Advanced SOC Incident Report: Port Scan Detection & Analysis

Report ID: SOC-IR-2026-001
Date: January 25, 2026
Classification: Confidential
Incident Severity: Medium
Status: Resolved

---

1. Executive Summary

A network reconnaissance activity was detected involving a **TCP SYN port scan** targeting an internal host (`192.168.0.170`). The scan originated from `192.168.0.179` using **Nmap's stealth scanning technique (`-sS`)**.

The activity was identified through **Wireshark packet analysis**, which revealed multiple SYN packets sent to a wide range of destination ports without completion of the TCP three-way handshake. No exploitation attempts or data exfiltration were observed. The incident was successfully contained and documented following SOC procedures.

---

2. Incident Timeline

Timestamp (UTC)	Event
2026-01-25 09:15:32	First SYN packet observed from attacker
09:16:18	Suspicious traffic identified during packet capture
09:17:05	SOC analyst initiated investigation
09:20:00	Attacker IP blocked at perimeter firewall
09:25:00	Incident documented and escalated
09:30:00	System owner notified
09:45:00	Scan activity ceased

---

3. Incident Details

- **Attack Type:** Network Reconnaissance – TCP SYN Port Scan
- **Attacker IP:** `192.168.0.179`
- **Victim IP:** `192.168.0.170`
- **Tool Identified:** Nmap
- **Observed Command:**

```
nmap -sS -p 1-1000 192.168.0.170
```

- **Protocols Involved:** TCP
- **Targeted Ports:** 1–1000
  - Common ports observed: 21, 22, 23, 25, 53, 80, 110, 139, 143, 443
- **Duration:** ~2 minutes
- **Packet Count:**
  - Total packets captured: 2280
  - SYN packets: 1000

---

4. Environment

- **Network Type:** Internal lab environment
- **Monitoring Tool:** Wireshark
- **Attacker System:** Linux-based (Kali Linux inferred)
- **Victim System:** Internal Linux host

---

5. Evidence & Wireshark Analysis

Wireshark Display Filter Used

```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

Observations

- Repeated TCP SYN packets sent to multiple destination ports.
- No ACK responses from the victim, indicating half-open connections.
- Consistent TTL value of 64, suggesting a Linux-based attacker.
- Average packet interval of ~120 milliseconds, indicating automated scanning behavior.

Packet Analysis Summary

- SYN packets sent sequentially to increasing port numbers.
- TCP handshake not completed.
- No established TCP sessions observed.

Evidence Files:

- PCAP: `port_scan_attack.pcap`
- Screenshots: Wireshark packet list, TCP details pane, statistics view.

---

6. Indicators of Compromise (IOCs)

Type	Value	Description
IPv4	192.168.0.179	Attacker IP
IPv4	192.168.0.170	Victim IP
Port Range	1–1000	Scanned ports
TCP Flags	SYN=1, ACK=0	SYN scan signature
Tool	Nmap	Reconnaissance utility

---

7. Impact Assessment

Security Aspect	Impact Level	Description
Confidentiality	Low	No data accessed
Integrity	None	No changes made
Availability	Low	No service disruption
Overall Risk	Medium	Reconnaissance may precede attacks

Potential Risk if Undetected:
Service enumeration followed by vulnerability exploitation and lateral movement.

---

8. Response Actions Taken

Containment

- Blocked attacker IP (`192.168.0.179`) at the perimeter firewall.
- Added detection logic for repeated SYN packets.

Investigation

- Reviewed packet captures for additional malicious behavior.
- Verified no other internal hosts were targeted.

Forensics

- Preserved PCAP files.
- Documented indicators for future correlation.

---

9. Lessons Learned & Recommendations

Immediate Actions

- Enable SYN rate limiting on edge devices.
- Improve alerting for port scan detection.

Long-Term Improvements

- Regular vulnerability scanning of internal hosts.
- Network segmentation to reduce attack surface.
- Deployment of honeypots for reconnaissance detection.

Monitoring Enhancements

- Create IDS rules for Nmap SYN scan detection.
- Increase logging visibility for denied connections.

---

10. Conclusion

The incident was successfully detected, analyzed, and contained using packet-level analysis in Wireshark. While no exploitation occurred, the activity represents a clear reconnaissance attempt that could lead to future attacks if left unaddressed. Appropriate mitigation steps were taken, and monitoring improvements were recommended to enhance detection capabilities.

---

11. Report Metadata

- **Prepared By:** *BATRAJU SAIRAM* – SOC Analyst (L1)
- **Next Review Date:** February 25, 2026

---

12. Appendices

- **Appendix A:** Wireshark Screenshots
- **Appendix B:** PCAP Metadata