Event Log Analysis

Thomas Benos

MSc UniWA, Cisco CyberOps
GR CSIRT Incident Responder
thomasbenos1291@gmail.com

Agenda

- Introduction to Windows Event Logs
- Important Windows Event Logs

Introduction to Windows Event Logs

Windows Event Logs

- **Definition:**
  - Windows Event Logs are a centralized repository of system, security, and application events that occur on a Windows operating system.
  - Event Logs serve as a critical component for system administrators, IT professionals, and forensic analysts to monitor, troubleshoot, and analyze system activities.
  - Events include timestamps indicating when the event occurred. These timestamps are crucial for timeline analysis and forensic investigations.
  - Windows Event Logs are of immense forensic significance, aiding in the reconstruction of events, identifying security incidents, and establishing timelines.

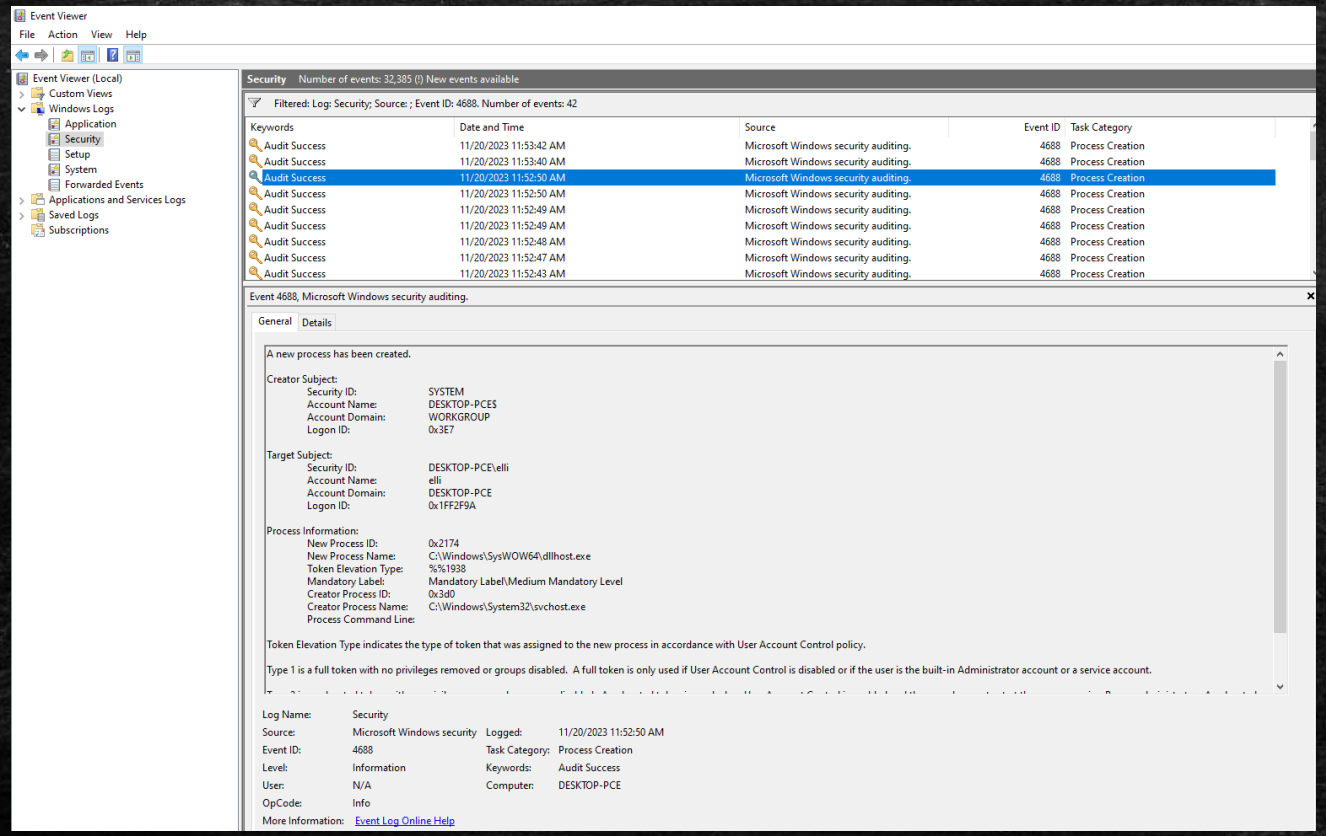
- **Location:**
  - C:\Windows\system32\winevt\
  - HKLM\System\CurrentControlSet\Services\EventLog\

