Network Traffic Security Analysis Report

Executive Summary

``markdown
Network Traffic Analysis Security Report
Date: March 20, 2025
Analyst: Senior Cybersecurity Analyst 1. Executive Summary
A comprehensive analysis of network traffic revealed **multiple port scanning activities** originating from 192.168.100.95 targeting 192.168.100.99. The scans include:
SYN scan (window size ≤ 1024 and > 1024)
XMAS, NULL, FIN, and UDP scans

These activities indicate **reconnaissance efforts** likely probing for vulnerable services or firewall misconfigurations. While no direct exploitation was observed, the scans pose a **medium risk** as they may precede deeper attacks. 2. Risk Assessment

Threat Type	Severity (CVSS)	Impact
SYN Scan	Medium (5.3)	Potential DoS or service discovery
XMAS/NULL/FIN Scans	Medium (4.3)	Firewall evasion attempts
UDP Scan	Low (3.1)	Service enumeration on UDP ports	**Key Risk Factors:**

Repeated scans from the same source (192.168.100.95) suggest **targeted probing**.
Lack of follow-up exploitation (per packet stats) implies reconnaissance phase.

3. Threat Observations
Technical Findings
Scan Patterns:
TCP Scans (Packets 199–207):
SYN scans with varying window sizes (≤1024 and >1024).
Stealth scans (XMAS, NULL, FIN) to bypass basic firewall rules.
UDP Scan: Short packets (≤8 bytes) to elicit ICMP responses.
Source/Destination:
Attacker IP: 192.168.100.95 (internal host).
Target IP: 192.168.100.99.

Behavioral Insights
Scans occurred within **seconds** (07:47:31), suggesting automated tools (e.g., Nmap).
No ARP/ICMP anomalies detected, indicating a **focused TCP/UDP probe.**

4. Recommendations
Immediate Actions
1. **Isolate Attacker Host:**
Quarantine 192.168.100.95 for forensic analysis (check for malware/compromise).
2. **Harden Target (192.168.100.99):**
Restrict inbound TCP/UDP ports to essentials via firewall rules.
Enable **SYN cookies** to mitigate SYN floods.

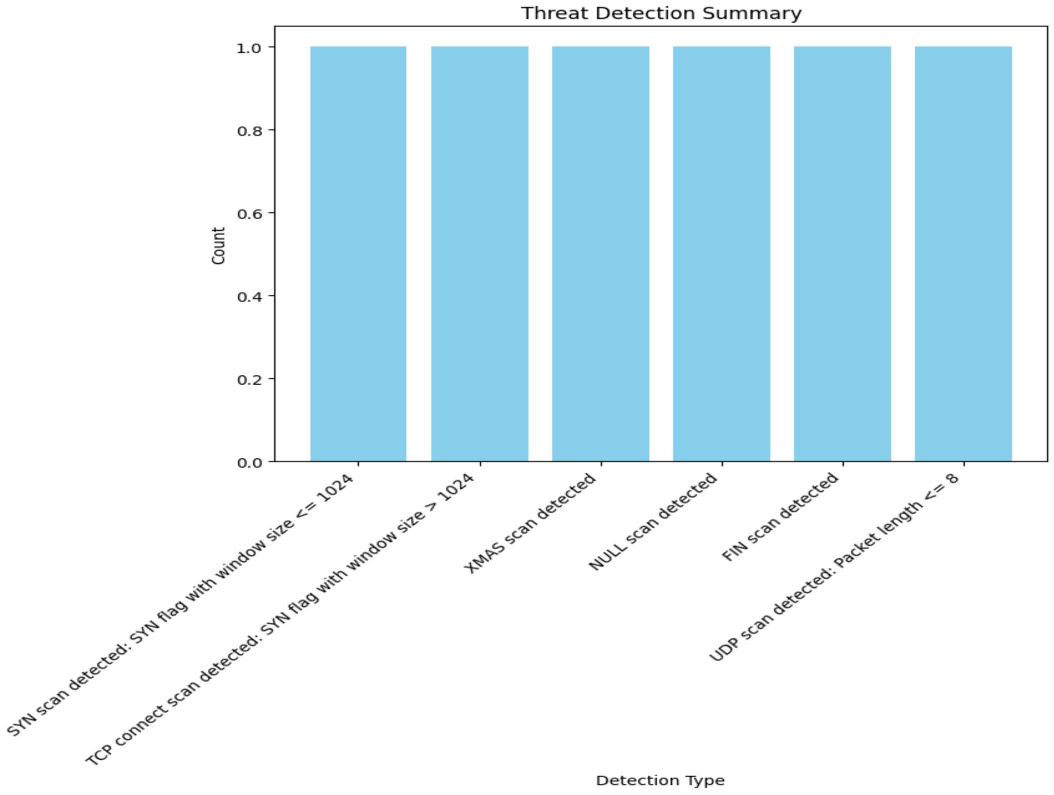
Long-Term Mitigations
Network Segmentation:
Implement VLANs to limit lateral movement.

IDS/IPS Tuning:
Update rules to flag stealth scans (XMAS/NULL/FIN) as high priority.
Logging Enhancements:
Enable detailed logging for all scan-related packets (source/destination ports).

Tooling Suggestions
Deploy **Zeek** or **Suricata** for real-time scan detection.
Conduct **vulnerability assessment** on 192.168.100.99 to address potential exposure.

Conclusion: Proactive containment and network hardening are advised to prevent escalation.
``

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

This report was automatically generated by DeepSeek AI
Report filename: security_report_20250325_231141.pdf
Generated on: 2025-03-25 23:12:10