Network Traffic Security Analysis Report

Overall Threat Assessment

Threat Level: 6/10

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Multiple port scanning activities detected from source IP 192.168.100.95 targeting 192.168.100.99.

High-risk reconnaissance activity observed, including SYN, XMAS, NULL, FIN, and TCP connect scans.

No malicious payloads (TCP/UDP/ICMP/ARP) detected, but scanning indicates **potential pre-attack reconnaissance**.

Risk Assessment

Critical Risk:

Port scanning (SYN, XMAS, NULL, FIN, TCP connect, UDP): Indicates active network probing, likely for vulnerability assessment before exploitation.

Repeat offender (192.168.100.95): Consistent scanning behavior suggests deliberate targeting.

Moderate Risk:

Lack of payloads reduces immediate impact, but scans may precede **lateral movement or exploitation**.

Threat Observations

Scanning Techniques Detected:

SYN scan (window size ≤ 1024): Packet #199, likely stealthy port discovery.

TCP connect scan (window size > 1024): Packet #201, mimics legitimate connections.

XMAS scan (packet #203): Sends FIN/URG/PSH flags to evade detection.

NULL scan (packet #205): No flags set, targeting RFC-noncompliant systems.

FIN scan (packet #207): Tests for open ports via FIN flag responses.

UDP scan (short packets): Often used for DNS/DHCP service discovery.

Source IP (192.168.100.95):

Scans occurred within seconds (12:47:31), suggesting automated tools (e.g., Nmap).

Targeted internal IP (192.168.100.99) implies insider threat or compromised host.

Recommendations

Immediate Actions:

Quarantine 192.168.100.95: Investigate for compromise or unauthorized access.
Block scanning IP at firewall: Implement ACLs to deny traffic from this host.

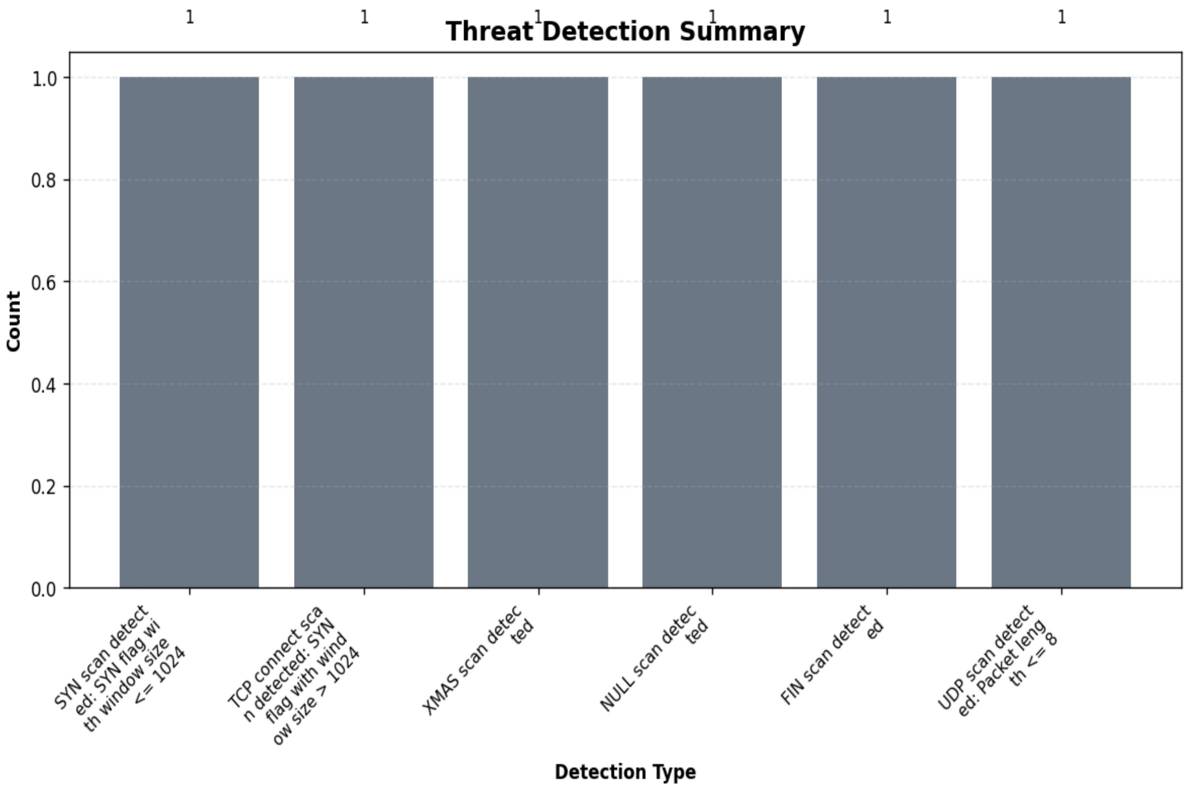
Long-Term Mitigations:

Enable IDS/IPS rules for scan signatures (e.g., SYN flood, anomalous flag combinations).
Segment internal networks to limit lateral movement post-reconnaissance.
Conduct endpoint forensics on 192.168.100.95 for malware/rootkits.

Detection Enhancements:

Deploy anomaly-based monitoring for unusual TCP flag patterns.
Log and alert on UDP scans (short packets, high port ranges).

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 wi<br/>th window size <= 1024
12:47:31.437	201	TCP	TCP connect scan detected: SYN<br/> 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_104143.pdf
SHA-256 Hash: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Generated on: 2025-04-25 10:42:18