Windows Event Logs

- **Categories:**
  - Windows Event Logs are categorized into three main types:
    1. **System Log:** Records events related to the operating system's core functionality.
    2. **Security Log:** Captures security-related events, including login attempts, user privilege changes, and more.
    3. **Application Log:** Logs events generated by applications and programs.
  - In Windows Event Logs are logged and other categories such as:
    - Windows Defender & Windows Firewall
    - Powershell
    - Task Scheduler
    - Server – Spercific Event Logs (DC, DNS, etc)
- **Event Levels:**
  - Events in the logs are assigned different levels:
    - **Informational:** General events providing information about system activities.
    - **Warning:** Indicates potential issues or abnormal conditions.
    - **Error:** Indicates critical errors or failures.
    - **Critical:** Signifies severe issues that may lead to system instability.

Windows Event Viewer

- **Windows Event Viewer:**
  - The Windows Event Viewer is the graphical interface for viewing and managing event logs. It allows users to filter, search, and export log entries.



Important Windows Event Logs

Tracking Account Usage - Security

- 4624 : Successful Logon
- 4625 : Failed Logon
- 4634/4647 : Successful Log Off
- 4648 : Logon using explicit credentials (Run As)
- 4672 : Account Logon with superuser rights (Admin)

Tracking Account Usage – Logon Types

- **Logon Types:**
  - Logon Type 2 – Interactive (local)
  - Logon Type 3 – Network (e.g via SSH)
  - Logon Type 4 – Batch (Scheduled Tasks)
  - Logon Type 5 – Service
  - Logon Type 7 – Unlock
  - Logon Type 8 – NetworkCleartext
  - Logon Type 9 – NewCredentials
  - Logon Type 10 – RemoteInteractive (RDP)
  - Logon Type 11 – CachedInteractive (cached credentials)
  - Logon type 12 – CachedRemoteInteractive (RDP cached credentials)
  - Logon type 13 - CachedUnlock

Tracking Account Usage – Windows System Accounts (1/2)

- **Windows System Accounts:**
  - Windows System Accounts are special accounts created by the operating system for specific system-level tasks and services.
  - These accounts are commonly used to run Windows services, ensuring that services have the necessary permissions to perform their tasks.
- **Common System Accounts:**
  - **NT AUTHORITY\SYSTEM:** The Local System account with extensive privileges, often used by system services.
  - **NT AUTHORITY\NETWORK SERVICE:** An account with network access privileges used by system services.
  - **NT AUTHORITY\LOCAL SERVICE:** An account with restricted privileges for local service processes.

