

Network Traffic Security Analysis Report

Executive Summary

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: - TCP-based stealth scans (SYN, XMAS, NULL, FIN) - UDP scan (short-length probes)

No actual malicious payloads (TCP/UDP/ICMP/ARP) were observed, but the activity indicates reconnaissance for potential vulnerabilities. Immediate action is required to mitigate further probing.

## 2. Risk Assessment		
SYN/XMAS/NULL/FIN Scans	Medium (Stealthy TCP scans to identify open ports and OS fingerprinting.	
UDP Scan	Low (Probing for UDP services (e.g., DNS, DHCP) with minimal packet length	

Key Risk: Reconnaissance precedes exploitation. The attacker (`192.168.100.95`) is likely mapping network defenses.

3. Threat Observations ### Scanning Techniques Detected 1. SYN Scan (Packet #199) - Window size ≤ 1024 suggests evasion attempts (e.g., bypassing IDS/IPS). 2. TCP Connect Scan (Packet #201) - Window size > 1024 indicates a less stealthy but faster scan. 3. XMAS/NULL/FIN Scans (Packets #203–207) - Abnormal TCP flag combinations to identify unfiltered ports. 4. UDP Scan - Probing with packets ≤ 8 bytes (typical for service discovery).

Traffic Patterns - Source IP: `192.168.100.95` (internal host, suggesting compromised device or insider threat). - Target IP: `192.168.100.99` (internal server). - Timing: All scans occurred within 200ms, indicating automated tools (e.g., Nmap).

4. Recommendations ### Immediate Actions

- 1. Isolate the Source Host - Quarantine `192.168.100.95` for forensic analysis (check for malware/unauthorized tools).**
- 2. Enforce Network Segmentation - Restrict internal host communication via VLANs/firewall rules (least privilege).**
- 3. Update IDS/IPS Rules - Add signatures for stealth scans (e.g., `alert tcp any any -> any any (flags: S; window: <=1024; msg:"SYN Scan";)`).**

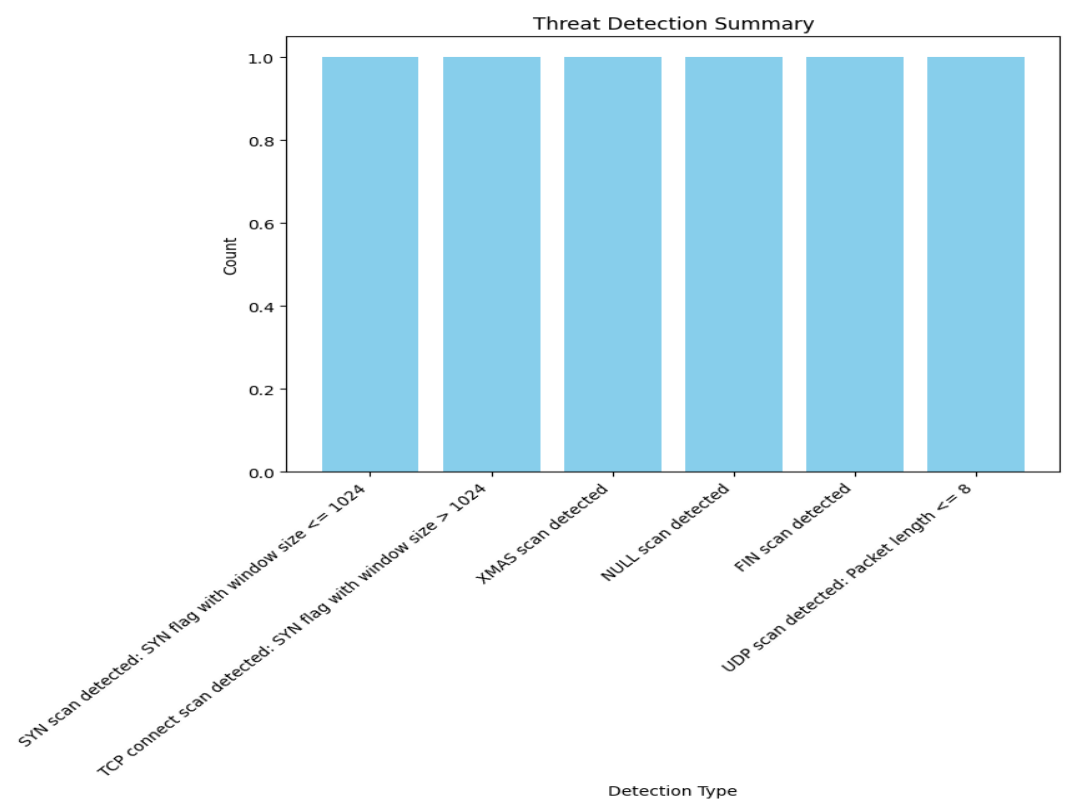
Long-Term Mitigations - Enable TCP Stack Hardening (e.g., SYN cookies, drop NULL/XMAS packets). - Conduct a Penetration Test to identify other vulnerable hosts. - Monitor for Lateral Movement (e.g., SMB/RDP connections from `192.168.100.95`).

Evidence Preservation - Retain full packet captures (PCAPs) of scans for incident response.

Report End

Key Notes for Stakeholders - The absence of attack packets suggests early-stage reconnaissance. - Internal scans imply a potential insider threat or lateral movement. - Recommendations align with NIST SP 800-61 (Incident Handling Guide).

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