**Internship Report**

**Title:** **Implement Endpoint Security & Monitoring**  
**Company:** Internee.pk  
**Internship Duration:** July- September  
**Intern:** Ammad Aziz  
**Project:** Strengthening Security Measures for a Web Application

**1. Introduction**

During my internship, I explored the setup, configuration, and **analysis of Sysmon logs** using **Wazuh SIEM**. The goal was to create a centralized system for real-time log collection, event correlation, and security monitoring. This setup allowed detection and investigation of potential malicious activities by leveraging **Sysmon Event IDs** and Wazuh's alerting capabilities.

**2. Objectives**

* Install and configure the **Wazuh SIEM server** and dashboard.
* Set up the **Windows 10 VM as a Wazuh agent** with Sysmon integration.
* Analyze key **Sysmon Event IDs** for detecting suspicious activities.
* Build a foundational understanding of **threat detection workflows** in a SOC environment.

**3. Tools and Technologies Used**

* **Wazuh (SIEM Platform)** – Log collection, correlation, and alerting.
* **Sysmon (System Monitor)** – Advanced event logging for process and network activities.
* **VirtualBox** – For hosting Windows and Wazuh virtual environments.
* **Windows 10 VM** – Monitored endpoint with Sysmon installed.
* **Bridge Networking** – To enable agent-server communication.

**4. Implementation Steps**

**Step 1: Wazuh Server Setup**

* Imported the **Wazuh OVA file** into VirtualBox.
* Configured the network adapter in **Bridge Mode**.
* Retrieved server IP via ip a and accessed the **Wazuh dashboard** in a browser.

**Step 2: Wazuh Agent and Sysmon Integration**

* Installed **Wazuh agent** on the Windows 10 VM.
* Edited ossec.conf to:
  + Update server IP.
  + Add **Sysmon event channels** for advanced logging.
* Restarted the Wazuh agent to start log transmission.

**Step 3: Sysmon Event ID Analysis**

After integration, I analyzed **critical Sysmon Event IDs** to detect specific types of suspicious activity. Key examples include:

|  |  |  |
| --- | --- | --- |
| Event ID | Description | Use Case |
| 1 | Process creation | Detecting suspicious executables like mimikatz.exe. |
| 5 | Process Termination | Detecting suspicious executables like mimikatz.exe. |
| 3 | Network connections | Monitoring unusual outbound connections. |
| 7 | Image loaded | Detecting DLL injection attempts. |
| 10 | Process access | Identifying credential dumping behaviors. |
| 11 | File created | Monitoring creation of executables in suspicious directories. |
| 13 | Registry modifications | Detecting persistence techniques. |

**Step 4: Verification**

* Confirmed **real-time log flow** to the Wazuh dashboard.
* Filtered logs by **Event ID** to detect specific behaviors.
* Simulated basic test activities (e.g., process executions) to validate alerts.

**5. Key Learnings**

* Understood how **Sysmon logs enhance endpoint visibility**.
* Learned to **map Event IDs** to common attack techniques.
* Built a foundational knowledge of **incident detection workflows** in SIEM systems.
* Developed troubleshooting skills for **network and agent configuration**.

**6. Challenges Faced**

* Network bridging issues during initial setup.
* Fine-tuning ossec.conf to properly include Sysmon logs.
* Managing the volume of logs while focusing on relevant event IDs.

**7. Future Work**

* Create **custom Wazuh rules** for specific Sysmon Event IDs.
* Implement **alerting thresholds** to minimize noise and false positives.
* Integrate Wazuh with additional tools for a **full SOC simulation**.

**8. Conclusion**

This internship task provided **hands-on SOC experience**, from setting up a SIEM solution to analyzing endpoint logs for security insights. By leveraging **Sysmon Event IDs** within Wazuh, I gained practical knowledge in detecting suspicious activities and building a foundation for advanced threat detection and incident response.