

Network Traffic Security Analysis Report

Overall Threat Assessment

Threat Level: 6/10

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Multiple port scan techniques detected from source IP 192.168.100.95 targeting 192.168.100.99. **Six distinct scan types** observed within a short timeframe (SYN, TCP connect, XMAS, NULL, FIN, and UDP scans). No malicious payloads or successful exploitation observed, but reconnaissance activity indicates **pre-attack probing**.
Risk Assessment

Critical Risk: Reconnaissance activity (**SYN/XMAS/NULL/FIN scans**) suggests an attacker is mapping network defenses.
High Risk: **TCP connect scan** (window size > 1024) indicates potential follow-up exploitation attempts.
Moderate Risk: **UDP scan** (packet length ≤ 8) could expose vulnerable UDP services.
Threat Observations

Scan Techniques Detected:

SYN scan (packet #199, window size ≤ 1024).
TCP connect scan (packet #201, window size > 1024).
XMAS scan (packet #203, flags: FIN/URG/PSH).
NULL scan (packet #205, no flags set).
FIN scan (packet #207, FIN flag only).
UDP scan (short packets, likely service discovery).

Source IP: 192.168.100.95 (internal host, suggesting **compromised device or insider threat**).
Target IP: 192.168.100.99 (internal host, possibly a critical asset).
Recommendations

Immediate Actions:

Isolate 192.168.100.95 for forensic analysis to rule out compromise.
Review firewall rules to block anomalous TCP/UDP scans (e.g., rate-limiting SYN packets).

Long-Term Mitigations:

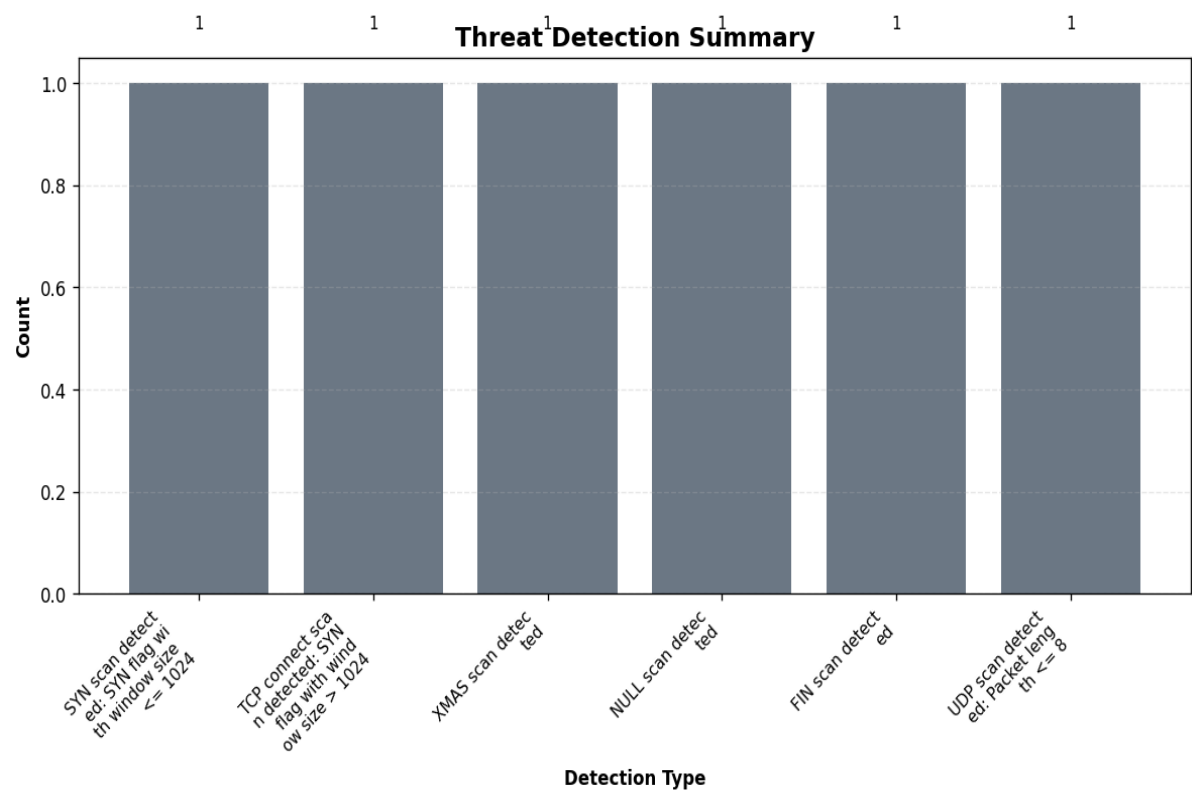
Enable TCP stack hardening (e.g., SYN cookies, drop NULL/XMAS/FIN scans).
Deploy IDS/IPS with signatures for stealth scans (e.g., Snort/Suricata).

