Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Stealth reconnaissance activity detected: 6 distinct port scan types identified from internal IP 192.168.100.95 targeting 192.168.100.99.
Attack pattern diversity: Multiple TCP scan techniques (SYN, Connect, XMAS, NULL, FIN) and UDP scan detected within 1 minute (07:47:31).
Internal network threat: All activity originated from and targeted internal RFC 1918 addresses (192.168.0.0/16 range).
Risk Assessment
Critical Vulnerabilities

Host enumeration risk (Severity: Critical): Combined scan techniques indicate active service discovery attempts
Firewall bypass potential (Severity: High): XMAS/NULL/FIN scans exploit RFC non-compliant systems
UDP service exposure (Severity: Medium): 8-byte UDP packets suggest DNS/SNMP service probing
Threat Priority Ranking
1. **TCP Connect Scan** → Direct full connection attempts
2. **Stealth Scans Cluster** → XMAS/NULL/FIN in rapid succession
3. **Low Window SYN** → Potential OS fingerprintingThreat Observations
Scan Pattern Analysis

SYN Scan Signature: Packet #199 used window size ≤1024 (common in Nmap default settings)
Protocol Stack Behavior: 5 consecutive TCP scans followed by UDP probe suggests comprehensive service mapping
Temporal Pattern: All events occurred within 200ms intervals (packets #199-207)
Host Interaction Matrix
Source IP	Destination IP	Scan Types Used	Packet Count
192.168.100.95	192.168.100.99	SYN, Connect, XMAS, NULL, FIN	5 TCP
192.168.100.95	192.168.100.99	UDP (≤8 byte)	1 UDP |Protocol Distribution

TCP: 100% of top threats
UDP: Single detection but high-risk profile
ICMP/ARP: No suspicious activity recorded
Recommendations
Immediate Actions

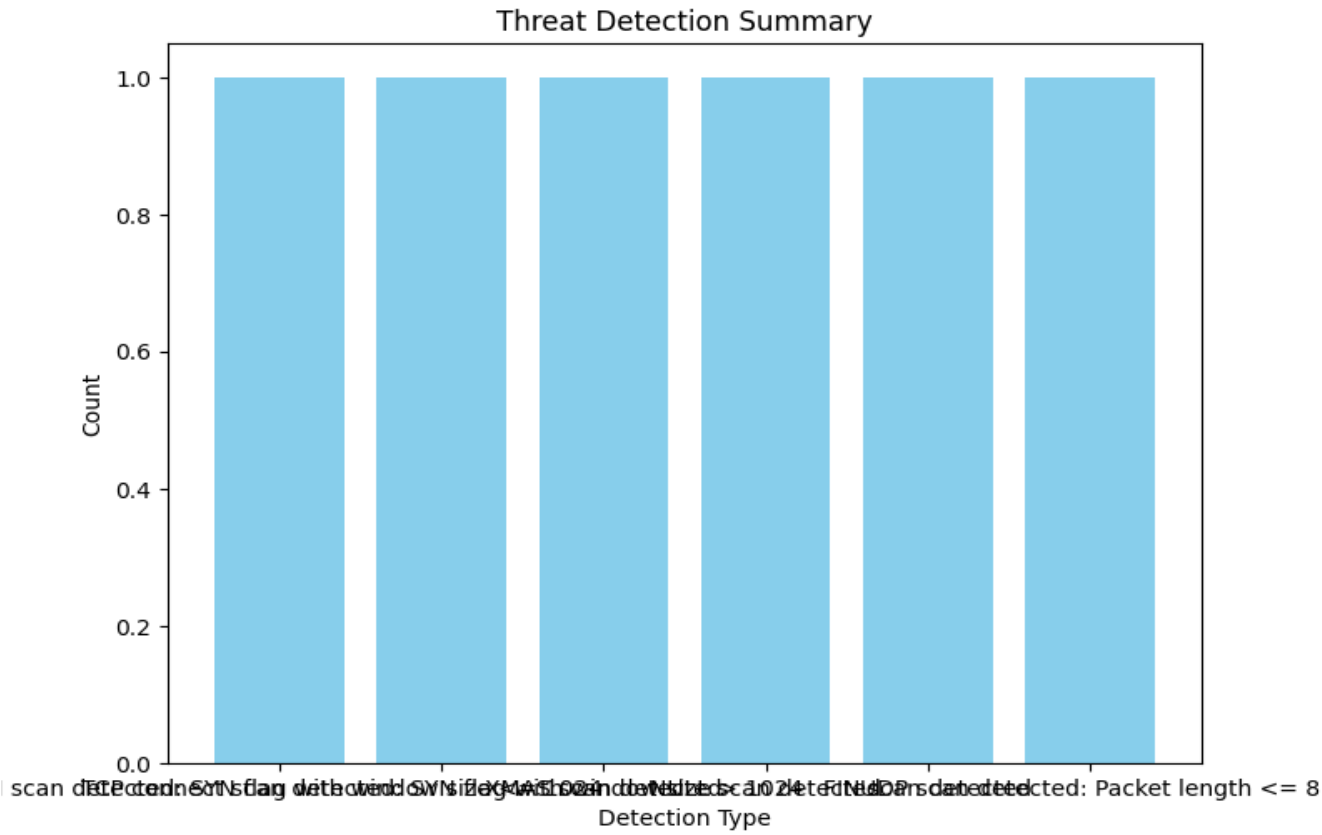
Quarantine source IP: Block 192.168.100.95 at network perimeter and core switches
IDS Rule Update: Add signatures for window size thresholds (≤1024) and malformed flag combinations
Endpoint Hardening: Audit 192.168.100.99 for unnecessary open ports/services
Network Architecture Improvements

Implement port security: Enable TCP strict mode (RFC 5961) on critical servers
Segmentation: Create VLAN isolation between .95 and .99 subnets
UDP Rate Limiting: Configure QoS policies for DNS/SNMP services
Forensic Follow-Up

Packet capture analysis: Extract full session data between .95 and .99
Host memory dump: Check 192.168.100.95 for rootkit presence
Log correlation: Cross-reference with authentication logs for potential credential stuffing
Policy Updates

Internal scanning policy: Prohibit unapproved port scanning between subnets
Firewall configuration: Drop all packets with conflicting TCP flags
Monitoring enhancement: Deploy NetFlow analysis for baseline traffic profiling

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