SPLUNK NMAP DETECTION REPORT

By: Monishraj Mathivanan

Date : 10TH Marh 2025

Contents

Splunk Nmap Detection and Source IP Tracking Report

1. Introduction

This report provides an overview of using Splunk and Sysmon for detecting Nmap scans performed on a Windows 10 machine. The test was conducted in a VirtualBox environment, where:

- Windows 10 (Victim Machine) had Splunk and Sysmon installed to monitor network activity.
- Kali Linux (Attacker Machine) performed an Nmap scan against Windows 10.
- Both machines were configured in a host-only adapter mode to ensure they were in the same network.
- The Windows firewall was temporarily disabled to allow ICMP packets and port scanning traffic.

2. Setup and Configuration

2.1 Environment Details

Victim Machine (Windows 10) Details:
- **OS:** Windows 10
- **Installed Tools:** Splunk Enterprise, Sysmon
- **Network:** Host-only adapter

Attacker Machine (Kali Linux) Details:
- **OS:** Kali Linux
- **Tool Used:** Nmap
- **Network:** Host-only adapter

2.2 Sysmon Installation & Configuration

Sysmon was installed and configured on Windows 10 to log all network events. The following command was executed to install Sysmon with a configuration file:

.sysmon64.exe -i sysmonconfig.xml

```
C:\Users\mmat0\Downloads\Sysmon> .\sysmon64.exe -i sysmonconfig.xml


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.90
Configuration file validated.
The service Sysmon64 is already registered. Uninstall Sysmon before reinstalling.


C:\Users\mmat0\Downloads\Sysmon>
```

3. Attack Execution - Nmap Scan

The attacker, using Kali Linux, executed an Nmap scan on the Windows 10 machine to detect open ports. The following command was used:

nmap -sV -p- 192.168.56.101

```
┌──(root㉿kali)-[/home/monish]
└─# nmap -Pn -sS -p- 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-09 21:27 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0090s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5040/tcp  open  unknown
8000/tcp  open  http-alt
8089/tcp  open  unknown
8191/tcp  open  limnerpressure
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
MAC Address: 08:00:27:F2:73:8E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 167.32 seconds
```

