

Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Multiple port scan techniques detected from internal IP 192.168.100.95 targeting 192.168.100.99 within a 1-minute window.

Scans include **SYN, TCP Connect, XMAS, NULL, FIN, and UDP** methods, indicating a systematic reconnaissance effort.

Zero detected attack packets (TCP/UDP/ICMP/ARP), suggesting the activity focused on network mapping rather than payload delivery.

Risk Assessment

Critical Risks:

Internal host (192.168.100.95) performing stealth scans, indicating potential lateral movement or compromised device.

High-severity XMAS/NULL/FIN scans (stealth techniques bypassing basic firewall rules).

UDP scan with minimal packet length, often used to identify vulnerable services (e.g., DNS, DHCP).

Elevated Risks:

Repeated SYN scan variants (window size anomalies) suggesting attacker experimentation.

Concentrated targeting of 192.168.100.99, potentially marking it as a high-value asset.

Threat Observations

Scan Patterns:

5 distinct TCP scan types detected in rapid succession (packets #199–207) at 2025-03-20 07:47.

SYN scan with **abnormally low window size (≤ 1024)** and high window size (> 1024) variants.

Stealth scans (XMAS/NULL/FIN) leveraging non-standard TCP flag combinations.

Source Behavior:

Consistent use of **null source/destination ports** in TCP scans, atypical for legitimate traffic.

No observed payloads, suggesting a pure reconnaissance phase.

Protocol Distribution:

100% of top threats involved TCP (5/5 events).

Single UDP scan detected with packet length ≤ 8 bytes (commonly used for service discovery).

Recommendations

Immediate Actions:

Quarantine 192.168.100.95 for forensic analysis to check for compromise.

Validate firewall rules blocking **TCP flags combinations** (e.g., FIN without SYN, XMAS flags).

Network Hardening:

Implement **rate limiting** on SYN packets per source IP to disrupt scan attempts.

Deploy IDS signatures targeting **window size anomalies** (e.g., window: ≤ 1024 AND tcp.flags.syn==1).

Asset Protection:

Restrict lateral communication to 192.168.100.99 using micro-segmentation.

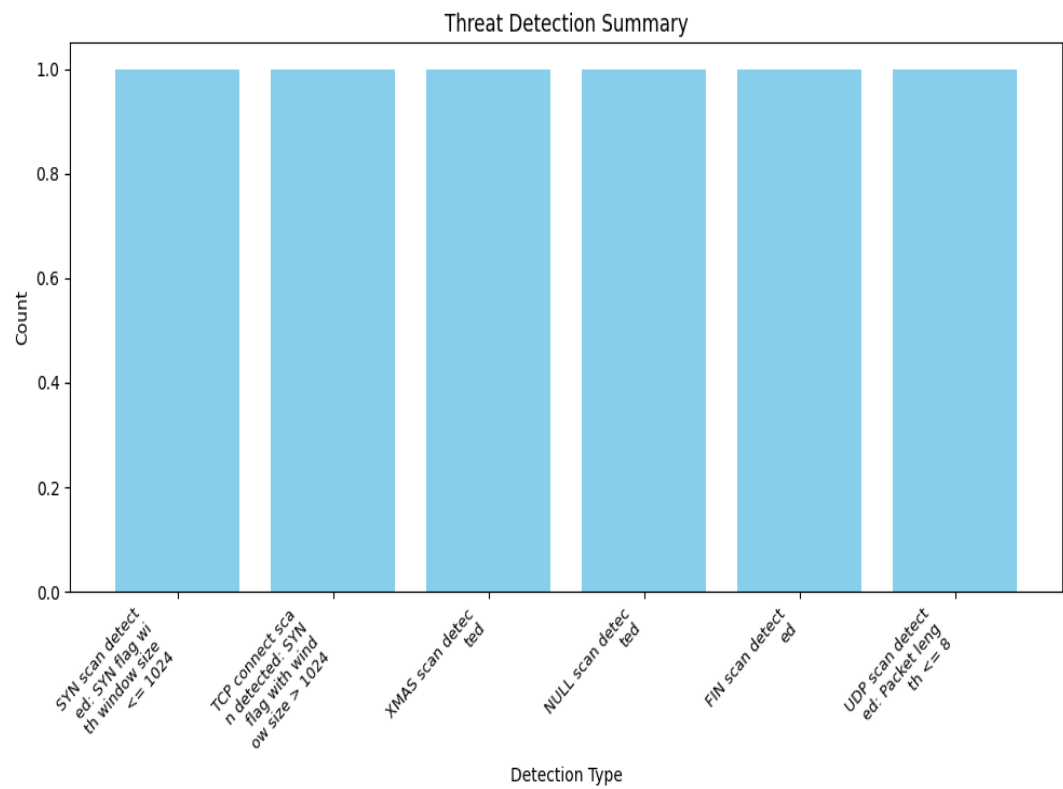
Enable logging for UDP packets ≤ 8 bytes on critical servers.

Monitoring Enhancements:

Correlate scan events with authentication logs for 192.168.100.95.

Deploy deception technologies (e.g., honeypots) to detect follow-up exploitation attempts.

Threat Detection Summary



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

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_20250407_190649.pdf

SHA-256 Hash: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

Generated on: 2025-04-07 19:07:56