Network Traffic Security Analysis Report

Overall Threat Assessment

Threat Level: 10/10

Table of Contents

Executive Summary

Network Traffic Security Analysis ReportExecutive Summary

398 instances of TCP connect scans detected from external IP 192.100.100.100 targeting internal IP 192.168.100.99.
Activity occurred in a concentrated timeframe (2025-03-20 13:42), indicating a rapid, systematic reconnaissance attempt.
No direct TCP/UDP/ICMP/ARP attack payloads observed, but scan behavior suggests preparation for potential exploitation.
Risk Assessment

Critical Risk: **TCP SYN scan activity** (Severity: **High**).

Reconnaissance scans may precede targeted attacks (e.g., vulnerability exploitation, lateral movement).
Source IP (192.100.100.100) is external, indicating potential threat actor probing.

Moderate Risk: Repeated connection attempts to internal IP 192.168.100.99 (likely a high-value asset).
Threat Observations

Technical Findings:

398 detections of TCP connect scan detected: SYN flag with window size > 1024.
Scans used **abnormally large TCP window sizes** (>1024), a tactic to bypass legacy intrusion detection systems.
Source IP 192.100.100.100 sent SYN packets **without completing handshakes**, consistent with a TCP half-open scan pattern.
All malicious packets targeted the same internal IP (192.168.100.99), suggesting deliberate focus.
No ports specified in traffic data, implying a broad port-sweep attempt.

Recommendations

Immediate Actions:

Block source IP 192.100.100.100 at the firewall and blacklist it in intrusion prevention systems (IPS).
Investigate internal host 192.168.100.99 for exposed services, open ports, or vulnerabilities.

Network Hardening:

Tune IDS/IPS rules to flag SYN packets with window sizes >1024 as high-priority alerts.
Implement **rate limiting** for SYN packets per source IP to mitigate scan attempts.
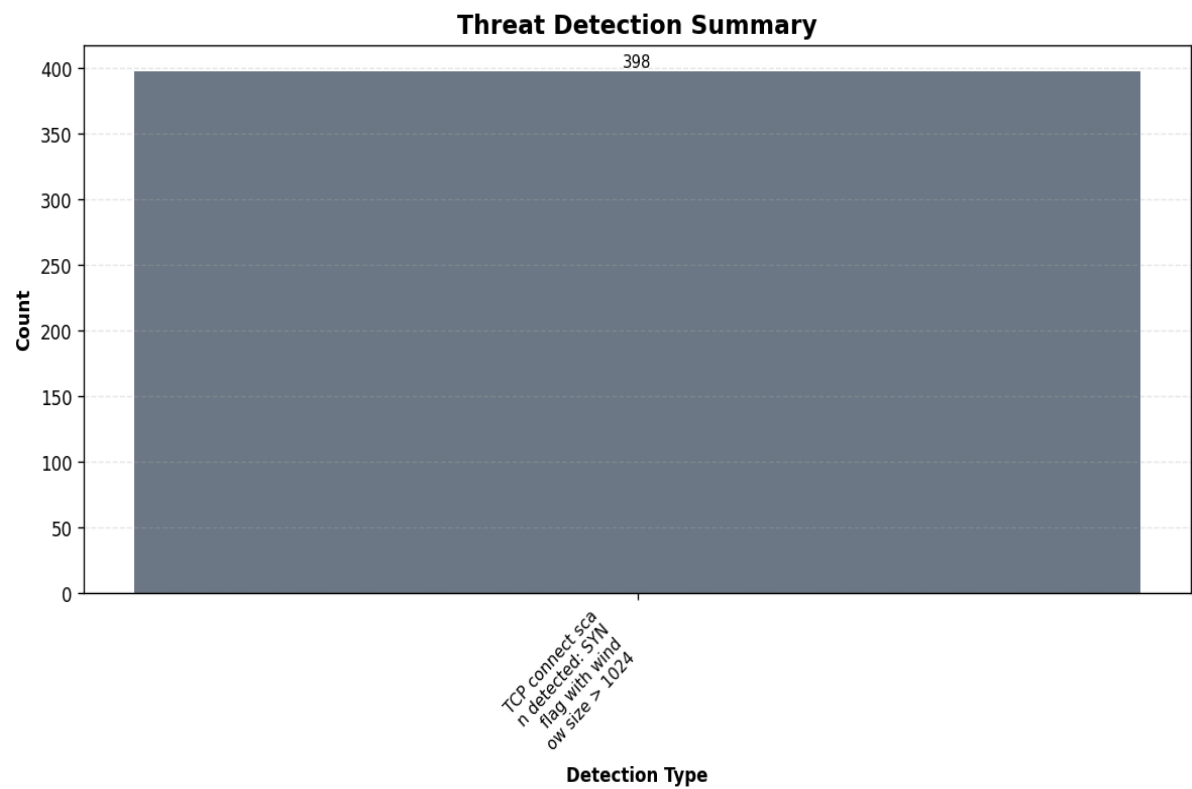
Long-Term Measures:

Conduct a **penetration test** on 192.168.100.99 to identify exploitable weaknesses.
Review and update **network segmentation policies** to restrict external access to critical internal assets.
Enable **TCP stack hardening** (e.g., SYN cookies, reduced SYN-RECEIVED state timeout) on edge devices.

Threat Detection Summary

Detection Details

Detection Type	Count
TCP connect scan detected: SYN flag with window size > 1024	398

Source/Destination Analysis

IP Address	As Source	As Destination	Total
192.100.100.100	5	0	5
192.168.100.99	0	5	5

Event Timeline

Time	Packet #	Protocol	Detection
13:42:19.729	1	TCP	TCP connect scan detected: SYN flag with window size > 1024
13:42:19.804	3	TCP	TCP connect scan detected: SYN flag with window size > 1024
13:42:19.853	5	TCP	TCP connect scan detected: SYN flag with window size > 1024
13:42:19.924	7	TCP	TCP connect scan detected: SYN flag with window size > 1024
13:42:19.969	9	TCP	TCP connect scan detected: SYN flag with window size > 1024

Appendix: Raw Traffic Analysis Data

```json
{
  "detection_counts": {
    "TCP connect scan detected: SYN flag with window size > 1024": 398
  },
  "attack_stats": {
    "tcp_packets": 0,
    "udp_packets": 0,
    "icmp_packets": 0,
    "arp_packets": 0
  },
  "top_threats": [
    {
      "packet_number": 1,
      "timestamp": "2025-03-20T13:42:19.729031",
      "minute": "2025-03-20 13:42",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.100.100.100",
      "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": 3,
      "timestamp": "2025-03-20T13:42:19.804804",
      "minute": "2025-03-20 13:42",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.100.100.100",
      "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": 5,
      "timestamp": "2025-03-20T13:42:19.853087",
      "minute": "2025-03-20 13:42",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.100.100.100",
      "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": 7,
      "timestamp": "2025-03-20T13:42:19.924889",
      "minute": "2025-03-20 13:42",
```

```
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.100.100.100",
      "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": 9,
      "timestamp": "2025-03-20T13:42:19.969205",
      "minute": "2025-03-20 13:42",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.100.100.100",
      "dst_ip": "192.168.100.99",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    }
  ]
}
```