Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

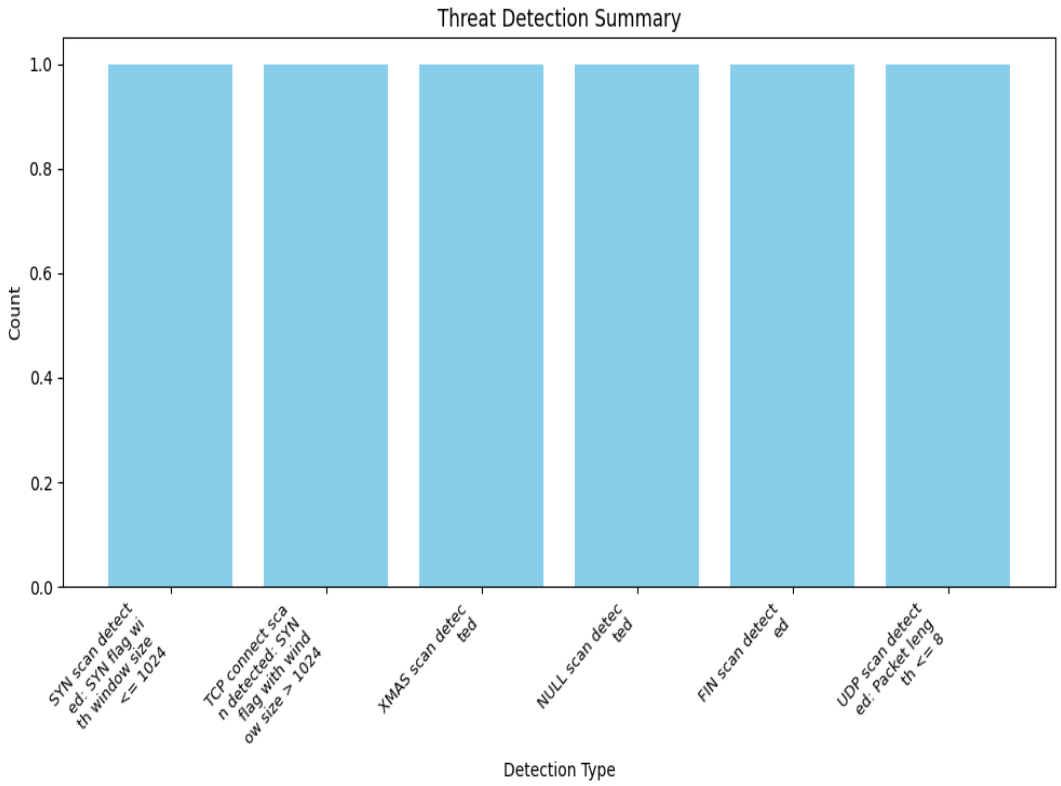
Reconnaissance activity detected from internal IP 192.168.100.95 targeting 192.168.100.99 via multiple TCP/UDP scan techniques.
Six distinct scan types identified, including SYN, TCP connect, XMAS, NULL, FIN, and UDP scans, indicating a systematic probing effort.
No direct attack packets (TCP/UDP/ICMP/ARP) observed post-scanning activity, suggesting reconnaissance as the primary objective.
Risk Assessment

Critical Risks:
High likelihood of pre-attack reconnaissance (Severity: High): Multiple stealth scans suggest an attacker is mapping network defenses and identifying vulnerabilities.
Internal host compromise risk (Severity: High): Scans originated from 192.168.100.95, indicating potential insider threat or compromised internal device.
Medium Risks:
UDP scan exposure (Severity: Medium): Short UDP packets (length ≤ 8) could indicate DNS/SNMP service enumeration attempts.
Threat Observations

Scan Pattern Analysis:
Source IP 192.168.100.95 executed **five TCP-based scans** (packets 199-207) within 0.2 seconds, including:
SYN scan (window size ≤ 1024)
TCP connect scan (window size > 1024)
XMAS/NULL/FIN scans (abnormal flag combinations)
UDP scan detected with minimal packet length (≤ 8 bytes), often used for service discovery.
Behavioral Indicators:
Sequential packet numbers (199, 201, 203, etc.) and identical source/destination IPs suggest automated tool usage (e.g., Nmap).
Absence of follow-up traffic implies scans were blocked or attackers abandoned further action.
Recommendations

Immediate Actions:
Quarantine 192.168.100.95 for forensic analysis to determine if it is compromised.
Block anomalous TCP flag combinations at firewalls (e.g., drop XMAS/NULL/FIN scans).
Enforce strict UDP payload inspection for packets under 64 bytes to critical services.
Long-Term Mitigations:
Implement network segmentation to restrict internal host-to-host communication.
Deploy IDS signatures targeting TCP window size anomalies and stealth scan patterns.
Enable TCP RST rate limiting to disrupt SYN/TCP connect scan effectiveness.
Conduct endpoint hardening on 192.168.100.99 to close non-essential ports/services.

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

Appendix: Raw Traffic Analysis Data


```
{
"detection_counts": {
"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
},
"attack_stats": {
"tcp_packets": 0,
"udp_packets": 0,
"icmp_packets": 0,
"arp_packets": 0
},
"top_threats": [
{
"packet_number": 199,
"timestamp": "2025-03-20T07:47:31.388726",
"minute": "2025-03-20 07:47",
"protocols": [
"TCP"
],
"src_ip": "192.168.100.95",
"dst_ip": "192.168.100.99",
"src_port": null,
"dst_port": null,
"detection_details": [
"SYN scan detected: SYN flag with window size <= 1024"
]
},
{
"packet_number": 201,
"timestamp": "2025-03-20T07:47:31.437189",
"minute": "2025-03-20 07:47",
"protocols": [
"TCP"
],
"src_ip": "192.168.100.95",
"dst_ip": "192.168.100.99",
"src_port": null,
"dst_port": null,
"detection_details": [
"TCP connect scan detected: SYN flag with window size > 1024"
]
},
{
"packet_number": 203,
"timestamp": "2025-03-20T07:47:31.489040",
"minute": "2025-03-20 07:47",
"protocols": [
```

```
"TCP"
],
"src_ip": "192.168.100.95",
"dst_ip": "192.168.100.99",
"src_port": null,
"dst_port": null,
"detection_details": [
"XMAS scan detected"
]
},
{
"packet_number": 205,
"timestamp": "2025-03-20T07:47:31.541120",
"minute": "2025-03-20 07:47",
"protocols": [
"TCP"
],
"src_ip": "192.168.100.95",
"dst_ip": "192.168.100.99",
"src_port": null,
"dst_port": null,
"detection_details": [
"NULL scan detected"
]
},
{
"packet_number": 207,
"timestamp": "2025-03-20T07:47:31.588889",
"minute": "2025-03-20 07:47",
"protocols": [
"TCP"
],
"src_ip": "192.168.100.95",
"dst_ip": "192.168.100.99",
"src_port": null,
"dst_port": null,
"detection_details": [
"FIN scan detected"
]
}
]
}
```