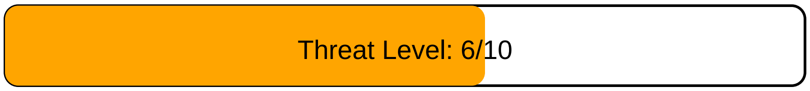
Network Traffic Security Analysis Report

Overall Threat Assessment



Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Multiple **stealth port scanning techniques** detected from source IP 192.168.100.95 targeting 192.168.100.99.

Scans include **SYN, TCP connect, XMAS, NULL, FIN, and UDP scans**—indicating a **reconnaissance phase** of a potential attack.

No malicious payloads observed (0 TCP/UDP/ICMP/ARP attack packets), suggesting the activity was purely exploratory.

Risk Assessment

Critical Risk: Active reconnaissance (192.168.100.95) using **evasive scanning methods** (XMAS/NULL/FIN scans bypass basic firewall rules).

High Risk: UDP scan detected (packet length ≤ 8), which could identify vulnerable UDP services.

Moderate Risk: Repeated TCP-based scans (SYN/TCP connect) suggest attacker persistence.

Threat Observations

Scanning Techniques Detected:

SYN scan (window size ≤ 1024 and > 1024)
TCP connect scan (window size > 1024)
XMAS scan (FIN/URG/PSH flags set)
NULL scan (no flags set)
FIN scan (FIN flag set)
UDP scan (minimal packet length)

Source IP: 192.168.100.95 consistently targeted 192.168.100.99 within seconds (12:47:31).

No payloads: Scans focused on port/service discovery without data exfiltration or exploitation attempts.

Recommendations

Immediate Actions:

Block 192.168.100.95 at the firewall and investigate its origin (compromised host or insider threat?).
Enable **SYN cookie protection** and **rate limiting** to mitigate TCP-based scans.

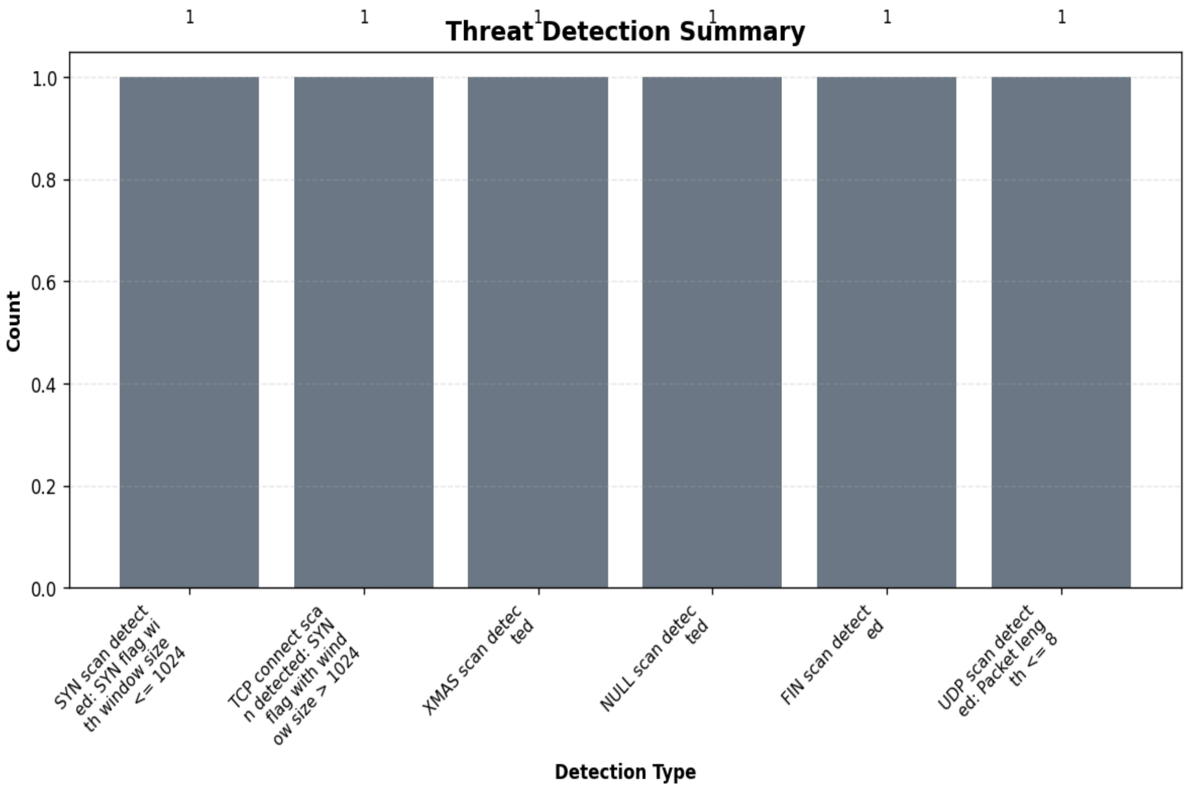
Long-Term Mitigations:

Deploy **intrusion detection rules** for NULL/XMAS/FIN scans (e.g., Snort/Suricata).
Segment the network to restrict internal host-to-host scanning.
Audit 192.168.100.99` for unnecessary open ports/services.

UDP Scan Defense:

Filter UDP packets with length ≤ 8 at the perimeter.
Monitor UDP services (e.g., DNS, DHCP) for anomalous traffic.

Threat Detection Summary



Detection Details

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