Case Report: Nmap Scan Detection

Case ID: INC-2025-0802-001

Date/Time: 02 August 2025, 8:15 PM

Reported By: SOC Analyst (L1) – Kabir Bagalkot

Summary:

A security alert was triggered because the IP address **192.168.177.129** tried to connect to the **1 unique host (192.168.177.130) 143 times.** This is an unusually high number of attempts and suggests someone might be scanning the network to find open ports or weakness.

Detection Details:

Detection Type: Nmap Scan Detection

Source IP: 192.168.177.129 (Attacker – Kali Linux)

Destination IP: 192.168.177.130 (Victim – Metasploitable 3)

Count: 143 connection attempts

Unique Ports Scanned – 143

Unique Hosts Scanned – 1

Log Source: Syslog (forwarded to Splunk)

Detection Query:

```
index=main (192.168.177.129 OR 192.168.177.130)

| search NOT "dhclient" NOT "DHCP"

| stats dc(host) as unique_hosts count by src_ip

| search unique_hosts > 1 OR count > 20
```

Query Explanation:

This query searches the **main** index for logs involving the IP's **192.168.177.129** or **192.168.177.130** excluding the event containing the **dhclient** and **DHCP.** It then calculates the number of **unique_hosts** and the total connection attempts **count** by **src_ip.** Finally, it filters to show only those where **unique_hosts** is greater than 20, which can indicate scanning activity.

True Positive: This is confirmed malicious activity because the source IP made a large number of scan attempts (143) in a short time.

Analysis:

After checking the Splunk logs and Wireshark packet captures, we confirmed that **192.168.177.129** made **143 connections attempts** to different open ports on **192.168.177.130.** This behavior matches typical scanning activity (like Nmap scans) used by attackers to find weakness.

Escalation: Yes, this needs to be escalated to the SOC level 2 (Incident Response) team.

Reason for Escalation:

- The attacker attempted connections to **143 ports** within a short timeframe, which indicates targeted reconnaissance activity.
- Further forensic analysis is required to determine the attacker’s intent, the full scope of scanning activity and whether any exploitation attempts occurred.
- L2 SOC analysts will conduct deeper investigations, including correlating data with firewall, IDS/IPS, and endpoint logs, and will take containment actions as required.

Proposed Action:

- **Block** or **isolate the source IP (192.168.177.129)** at the firewall to prevent further reconnaissance attempts.
- **Review network-wide logs** for any additional scanning or suspicious activity originating from this IP address.
- **Perform a vulnerability assessment** on the victim system (192.168.177.130) to identify any exposed or exploitable ports.
- **Update SIEM use cases and correlation rules** to ensure similar scanning patterns are detected and alerted on promptly.

Status: This incident has been escalated to the SOC L2 team for in-depth investigation and containment. Awaiting their findings and recommendations.