

Network Traffic Security Analysis Report

Overall Threat Assessment



Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Multiple port scanning techniques detected from source IP 192.168.100.95 targeting 192.168.100.99. **Critical reconnaissance activity** observed, including SYN, XMAS, NULL, FIN, and UDP scans. No actual attack packets (TCP/UDP/ICMP/ARP) were observed post-scanning. Risk Assessment

High Risk:

- SYN Scan (Packet #199):** Indicates active reconnaissance to identify open ports.
- XMAS Scan (Packet #203):** Evasion technique to bypass basic firewall rules.
- NULL Scan (Packet #205):** Stealthy method to probe systems without standard TCP flags.

Medium Risk:

- FIN Scan (Packet #207):** Used to detect closed ports without full handshake.
- UDP Scan:** Short-length packets suggest service enumeration attempts.

Threat Observations

Source IP 192.168.100.95 performed a full suite of port scans:

- SYN scan (window size ≤ 1024) at 2025-03-20 12:47:31.388726.
- TCP connect scan (window size > 1024) at 2025-03-20 12:47:31.437189.
- XMAS scan (FIN/URG/PSH flags) at 2025-03-20 12:47:31.489040.
- NULL scan (no flags) at 2025-03-20 12:47:31.541120.
- FIN scan (FIN flag only) at 2025-03-20 12:47:31.588889.

No post-scan exploitation traffic detected, suggesting reconnaissance phase. Recommendations

Immediate Actions:

- Block 192.168.100.95 at the firewall** and investigate its legitimacy.
- Enable TCP anomaly detection** to flag abnormal flag combinations (e.g., XMAS/NULL scans).

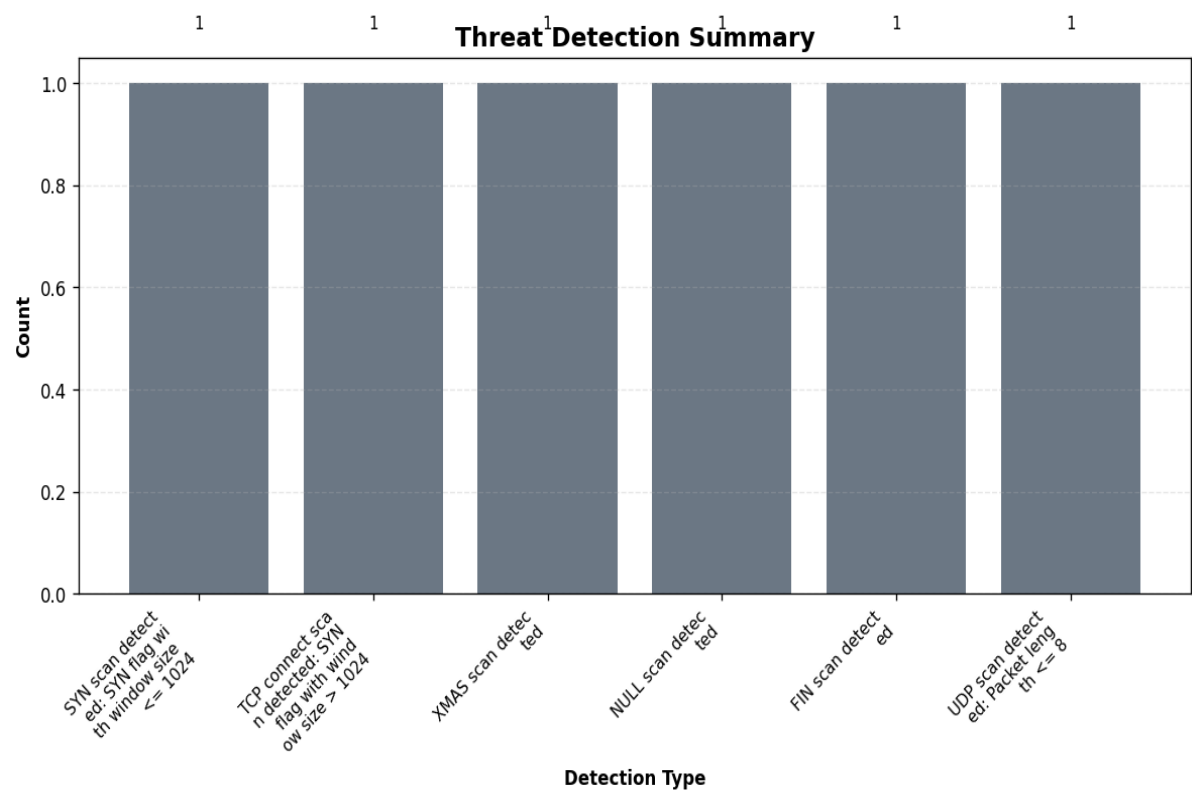
Long-Term Mitigations:

Deploy IDS/IPS rules to detect and drop stealth scans (e.g., Snort/Suricata rules for FIN/XMAS/NULL scans).

Segment internal networks to limit lateral movement if the source is compromised.

Review endpoint logging on 192.168.100.99 for follow-up connection attempts.

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_20250424_215949.pdf

SHA-256 Hash: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

Generated on: 2025-04-24 22:00:20