing attempts
Potential MITM positioning within local subnet
Recommendations

Immediate Containment:

Quarantine 192.168.153.154 and 192.168.153.2 for forensic investigation
Implement ARP inspection with dynamic MAC-IP binding

Network Hardening:

Deploy DNS query monitoring with entropy-based alerting (threshold: 3.0+)
Configure SYN flood protection with rate limiting (max 5 SYN/sec per host)
Implement egress filtering for internal-to-external TCP scans

Threat Hunting:

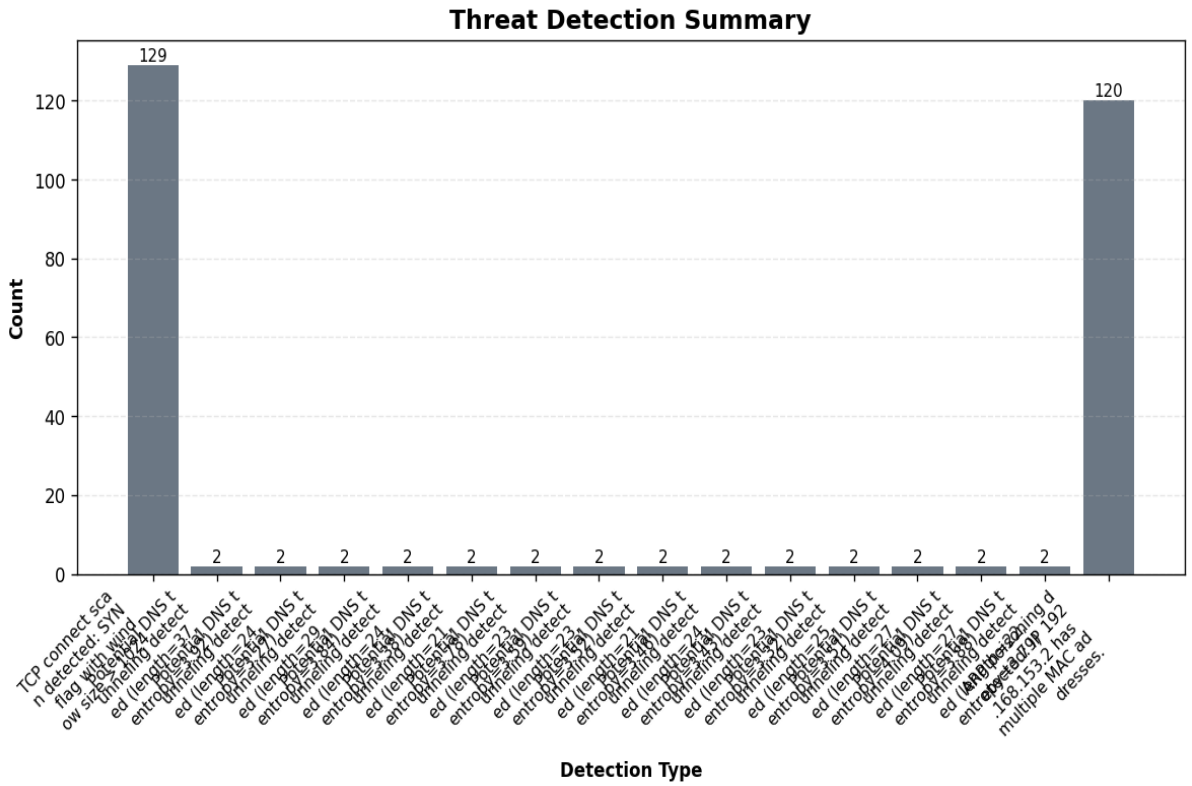
Analyze full packet captures for DNS TXT/AAAA record patterns
Investigate historical traffic from 192.168.153.154 for C2 indicators
Review DHCP logs for MAC address spoofing evidence

Architectural Improvements:

Segment internal network zones to limit lateral movement
Deploy DNSSEC validation for all recursive resolvers
Update IDS/IPS signatures for TCP window size scanning patterns

``

Threat Detection Summary



Detection Details

Detection Type	Count
TCP connect scan detected: SYN flag with window size > 1024	129
Potential DNS tunneling detected (length=37, entropy=3.92)	2
Potential DNS tunneling detected (length=24, entropy=3.27)	2
Potential DNS tunneling detected (length=29, entropy=3.84)	2
Potential DNS tunneling detected (length=24, entropy=3.38)	2
Potential DNS tunneling detected (length=21, entropy=3.78)	2
Potential DNS tunneling detected (length=23, entropy=3.59)	2
Potential DNS tunneling detected (length=23, entropy=3.52)	2