Conduct endpoint audits on 192.168.100.95 for malware or unauthorized tools.

Network Segmentation:

Restrict internal host communication to minimize lateral movement risks.

Threat Detection Summary



Detection Details

Detection Type	Count
SYN scan detected: SYN flag with window size <= 1024	1
TCP connect scan detected: SYN flag with window size > 1024	1
XMAS scan detected	1
NULL scan detected	1
FIN scan detected	1
UDP scan detected: Packet length <= 8	1

Source/Destination Analysis

IP Address	As Source	As Destination	Total
192.168.100.95	5	0	5
192.168.100.99	0	5	5

Event Timeline

Time	Packet #	Protocol	Detection
12:47:31.388	199	TCP	SYN scan detected: SYN flag with window size <= 1024
12:47:31.437	201	TCP	TCP connect scan detected: SYN flag with window size > 1024
12:47:31.489	203	TCP	XMAS scan detected
12:47:31.541	205	TCP	NULL scan detected
12:47:31.588	207	TCP	FIN scan detected

Appendix: Raw Traffic Analysis Data

```
{
  "detection_counts": {
    "SYN scan detected: SYN flag with window size <= 1024": 1,
    "TCP connect scan detected: SYN flag with window size > 1024": 1,
    "XMAS scan detected": 1,
    "NULL scan detected": 1,
    "FIN scan detected": 1,
    "UDP scan detected: Packet length <= 8": 1
  },
  "attack_stats": {
    "tcp_packets": 0,
    "udp_packets": 0,
    "icmp_packets": 0,
    "arp_packets": 0
  },
  "top_threats": [
    {
      "packet_number": 199,
      "timestamp": "2025-03-20T12:47:31.388726",
      "minute": "2025-03-20 12:47",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.100.95",
      "dst_ip": "192.168.100.99",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "SYN scan detected: SYN flag with window size <= 1024"
      ]
    },
    {
      "packet_number": 201,
      "timestamp": "2025-03-20T12:47:31.437189",
      "minute": "2025-03-20 12:47",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.100.95",
      "dst_ip": "192.168.100.99",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 203,
      "timestamp": "2025-03-20T12:47:31.489040",
      "minute": "2025-03-20 12:47",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.100.95",
      "dst_ip": "192.168.100.99",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "XMAS scan detected"
      ]
    }
  ]
}
```

```
},
{
  "packet_number": 205,
  "timestamp": "2025-03-20T12:47:31.541120",
  "minute": "2025-03-20 12:47",
  "protocols": [
    "TCP"
  ],
  "src_ip": "192.168.100.95",
  "dst_ip": "192.168.100.99",
  "src_port": null,
  "dst_port": null,
  "detection_details": [
    "NULL scan detected"
  ]
},
{
  "packet_number": 207,
  "timestamp": "2025-03-20T12:47:31.588889",
  "minute": "2025-03-20 12:47",
  "protocols": [
    "TCP"
  ],
  "src_ip": "192.168.100.95",
  "dst_ip": "192.168.100.99",
  "src_port": null,
  "dst_port": null,
  "detection_details": [
    "FIN scan detected"
  ]
}
]
```

This report was automatically generated by DeepSeek AI

Filename: security_report_20250422_223224.pdf

SHA-256 Hash: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

Generated on: 2025-04-22 22:32:54