

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. Scans include **SYN, TCP connect, XMAS, NULL, FIN, and UDP scans**, indicating a reconnaissance effort. No malicious payloads observed (0 TCP/UDP/ICMP/ARP attack packets), but scans may precede exploitation. Risk Assessment

Critical Risk: Active reconnaissance (192.168.100.95 performing stealth scans to map vulnerabilities).
High Risk:

XMAS/NULL/FIN scans evade basic firewall rules by abusing TCP protocol quirks.
UDP scan (length ≤ 8 bytes) suggests service enumeration attempts.

Moderate Risk: Lack of port/protocol details in logs limits granular analysis.
Threat Observations

Scan Patterns:

All scans occurred within seconds (12:47:31), suggesting automated tools (e.g., Nmap). TCP scans used varied techniques (SYN window size manipulation, flag combinations).

Source Attribution:

Internal IP (192.168.100.95) implies compromised host or insider threat.

Protocol Abuse:

XMAS/NULL scans exploit RFC non-compliance in systems to identify open ports.
UDP scan targets stateless protocols (e.g., DNS, DHCP) for service discovery.

Recommendations

Immediate Actions:

Quarantine 192.168.100.95 and investigate for malware/unauthorized access.
Update IDS/IPS rules to flag anomalous TCP flag combinations (e.g., FIN without SYN).

Network Hardening:

Block unused ports and restrict internal lateral movement via VLAN segmentation.

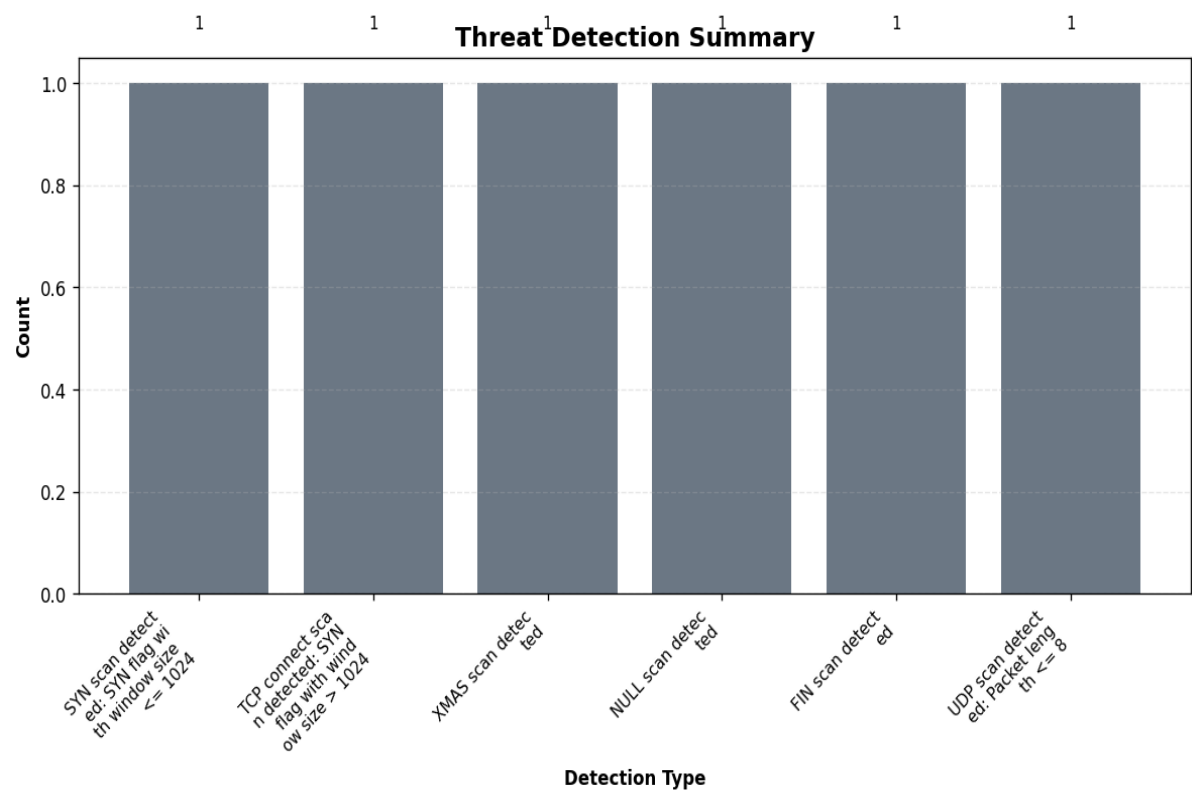
Enable TCP stack hardening (e.g., SYN cookies, drop NULL/XMAS packets at firewall).

Monitoring Enhancements:

Log full packet headers (ports, payload snippets) for future forensic analysis.

Deploy endpoint detection on 192.168.100.95 to identify scanning tools.

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_20250425_104404.pdf

SHA-256 Hash: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

Generated on: 2025-04-25 10:44:31