Sysmon

## **Task 1 – Introduction**

* Sysmon (**System Monitor**) is a Windows system service and device driver that logs detailed system activity to the Windows Event Log.
* Part of the **Sysinternals Suite**, commonly used for **threat hunting and incident response**.

## **Task 2 – Sysmon Overview**

* Captures:
  + **Process creation** (with hashes, parent/child info).
  + **Network connections** (IP, ports, process ID).
  + **File creation time changes**.
  + **Registry modifications**.
  + **Named pipe usage**.
* Outputs logs to **Applications and Services Logs → Microsoft → Windows → Sysmon → Operational**.

## **Task 3 – Installing and Preparing Sysmon**

* Download: Sysinternals Suite
* Install:

powershell

CopyEdit

sysmon64.exe -accepteula -i sysmonconfig.xml

* sysmonconfig.xml defines **what to log** (rules, filters).
* Use community configs like **SwiftOnSecurity’s** as a baseline.

## **Task 4 – Cutting out the Noise**

* Avoid overwhelming logs by filtering **known good** processes and locations.
* Focus on:
  + Unusual parent-child process relationships.
  + Processes running from temp directories.
  + Suspicious network connections.
* Use **include/exclude rules** in sysmonconfig.xml.

## **Task 5 – Hunting Metasploit**

* Look for:
  + **Unusual network connections** to attacker IPs.
  + Reverse shell processes (e.g., powershell.exe spawned from cmd.exe).
  + Event IDs: **1** (Process Create) & **3** (Network Connection).

## **Task 6 – Detecting Mimikatz**

* Indicators:
  + Execution of mimikatz.exe or renamed binaries.
  + Processes accessing **LSASS.exe** memory (Event ID 10).
  + Parent process anomalies (e.g., PowerShell → mimikatz).

## **Task 7 – Hunting Malware**

* Watch for:
  + **Unsigned executables** in unusual directories.
  + Script execution from temp/appdata.
  + Process injection (Event ID 8).

## **Task 8 – Hunting Persistence**

* Persistence indicators:
  + Registry Run keys modifications (Event ID 13).
  + Scheduled task creation (Event ID 1 with schtasks.exe).
  + Service installation (Event ID 6).

## **Task 9 – Detecting Evasion Techniques**

* Signs:
  + Clearing logs (wevtutil cl).
  + Tampering with Sysmon service.
  + Disabling security tools.

## **Task 10 – Practical Investigations**

* Use Sysmon logs for:
  + Tracing initial infection vector.
  + Identifying C2 (Command & Control) connections.
  + Mapping attacker’s lateral movement.
* Combine Sysmon data with **SIEM tools** for advanced correlation.

     