Auditing Accounts

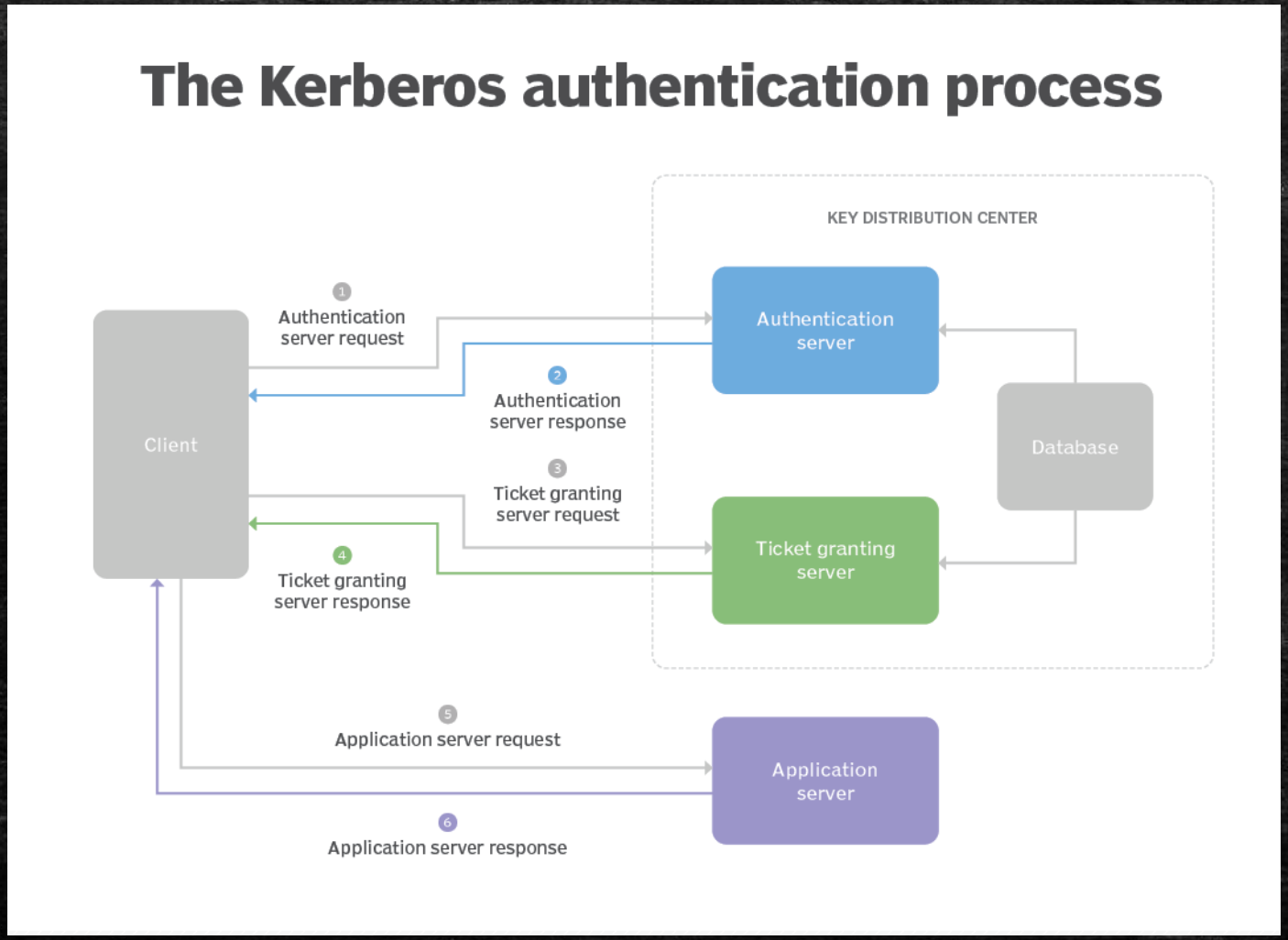
- 4720 : Account created
- 4722 : User account was enabled
- 4724 : Attempt to reset accounts' password
- 4728 : Member added to security enabled global group
  - Global means the group can be granted access in any trusting domain but may only have members from its own domain.
- 4732 : Member added to security enabled local group
- 4735 : Security enabled local group changed
- 4756 : Member added to security enabled universal group
  - Universal means the group can be granted access in any trusting domain and may have members from any trusted domain.

- auditpol /set /category:"Account Management" /success:enable /failure:enable

Kerberos Authentication in Windows (1/3)

- **Definition:**
  - Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.
- **Key Components:**
  - **Key Distribution Center (KDC):**
    - Centralized authentication server managing authentication requests.
    - Consists of the Authentication Server (AS) and Ticket Granting Server (TGS).
  - **Tickets:**
    - Authentication tickets are issued by the KDC.
    - Ticket Granting Ticket (TGT) and Service Tickets are key components.
  - **Principals:**
    - Entities in the Kerberos system, such as users and services.
    - Identified by a principal name.

Kerberos Authentication in Windows (2/3)



Audit Logon Events (Domain Logons) - Kerberos

Event ID	Description
4768	A Kerberos authentication ticket (TGT) was requested.
4769	A Kerberos service ticket was requested (TGS).
4771	Kerberos pre-authentication failed.
4772	A Kerberos authentication ticket request failed.
4774	An account was mapped for logon using Kerberos authentication.
4776	The domain controller attempted to validate the credentials for an account.
4777	The domain controller failed to validate the credentials for an account.
4778	A session was reconnected to a Window Station.
4779	A session was disconnected from a Window Station.
4781	The name of an account was changed.
4765	SID History was added to an account.
4766	An attempt to add SID History to an account failed.
4770	A Kerberos service ticket request was made.
4773	A Kerberos service ticket request failed.

