

Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Coordinated scanning activity detected originating from internal IP 192.168.100.95 targeting 192.168.100.99.

Multiple stealth port-scanning techniques observed, including SYN, XMAS, NULL, FIN, and UDP scans.

Critical reconnaissance phase identified, suggesting potential preparation for lateral movement or exploitation.

Risk Assessment

Critical Severity:

Stealth scan patterns (XMAS, NULL, FIN) indicate an attacker evading basic detection mechanisms.

Internal IP involvement (192.168.100.95) raises concerns about compromised hosts or insider threats.

High Severity:

UDP scan (packet length ≤ 8) targeting stateless protocols could expose vulnerable services.

SYN scan variations (window size anomalies) suggest fingerprinting attempts to identify OS/services.

Threat Observations

Scanning Techniques:

SYN scan (packet #199, window ≤ 1024) and **TCP connect scan** (packet #201, window > 1024) detected within seconds.

Advanced TCP flag abuse: XMAS (packet #203), NULL (packet #205), and FIN (packet #207) scans observed in rapid succession.

Low-footprint UDP scan detected, likely probing for DNS, DHCP, or other UDP-based services.

Behavioral Patterns:

All scans originated from 192.168.100.95 within a 1-second timeframe (07:47:31), indicating automated tool usage (e.g., Nmap).

Absence of follow-up attack packets (0 TCP/UDP/ICMP/ARP attack packets logged) suggests

reconnaissance phase in progress.

Recommendations

Immediate Actions:

Quarantine 192.168.100.95 for forensic analysis to determine if it is compromised or malicious.

Enhance IDS/IPS rules to flag TCP flag anomalies (e.g., FIN without ACK, XMAS combinations).

Network Hardening:

Implement RFC 3704 filtering to block internally originated spoofed traffic.

Restrict UDP services to authorized hosts and deploy UDP flood protection mechanisms.

Monitoring Enhancements:

Deploy endpoint detection on 192.168.100.99 to identify follow-up exploitation attempts.

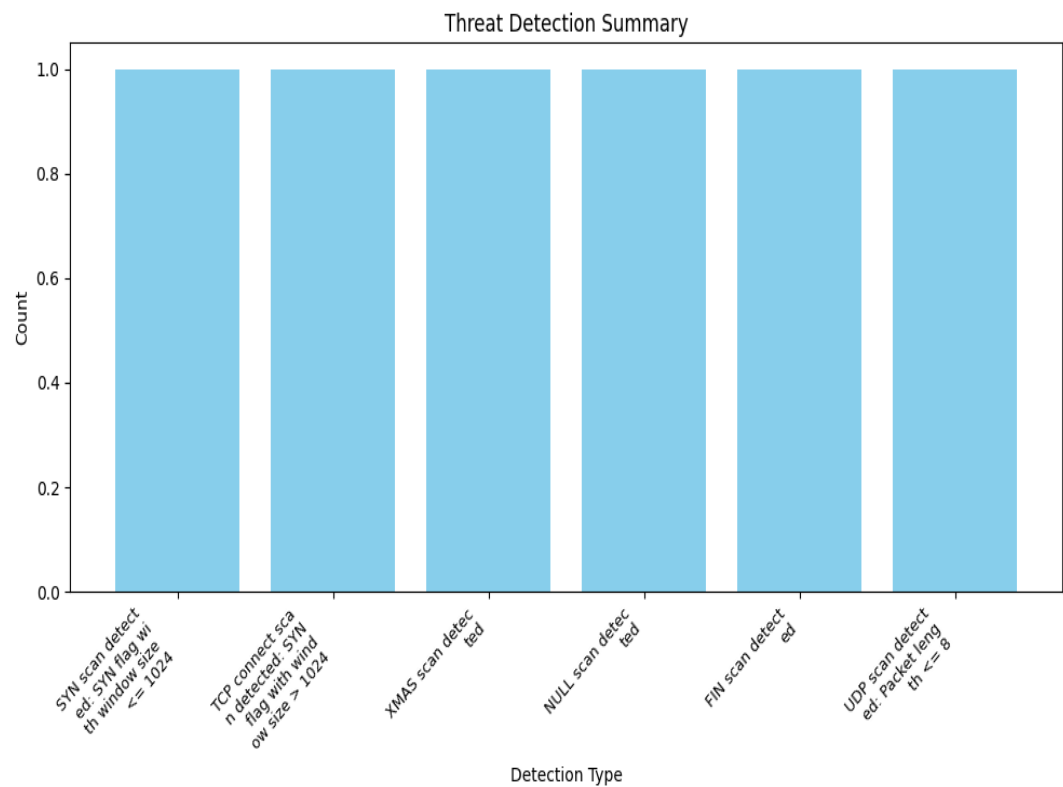
Enable flow analysis for internal traffic to detect low-and-slow scanning patterns.

Policy Updates:

Enforce strict egress filtering to limit internal hosts from initiating irregular TCP flag combinations.

Segment the 192.168.100.0/24 network to reduce lateral movement opportunities.

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