Network Traffic Security Analysis Report

Overall Threat Assessment

Table of Contents

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Active reconnaissance activity detected with multiple TCP/UDP scan types originating from internal IP 192.168.100.95.
Five distinct stealth scan techniques identified within a 0.2-second window targeting 192.168.100.99.
No direct attack payloads observed (0 TCP/UDP/ICMP/ARP attack packets recorded).
Risk Assessment
Critical Vulnerabilities

Internal host compromise risk: Scans originated from internal IP 192.168.100.95 (**High Severity**)
Network mapping exposure: Combined SYN/XMAS/NULL/FIN/UDP scans enable full port/service enumeration (**Critical Severity**)
Legacy system vulnerability: NULL/XMAS/FIN scans may indicate unprotected systems vulnerable to obsolete scan techniques (**Medium Severity**)
Threat Observations
Scan Pattern Analysis

Multi-technique TCP scan campaign detected at 2025-03-20 07:47:

Packet #199: SYN scan (window size ≤1024)
Packet #201: TCP connect scan (window size >1024)
Packet #203: XMAS scan (FIN/URG/PUSH flags)
Packet #205: NULL scan (no flags set)
Packet #207: FIN scan (FIN flag only)

UDP scan indicator: 1 detection of packets ≤8 bytes (typical for port probing)
Behavioral red flags:

Rapid scan sequence: 5 distinct techniques in 0.2 seconds
Persistent targeting: All scans directed to 192.168.100.99
Source obfuscation: Null port values suggest raw packet crafting

Host Risk Profile

Source IP 192.168.100.95 exhibits characteristics of:

Compromised internal device
Unauthorized security testing
Potential command-and-control activity

Recommendations
Immediate Actions

Quarantine source IP 192.168.100.95 for forensic investigation
Implement egress filtering on border devices to block outgoing scan patterns:

``iptables -A OUTPUT -p tcp --tcp-flags ALL FIN,URG,PSH -j DROP`
`iptables -A OUTPUT -p tcp --tcp-flags ALL NONE -j DROP`

Enable TCP strict mode on network stack for all endpoints:

`sysctl -w net.ipv4.tcp_ignore_invalid_rst=1`Long-Term Mitigations

Deploy network segmentation between 192.168.100.95 and critical assets
Configure IDS/IPS rules to detect:

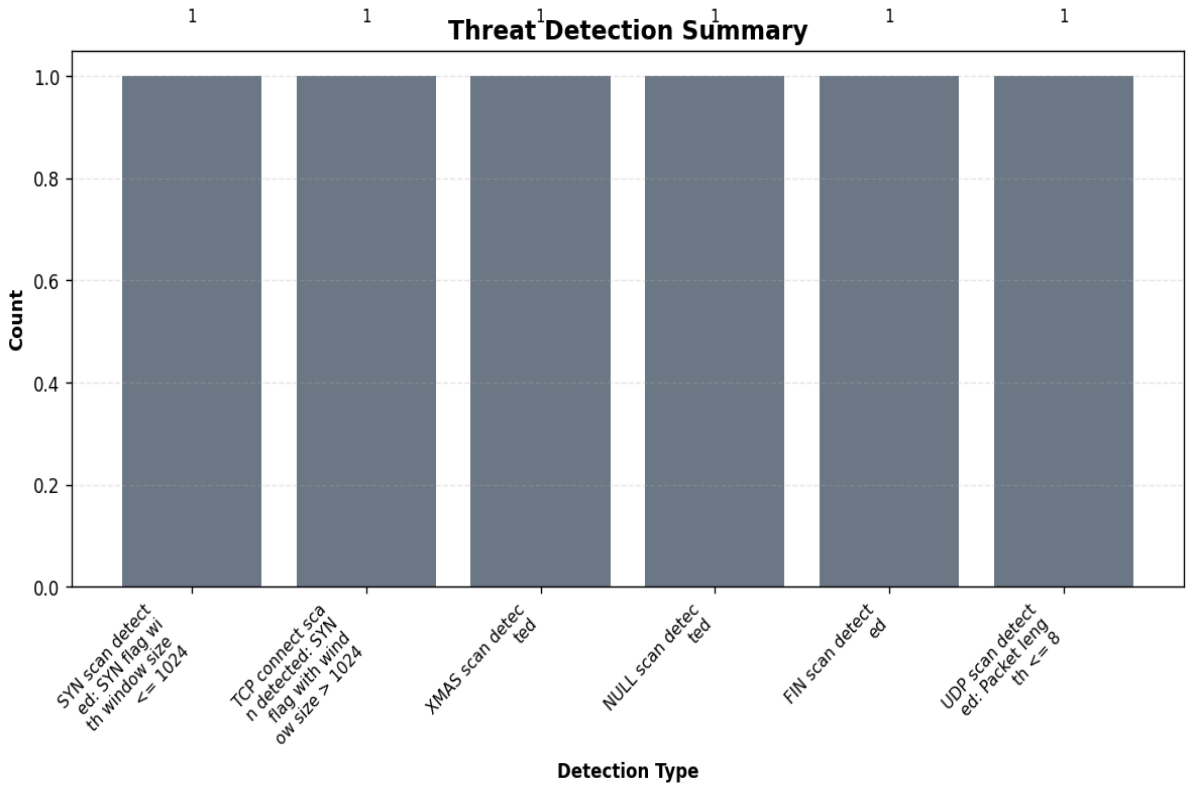
Consecutive scan-type packets from single sources
TCP window size anomalies (≤1024 and >1024 thresholds)

Implement endpoint protection with process monitoring to detect raw socket usage
Protocol Hardening

Enforce RFC-compliant TCP handling to mitigate NULL/XMAS/FIN scan effectiveness
Rate-limit UDP packets ≤8 bytes at network perimeter
Deploy port randomization techniques for responsive services
Enable TCP challenge ACKs to identify scanning tools:

`sysctl -w net.ipv4.tcp_challenge_ack_limit=1000``

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
07:47:31.388	199	TCP	SYN scan detected: SYN flag wi th window size <= 1024
07:47:31.437	201	TCP	TCP connect scan detected: SYN flag with window size > 1024
07:47:31.489	203	TCP	XMAS scan detected
07:47:31.541	205	TCP	NULL scan detected
07:47:31.588	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": "2025-03-20T07:47:31.388726",
      "minute": "2025-03-20 07:47",
      "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": "2025-03-20T07:47:31.437189",
      "minute": "2025-03-20 07:47",
      "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": "2025-03-20T07:47:31.489040",
      "minute": "2025-03-20 07:47",
      "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": "2025-03-20T07:47:31.541120",
      "minute": "2025-03-20 07:47",
      "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": "2025-03-20T07:47:31.588889",
      "minute": "2025-03-20 07:47",
      "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_20250408_143124.pdf

SHA-256 Hash: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Generated on: 2025-04-08 14:32:48