Kerberos – Related Attacks & Detection (1/2)

- **Golden Ticket Attack:**
  - **Description:** In a Golden Ticket attack, an attacker forges a Ticket Granting Ticket (TGT) with arbitrary user credentials, granting unauthorized access to the Kerberos realm.
  - **Event IDs:**
    - 4768: Request for a TGT.
    - 4771: Pre-authentication failure (brute force attempts).
    - 4769: Request for a Kerberos service ticket (TGS).
- **Silver Ticket Attack:**
  - **Description:** In a Silver Ticket attack, an attacker forges a service ticket for a specific service, allowing unauthorized access to that service.
  - **Event IDs:**
    - 4768: Request for a TGT.
    - 4771: Pre-authentication failure (if the attacker lacks necessary information).
    - 4769: Request for a Kerberos service ticket (TGS).

Kerberos – Related Attacks & Detection (2/2)

- **Pass-the-Ticket Attack:**
  - **Description:** In a Pass-the-Ticket attack, an attacker uses a captured service ticket to access a service without directly compromising user credentials.
  - **Event IDs:**
    - 4769: Request for a Kerberos service ticket (TGS).
    - 4771: Pre-authentication failure (if the attacker tries to forge a TGT).
- **Overpass-the-Hash (Pass-the-Key) Attack:**
  - **Description:** In this attack, an attacker uses captured Kerberos tickets without needing the user's password, potentially leading to lateral movement.
  - **Event IDs:**
    - 4768: Request for a TGT.
    - 4771: Pre-authentication failure (if the attacker tries to forge a TGT).
    - 4769: Request for a Kerberos service ticket (TGS).
- **Kerberoasting:**
  - **Description:** In Kerberoasting, an attacker requests service tickets for services using Ticket Granting Tickets (TGTs), aiming to crack the Ticket Encryption Key offline.
  - **Event IDs:**
    - 4768: Request for a TGT.
    - 4771: Pre-authentication failure (if the attacker tries to forge a TGT).
    - 4769: Request for a Kerberos service ticket (TGS).

Privilege Escalation (1/2)

- **Event ID 4624: Successful Logon**
  - **Indicators:**
    - Look for logon events with high-privileged accounts.
    - Monitor logons with the "Network" and "Service" logon types.
- **Event ID 4672: Special Privileges Assigned to New Logon**
  - **Indicators:**
    - Detect the assignment of special privileges to a user.
    - Look for privilege escalation attempts.
- **Event ID 4688: New Process Created**
  - **Indicators:**
    - Detect the creation of new processes, especially by accounts with high privileges.
    - Monitor command-line arguments for potential exploitation.

Privilege Escalation (2/2)

- **Event ID 7045: Service Installation**
  - **Indicators:**
    - Monitor the installation of new services.
    - Look for changes in service start types or binary paths.
- **Event ID 1102: Audit Log Cleared**
  - **Indicators:**
    - Unusual clearing of security logs may indicate an attempt to cover tracks.
    - Regularly review log clearing events.
- **Event ID 4673: A Privileged Service Was Called**
  - **Indicators:**
    - Detect attempts to use privileged services.
    - Monitor for unauthorized service calls.

RDP Event Logs

- **Purpose:**
  - Auditing RDP involves monitoring and recording events related to the use of Remote Desktop Protocol on a Windows system.
  - In digital forensics, auditing RDP is crucial for monitoring remote access activities, detecting unauthorized logon attempts, and investigating security incidents.

