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. The scans included:
TCP-based stealth scans (SYN, XMAS, NULL, FIN)
UDP scan attempts (short-length packets)

No actual malicious payloads (TCP/UDP/ICMP/ARP) were observed, but the reconnaissance activity indicates **probing for vulnerabilities** and potential future exploitation. 2. Risk Assessment

Threat Type	Severity (CVSS)	Description
SYN Scan	Medium (5.3)	Probing for open TCP ports with low window size (<= 1024).
TCP Connect Scan	Medium (5.3)	Standard port scan with SYN flags (window size > 1024).
XMAS/NULL/FIN Scans	High (7.5)	Stealthy scans bypassing basic firewall rules (RFC-violating packets).
UDP Scan	Low (3.7)	Probing for open UDP services (short packets may evade detection).

Critical Notes:
The attacker (192.168.100.95) tested multiple scanning techniques, suggesting **deliberate reconnaissance**.
Repeated TCP scans (SYN, XMAS, NULL, FIN) indicate **targeted probing** of 192.168.100.99.

3. Threat Observations
Key Findings:
1. **Scanning Techniques Detected:**
SYN Scan (Packet #199): Low window size (<= 1024) suggests evasion attempts.
TCP Connect Scan (Packet #201): Standard SYN scan with larger window size.
XMAS Scan (Packet #203): TCP flags FIN/URG/PSH set (stealthy).
NULL Scan (Packet #205): No flags set (evades stateless firewalls).
FIN Scan (Packet #207): Only FIN flag set (bypasses SYN-based detection).

2. **Source-Destination Pattern:**
All scans originated from 192.168.100.95 → 192.168.100.99 (internal IPs).
Implication: Potential insider threat or compromised internal host.

3. **UDP Scan:**
Short packets (length <= 8) suggest UDP service discovery (e.g., DNS, DHCP).

4. Recommendations
Immediate Actions:
1. **Isolate the Attacker:**
Block 192.168.100.95 at the network firewall.
Investigate the host for signs of compromise (malware, unauthorized access).

2. **Harden Target Host (192.168.100.99):**

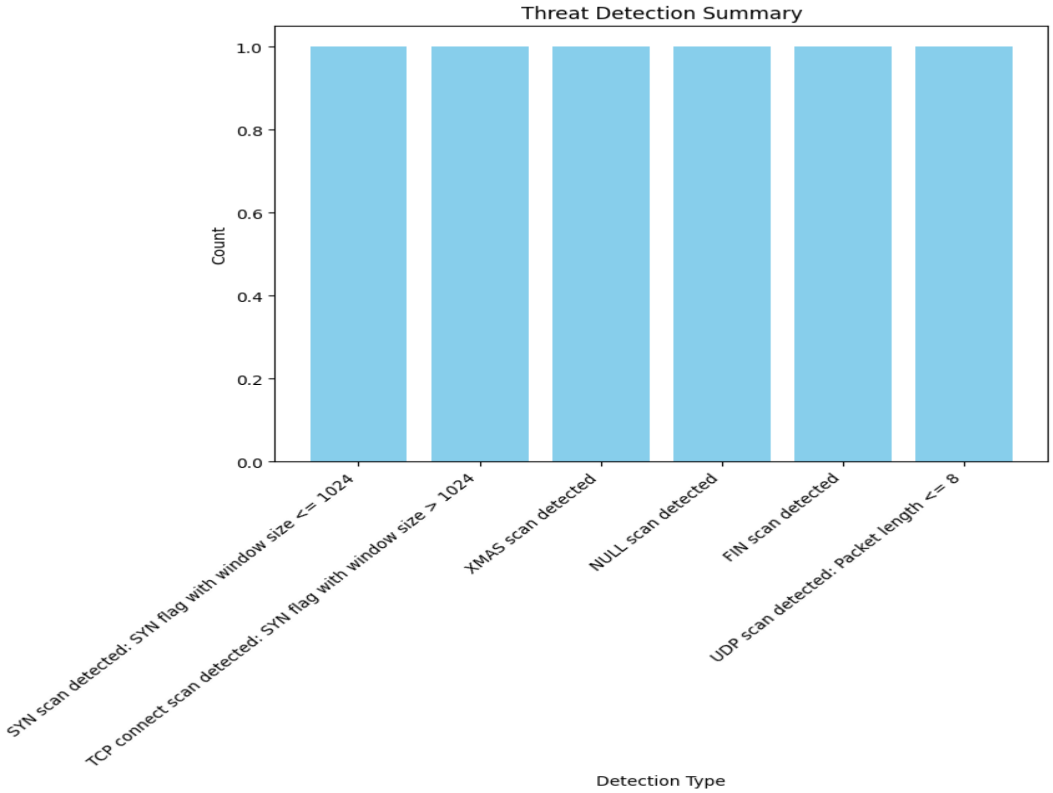
Review open ports/services and disable unnecessary ones.
Implement **rate limiting** to throttle scan attempts.

3. **Update Detection Rules:**
Add IDS/IPS signatures for XMAS/NULL/FIN scans (e.g., Snort/Suricata rules).
Enable logging for UDP packets with length <= 8.

Long-Term Mitigations:
Network Segmentation: Restrict internal host-to-host communication via VLANs/firewalls.
Endpoint Protection: Deploy host-based firewalls (e.g., Windows Firewall, iptables) to drop stealth scans.
User Awareness: If the source IP is a user device, conduct a security audit for rogue tools (e.g., Nmap).

Final Note: While no exploitation was observed, the scans indicate **pre-attack reconnaissance**. Proactive containment is advised.
``

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_231351.pdf
Generated on: 2025-03-25 23:14:28