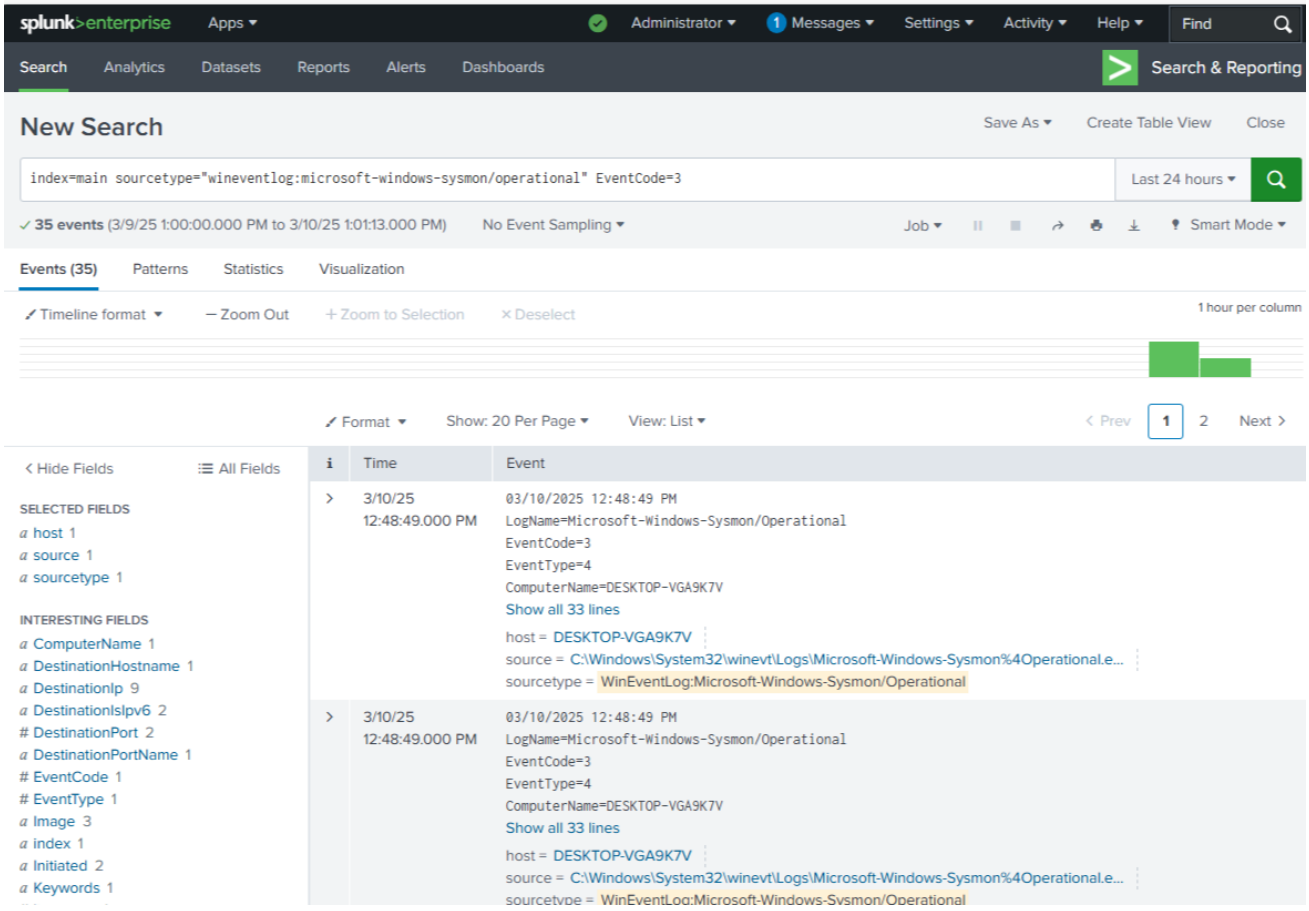
4. Detection Using Splunk

4.1 Why We Used Event Code 3 to Filter Search

Event Code 3 in Sysmon refers to network connection events, which log details of all outgoing and incoming connections on the system. This event is crucial in identifying network-based attacks, such as port scanning, unauthorized access attempts, and malware communications. Since an Nmap scan involves making multiple network connections, filtering by Event Code 3 ensures we capture relevant data related to the attack.

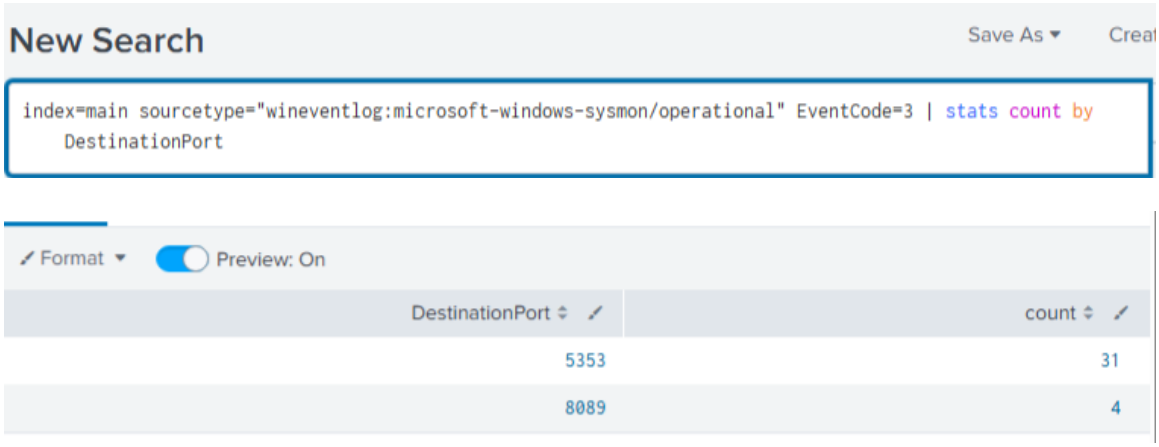
4.2 Searching for Event Code 3 (Network Connection Initiated)

index=main sourcetype="wineventlog:microsoft-windows-sysmon/operational" EventCode=3



