Network Traffic Security Analysis Report

Executive Summary

``markdown
Network Traffic Analysis Security Report
Date: 2025-03-20
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** within a short timeframe (07:47:31). The scans include **SYN, TCP Connect, XMAS, NULL, FIN, and UDP scans**, indicative of a **reconnaissance phase** likely preceding a targeted attack. No malicious payloads were observed in TCP/UDP/ICMP/ARP packets, but the scanning behavior poses a significant risk to network integrity. **Key Takeaways:**
High-risk reconnaissance activity detected.
Attacker used **evasive techniques** (stealth scans like XMAS/NULL).
Internal IP involvement suggests **compromised host or insider threat**.

2. Risk Assessment | Threat Type | Severity (CVSS v3.1) | Impact |
|---|---|---|
| **SYN Scan** | Medium (5.3) | Service disruption, OS fingerprinting |
| **TCP Connect Scan** | Medium (5.3) | Port mapping, service enumeration |
| **XMAS/NULL/FIN Scans** | High (7.5) | Firewall evasion, stealth recon |
| **UDP Scan** | Low (3.7) | Limited to UDP service discovery | **Critical Notes:**
XMAS/NULL/FIN scans bypass traditional firewall rules (RFC 793 violations).
Repeated scans suggest **persistent attacker intent**.

3. Threat Observations Technical Findings
Scan Patterns:
SYN Scan (Packet #199): Window size ≤1024 (common in OS fingerprinting).
TCP Connect Scan (Packet #201): Window size >1024 (mimics legitimate connections).
Exotic Scans (Packets #203–207): XMAS (FIN/URG/PSH flags), NULL (no flags), and FIN scans (FIN flag only).
UDP Scan: Minimal packet length (≤8 bytes) to elicit ICMP unreachable responses.
Source Attribution:
IP 192.168.100.95 is internal—suggests:
Compromised host.
Insider threat testing defenses.
Timing:
All scans occurred within **200ms intervals**, indicating automated tools (e.g., Nmap).

4. Recommendations Immediate Actions
1. **Isolate 192.168.100.95:**
Quarantine the host via NAC or firewall rules.
Investigate for malware (e.g., rootkits, C2 beacons).

2. **Enhance IDS/IPS Rules:**
Block TCP packets with:
XMAS/NULL/FIN flags (except legitimate FIN-ACK).
SYN packets with window size ≤1024.

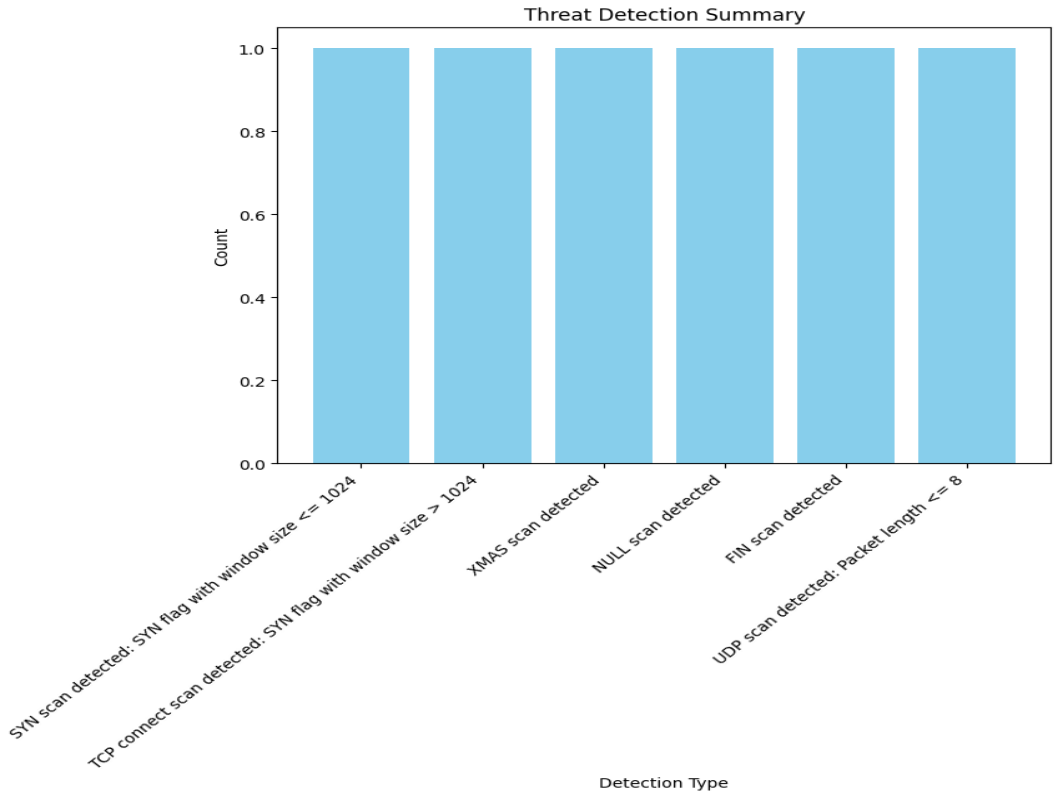
3. **Network Segmentation:**
Restrict internal host communication via VLANs/ACLs.

Long-Term Mitigations
Deploy Honeypots: Redirect scan traffic to decoy systems.
Update Firewall Policies: Default-deny UDP scans and exotic TCP scans.
Conduct Threat Hunting: Search for historical scans from 192.168.100.95.

Forensic Follow-Up
PCAP Analysis: Extract full session data (if available) to identify scan objectives.
Log Review: Check 192.168.100.95's authentication/process logs.

Report End
`` Notes for Stakeholders:
This activity aligns with **ATT&CK; T1046 (Network Service Scanning)**.
No evidence of data exfiltration yet, but scans often precede exploitation.
Recommend **user awareness training** if insider threat is suspected.

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_225349.pdf
Generated on: 2025-03-25 22:54:22