Network Traffic Security Analysis Report

Overall Threat Assessment

Threat Level: 10/10

Table of Contents

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

398 instances of TCP connect scans detected from a single source IP (192.100.100.100) targeting 192.168.100.99.
No malicious UDP, ICMP, or ARP traffic observed.
Attack pattern: Repeated SYN packets with abnormally large window sizes (>1024), indicative of reconnaissance activity.
Risk Assessment

Critical Risk: **TCP SYN scanning** (severity: **High**) – Indicates active network reconnaissance, potentially preceding exploitation.
Source IP (192.100.100.100) should be treated as hostile due to repeated scanning behavior.
Target Risk: Internal IP (192.168.100.99) may be exposed to follow-up attacks if ports/services are vulnerable.
Threat Observations

Scanning Technique:

TCP SYN scans with window sizes >1024 (unusual for legitimate traffic, often used to bypass basic detection).
No completed handshakes (no ACK responses observed), suggesting a stealthy scan.

Traffic Pattern:

High frequency (398 detections) from a single source within a short timeframe.
Targeted at internal IP (192.168.100.99), indicating possible interest in a specific host.

Protocol Analysis:

No malicious UDP/ICMP/ARP packets, confirming the attack is TCP-focused.

Recommendations

Immediate Actions:

Block source IP (192.100.100.100) at the firewall to prevent further scanning.
Review logs on 192.168.100.99 for signs of prior compromise.

Long-Term Mitigations:

Deploy IDS/IPS rules to flag SYN packets with abnormal window sizes.
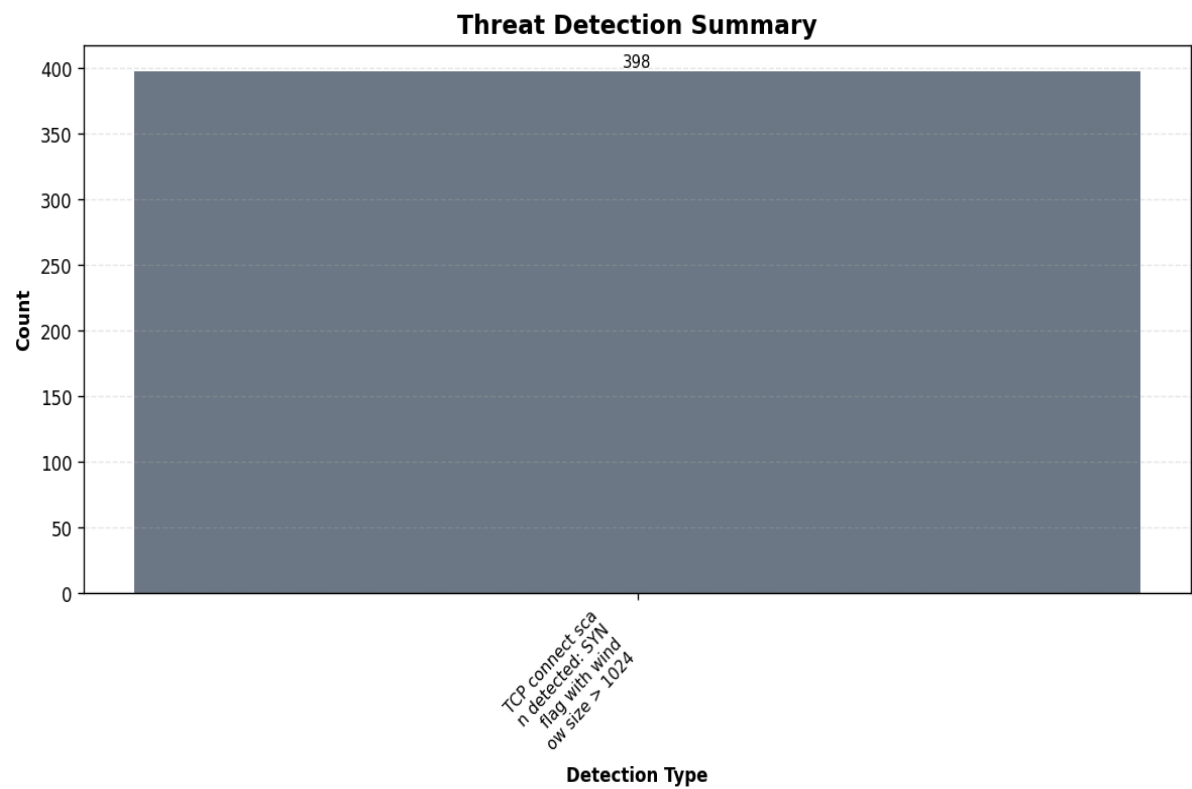**Segment internal networks** to limit lateral movement if a breach occurs.
Conduct vulnerability scans on 192.168.100.99 to identify exposed services.

Monitoring Enhancements:

Enable SYN flood protection on perimeter devices.
Alert on repeated SYN scans from single sources.

Threat Detection Summary

Threat Detection Summary

398

Count

400

350

300

250

200

150

100

50

0

TCP connect sca
n detected: SYN
flag with wind
ow size > 1024

Detection Type

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

```
{
  "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"
      ]
    }
  ]
}
```