Security Event IDs

- 4624 + Logon Type 3 or 10 : Successful logon (including RDP logons)
- 4625 + Logon Type 3 or 10 : Failed logon attempts.
- 4778: Reconnection to a Windows Station (possibly RDP)
- 4779: Disconnection from a Windows Station (possibly RDP)

RemoteDesktopServices-RDPCoreTS

- 131: New TCP Connection Accepted from <src_ip:src_port>
- 98: TCP Connection has been successfully established

Audit RDP – Source PC

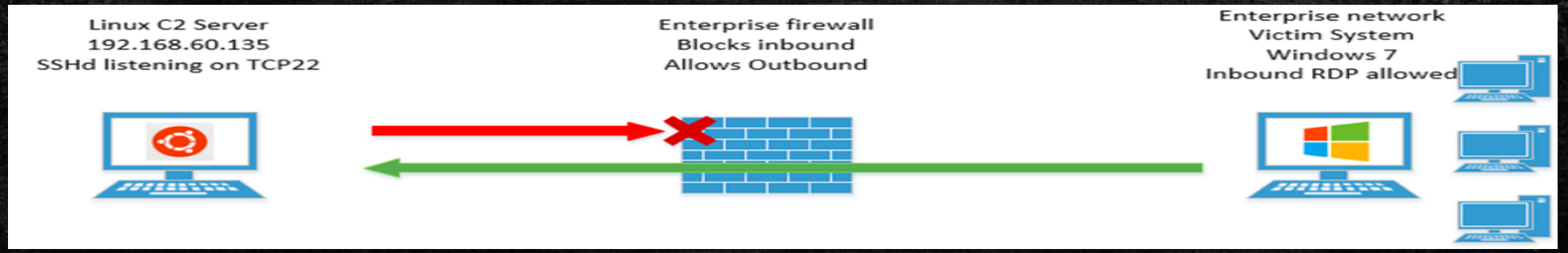
Event Log	Event IDs	Description
Security	4648	A Logon Was Attempted Using Explicit Credentials
TerminalServices-RDPClient/Operational	1024	RDP ClientActiveX is trying to connect to the server <SERVER>
	1102	The client has initiated a multi-transport connection to the server <SERVER>

Audit RDP – Destination PC

Event Log	Event IDs	Description
Security	4624 / 4625	An account was successfully logged on / failed to log on
	4778 / 4779	A session was reconnected to / disconnected from a Windows Station
	4634	An account was logged of
	4647	User initiated logoff
TerminalServices-RemoteConnectionManager/Operational	1149	User Authentication Succeeded
RemoteDesktopServices-RDPCoreTS /Operational	98	A TCP Connection has been successfully established
	131	New TCP Connection Accepted from <src_ip:src_port>
TerminalServices-LocalSessionManager/Operational	21, 22, 25	Remote Desktop Services: Session Logon Succeeded Remote Desktop Services: Shell start notification received Remote Desktop Services: Session Reconnection Succeeded
	23,40	Remote Desktop Services: Session Logoff Succeeded Session <x> has been disconnected reason code <z>

RDP Tunnelling Attack - Tunneling RDP over SSH

- **RDPing Against the Rules:**
  - Threat actors use native Windows RDP utilities for lateral movement in compromised environments.
  - They leverage RDP for remote access during targeted compromises, making intrusions harder to detect without malware.
- **Inbound RDP Tunneling:**
  - Plink (PuTTY Link) is commonly used for RDP tunneling, creating encrypted tunnels for communication.
  - Event ID 1149 (TCP Connection Succeeded) may reveal RDP tunneling activities.



RDP Tunnelling Attack - Tunneling RDP over SSH

- **Windows Event IDs:**
  - **Event ID 4624**: Successful logon in Windows Security Logs.
    - From a user account
    - Process = "sshd.exe"/ "plink.exe"
    - From (source) localhost (127.0.0.1)
    - Logon Types = 3 (Network), 8 (Network Cleartext)
    - All the above indicate a tunnelled logon routed from a listening localhost port to the localhost's RDP port TCP 3389.
  - **Event ID 4625**: Failed logon in Windows Security Logs.
  - **Event ID 21, 22, 25**: TerminalServices-LocalSessionManager/Operational logs for successful interactive logons and reconnections.
  - **Event ID 1149**: TerminalServices-RemoteConnectionManager/Operational logs for successful TCP connection.
  - **Event ID 131, 98**: RemoteDesktopServices-RDPCoreTS/Operational logs for RDP-related events.