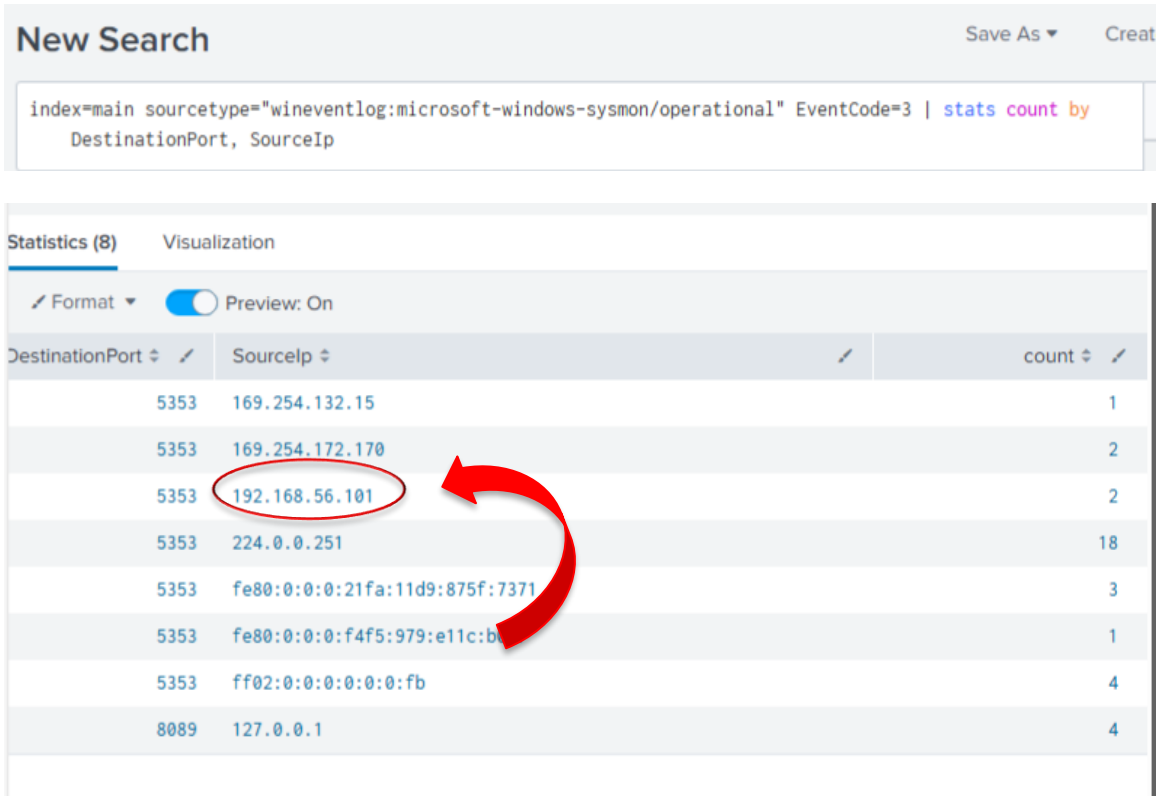
4.3 Finding the Most Targeted Ports

index=main sourcetype="wineventlog:microsoft-windows-sysmon/operational" EventCode=3 | stats count by DestinationPort



4.4 Identifying the Source of the Attack

index=main sourcetype="wineventlog:microsoft-windows-sysmon/operational" EventCode=3 | stats count by DestinationPort, SourceIp



5. Findings

Here's what I found:

- The Nmap scan successfully targeted the Windows 10 machine.
- Sysmon logs captured all network connection attempts initiated by the attacker.
- Splunk queries efficiently detected suspicious activity by analyzing destination ports and source IPs.
- The attacker's IP address (192.168.56.101) was identified using Splunk analysis.
- The most targeted port was 5353, which is associated with multicast DNS (mDNS), a common target for enumeration in penetration testing.

6. Conclusion

This experiment demonstrates the effectiveness of SIEM (Security Information and Event Management) solutions like Splunk in detecting and analyzing network attacks. By leveraging Sysmon logging and Splunk queries, we were able to:

- Detect an Nmap scan.
- Identify targeted ports.
- Trace the attack back to the attacker's IP.

Importance of SIEM in Cybersecurity

- Real-time detection of suspicious activities.
- Centralized monitoring of network traffic.
- Forensic analysis for cybersecurity investigations.
- Mitigation and response to cyber threats before they cause harm.