Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Multiple stealth network reconnaissance activities detected within a 1-minute window (2025-03-20 07:47).
Single internal source IP (192.168.100.95) targeting destination IP 192.168.100.99 using 5 distinct TCP scan types and 1 UDP scan.
No direct exploit payloads observed (0 TCP/UDP/ICMP/ARP attack packets logged).
Risk Assessment
Critical Vulnerabilities

High-risk reconnaissance patterns: Aggressive port scanning indicates active network mapping, likely pre-attack intelligence gathering.
Stealth scan techniques: XMAS, NULL, and FIN scans evade basic firewall/IDS detection.
Internal threat vector: Attacker IP (192.168.100.95) resides within the 192.168.100.0/24 subnet, suggesting **potential compromised internal asset**.
UDP exposure risk: Short-length UDP packets (<=8 bytes) indicate service enumeration attempts on stateless protocols.
Severity Levels

Critical: TCP Connect Scan (window size >1024) + SYN Scan (window size <=1024)
High: XMAS/NULL/FIN stealth scans
Medium: UDP scan (limited payload analysis)
Threat Observations
Technical Findings

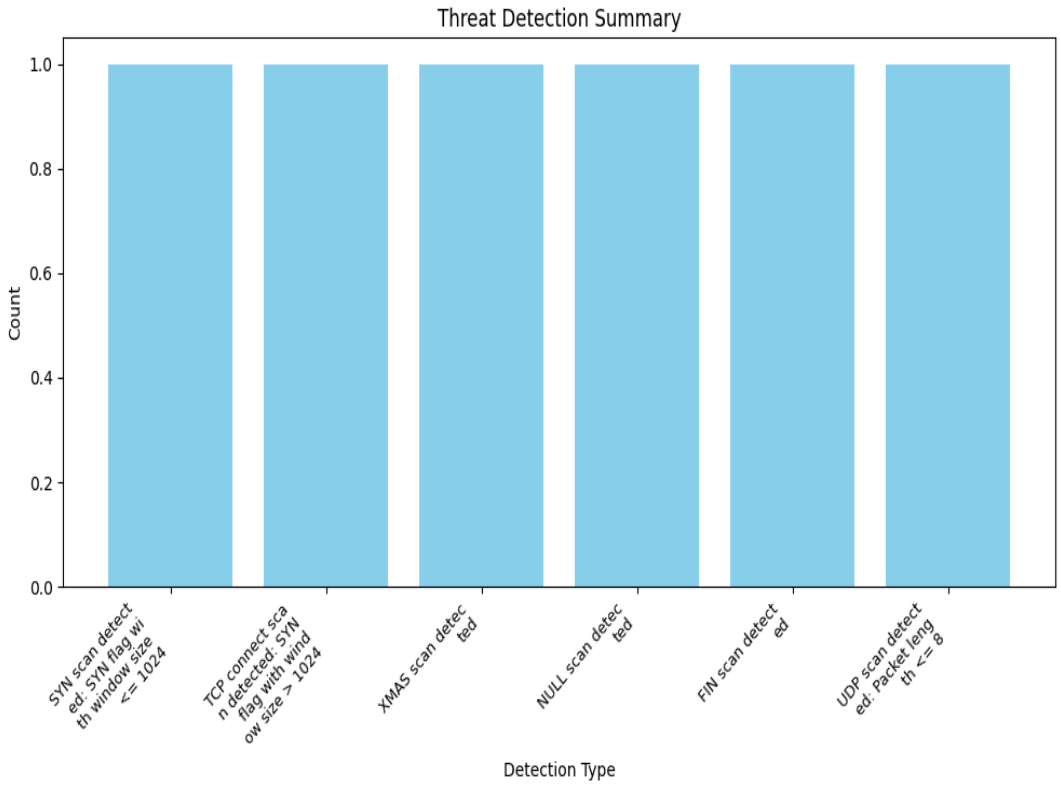
Scan pattern diversity: Attacker cycled through 5 TCP scan methods (SYN, Connect, XMAS, NULL, FIN) in rapid succession (packets 199-207).
Window size manipulation: SYN scans used both <=1024 and >1024 window sizes, suggesting tool customization or multiple scanning tools.
Stealth technique usage:
XMAS scan (PSH+URG+FIN flags)
NULL scan (no flags set)
FIN scan (FIN flag only)
Target focus: All malicious packets targeted 192.168.100.99, indicating specific host interest.
Protocol distribution: 100% of top threats used TCP (5/5 events), with 1 UDP scan logged separately.
Recommendations
Immediate Actions

Quarantine 192.168.100.95: Initiate forensic analysis to determine if device is compromised.
Enhance IDS/IPS rules:
Block TCP packets with conflicting flag combinations (e.g., FIN without prior SYN)
Alert on sequential scan-type variations from single sources
Implement network segmentation: Restrict internal-east-west communication between 192.168.100.95 and 192.168.100.99.
Configuration Hardening

Deploy TCP stack hardening on 192.168.100.99:
Reject NULL/XMAS/FIN scans at OS level (e.g., iptables DROP invalid packets)
Reduce SYN-ACK retry attempts to mitigate SYN flood risks
Enable UDP payload inspection: Block UDP packets <64 bytes except DNS/DHCP.
Monitoring Enhancements

Create baselines for normal internal host communication patterns.
Deploy endpoint detection on 192.168.100.95: Hunt for rootkits, credential dumpers, or pentesting tools.
Audit user accounts with access to 192.168.100.95: Verify legitimacy of recent logins.

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_20250407_185200.pdf
Generated on: 2025-04-07 18:53:03