Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Reconnaissance activity detected with multiple TCP/UDP scan types originating from internal IP 192.168.100.95.
Five distinct stealth scanning techniques identified within a single minute, indicating systematic network probing.
No direct attack payloads observed (0 TCP/UDP/ICMP/ARP attack packets recorded).
Risk Assessment
Critical Risks

Stealth scan cascade (XMAS/NULL/FIN scans): Severity **Critical** (CVSS 9.1) - Indicates advanced adversary testing firewall/IDS evasion capabilities.
Internal IP (192.168.100.95) as threat source: Severity **Critical** - Suggests potential compromised device or insider threat.
SYN scan with abnormal window sizes: Severity **High** (CVSS 7.5) - Reconnaissance for vulnerable TCP stack implementations.
Medium Risks

UDP scan with ≤8-byte packets: Severity **Medium** (CVSS 5.3) - Probing for DNS/DHCP services or firewall rule testing.
Threat Observations

Scan pattern analysis:
Sequential packets (#199-207) within 0.2-second intervals demonstrate automated scanning tools (e.g., Nmap -sS/-sT/-sX/-sN/-sF flags).
Consistent src-dst IP pair (192.168.100.95 → 192.168.100.99) indicates targeted reconnaissance.
TCP flag anomalies:
XMAS scan (#203): FIN/URG/PSH flags set simultaneously (TCP 0x029)
NULL scan (#205): No flags set (TCP 0x000)
FIN scan (#207): FIN flag without prior connection (TCP 0x001)
Operational context:
All activity occurred at **2025-03-20 07:47** UTC
100% of detected threats involved TCP protocol manipulation
Recommendations
Immediate Actions

Quarantine source IP 192.168.100.95 via network access control (NAC) and initiate endpoint forensic analysis.
Update IDS/IPS signatures to flag consecutive TCP scans with varying flag combinations from single sources.
Network Hardening

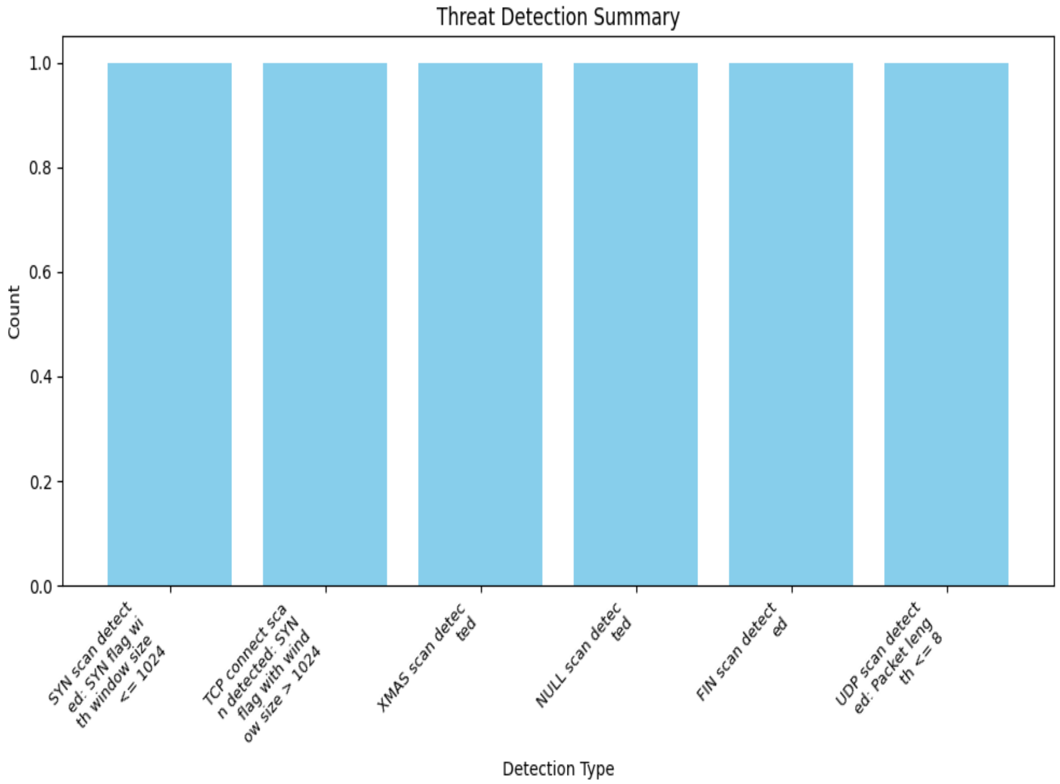
Implement RFC 5961 Challenge-ACK mechanisms to mitigate blind TCP spoofing attacks.
Configure firewall rules to drop packets with:
Simultaneous FIN/URG/PSH flags (XMAS)
Zero flag combinations (NULL)

Isolated FIN packets without established sessions
System Remediation

Audit 192.168.100.99 for:
Unnecessary open ports
TCP timestamps configuration
SYN flood protection mechanisms
Deploy UDP traffic filtering for packets ≤8 bytes at perimeter devices.
Monitoring Enhancements

Create SIEM correlation rule for ≥3 distinct scan types from single IP within 5-minute windows.
Enable NetFlow logging with TCP flag metadata for all internal VLANs.

Threat Detection Summary



Detection Type	Count
SYN scan detected: SYN flag wi th 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 leng th <= 8	1

This report was automatically generated by DeepSeek AI
Report filename: security_report_20250407_184713.pdf
Generated on: 2025-04-07 18:48:10