Potential DNS tunneling detected (length=21, entropy=3.46)	2
Potential DNS tunneling detected (length=24, entropy=3.43)	2
Potential DNS tunneling detected (length=23, entropy=3.32)	2
Potential DNS tunneling detected (length=25, entropy=3.51)	2
Potential DNS tunneling detected (length=27, entropy=4.09)	2
Potential DNS tunneling detected (length=27, entropy=3.88)	2
Potential DNS tunneling detected (length=22, entropy=3.79)	2
ARP poisoning detected: IP 192.168.153.2 has multiple MAC addresses.	120

Source/Destination Analysis

IP Address	As Source	As Destination	Total
192.168.153.154	4	1	5
204.79.197.203	0	1	1
204.79.197.200	0	1	1
192.168.153.2	1	1	2
213.139.38.16	0	1	1

Event Timeline

Time	Packet #	Protocol	Detection
05:28:08.813	33	TCP	TCP connect scan detected: SYN flag with window size > 1024
05:28:08.897	40	TCP	TCP connect scan detected: SYN flag with window size > 1024
05:28:09.240	221	UDP, DNS	Potential DNS tunneling detect ed (length=37, entropy=3.92)
05:28:09.335	297	UDP, DNS	Potential DNS tunneling detect ed (length=37, entropy=3.92)
05:28:09.336	298	TCP	TCP connect scan detected: SYN flag with window size > 1024

Appendix: Raw Traffic Analysis Data


```
{
  "detection_counts": {
    "TCP connect scan detected: SYN flag with window size > 1024": 129,
    "Potential DNS tunneling detected (length=37, entropy=3.92)": 2,
    "Potential DNS tunneling detected (length=24, entropy=3.27)": 2,
    "Potential DNS tunneling detected (length=29, entropy=3.84)": 2,
    "Potential DNS tunneling detected (length=24, entropy=3.38)": 2,
    "Potential DNS tunneling detected (length=21, entropy=3.78)": 2,
    "Potential DNS tunneling detected (length=23, entropy=3.59)": 2,
    "Potential DNS tunneling detected (length=23, entropy=3.52)": 2,
    "Potential DNS tunneling detected (length=21, entropy=3.46)": 2,
    "Potential DNS tunneling detected (length=24, entropy=3.43)": 2,
    "Potential DNS tunneling detected (length=23, entropy=3.32)": 2,
    "Potential DNS tunneling detected (length=25, entropy=3.51)": 2,
    "Potential DNS tunneling detected (length=27, entropy=4.09)": 2,
    "Potential DNS tunneling detected (length=27, entropy=3.88)": 2,
    "Potential DNS tunneling detected (length=22, entropy=3.79)": 2,
    "ARP poisoning detected: IP 192.168.153.2 has multiple MAC addresses.": 120
  },
  "attack_stats": {
    "tcp_packets": 0,
    "udp_packets": 0,
    "icmp_packets": 0,
    "arp_packets": 0
  },
  "top_threats": [
    {
      "packet_number": 33,
      "timestamp": "2017-10-18T05:28:08.813858",
      "minute": "2017-10-18 05:28",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.153.154",
      "dst_ip": "204.79.197.203",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 40,
      "timestamp": "2017-10-18T05:28:08.897855",
      "minute": "2017-10-18 05:28",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.153.154",
      "dst_ip": "204.79.197.200",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 221,
      "timestamp": "2017-10-18T05:28:09.240873",
      "minute": "2017-10-18 05:28",
```

```
    "protocols": [
      "UDP",
      "DNS"
    ],
    "src_ip": "192.168.153.154",
    "dst_ip": "192.168.153.2",
    "src_port": null,
    "dst_port": null,
    "detection_details": [
      "Potential DNS tunneling detected (length=37, entropy=3.92)"
    ]
  },
  {
    "packet_number": 297,
    "timestamp": "2017-10-18T05:28:09.335845",
    "minute": "2017-10-18 05:28",
    "protocols": [
      "UDP",
      "DNS"
    ],
    "src_ip": "192.168.153.2",
    "dst_ip": "192.168.153.154",
    "src_port": null,
    "dst_port": null,
    "detection_details": [
      "Potential DNS tunneling detected (length=37, entropy=3.92)"
    ]
  },
  {
    "packet_number": 298,
    "timestamp": "2017-10-18T05:28:09.336478",
    "minute": "2017-10-18 05:28",
    "protocols": [
      "TCP"
    ],
    "src_ip": "192.168.153.154",
    "dst_ip": "213.139.38.16",
    "src_port": null,
    "dst_port": null,
    "detection_details": [
      "TCP connect scan detected: SYN flag with window size > 1024"
    ]
  }
 ]
}
```