Example Plink Executable Command:

plink.exe <users>@<IP or domain> -pw <password> -P 22 -2 -4 -T -N -C -R 12345:127.0.0.1:3389

Lateral Movement

- **Definition:**
  - Lateral movement refers to the techniques and methods attackers use to progressively move through a network, gaining access to different systems and resources.
- **5140: Network Share Accessed**
  - **Indicators of Lateral Movement:**
    - Frequent access to multiple network shares.
    - Access from unusual or unauthorized systems.
- **5145: Shared Object Accessed**
  - **Indicators of Lateral Movement:**
    - Frequent access to sensitive or critical files.
    - Access from unexpected sources.
- **5142 - 5144: Net Share Creation, Modification, Deletion**
  - **Indicators of Lateral Movement:**
    - Unusual creation, modification, or deletion of network shares.
    - Rapid changes to share configurations.

Lateral Movement

- **4624: Successful Logon**
  - **Indicators of Lateral Movement:**
    - Multiple logons from different systems.
    - Logons at odd hours or from unusual locations.
- **4625: Failed Logon**
  - **Indicators of Lateral Movement:**
    - Repeated failed logon attempts.
    - Account lockouts due to excessive failed logon attempts.
- **7045: Service Creation (System)**
  - **Indicators of Lateral Movement:**
    - Creation of suspicious services.
    - Changes to existing services.
    - Event ID 7045 is the most important event log entry to detect ransomware operators once they have gained access to a target network.
    - Over 90% of the ransomware incidents where adversaries moved laterally to at least one system.

Services Events (1/2)

- **4697: A service was installed in the system.**
  - **Indicators of Suspicious Activity:**
    - Installation of services from unknown or unauthorized sources.
    - Changes to existing services.
- **4698: Scheduled Task Created**
  - **Indicators of Suspicious Activity:**
    - Creation of scheduled tasks associated with services.
    - Changes to existing scheduled tasks.
- **4699: Service Installed by Account**
  - **Indicators of Suspicious Activity:**
    - Installation of services by non-administrator or suspicious accounts.

Services Events (2/2)

- **7034: Service Started or Stopped**
  - **Indicators of Suspicious Activity :**
    - Normal operation of services.
    - Changes in service states.
- **7035: Service Sent a Start/Stop Control**
  - **Description:** Logged when a service sends a start/stop control to another service.
  - **Indicators of Suspicious Activity :**
    - Communication between services.
    - Dependency relationships between services.
- **7036: Service Started or Stopped**
  - **Indicators of Suspicious Activity :**
    - Normal operation of services.
    - Changes in service states.
- **7040: Start Type Change**
  - **Indicators of Suspicious Activity:**
    - Changes to the start type of critical or security-related services.

Powershell Events – Capturing the Command Line

Windows Event Logs:

- **Event ID 4103: PowerShell Script Module Logging**
  - **Indicators:**
    - Attackers uses several obfuscated commands and calls self-defined variables and system commands.
    - Monitor for unusual PowerShell activities.
    - Hunting these EventIDs provide SOC operations to record all the obfuscated commands as pipeline execution details under EventID 4103.
- **Event ID 4104: PowerShell Script Block Logging**
  - **Indicators:**
    - Detection of unauthorized access or modification of script contents.
    - Captures the entire scripts that are executed by remote machines.
- **Event ID 4105/4106: PowerShell Script Start/Stop**

System Monitor (Sysmon)

- **Overview:**
  - A powerful Windows system service and device driver that, when installed and configured, logs detailed information about specific system events to the Windows event log.
  - Part of the Sysinternals suite of advanced system utilities provided by Microsoft.
  - Sysmon is designed to enhance system visibility by providing detailed information about various system activities and events.
  - Sysmon, can even capture all deleted .exe files to determine if there is an attacker in your environment trying to hide their path.
- **Event Categories:**
  - Sysmon logs events in several categories, including process creation, network connection, process termination, image loading, driver loading, and more.
  - Captures extensive details about events, such as process names, command-line arguments, parent-child process relationships, hash values of files, network connections, and more.
- **Configuration:**
  - Sysmon is configured using an XML configuration file. This file can be customized to specify the events to log, configure filters, and define output formats.

System Monitor (Sysmon)

- **Use in Security Monitoring:**
  - Sysmon is a valuable tool for security monitoring and incident response.
  - It helps in detecting and investigating suspicious or malicious activities on a Windows system.
- **Integration with SIEM:**
  - can be forwarded to a Security Information and Event Management (SIEM) system for centralized monitoring and analysis.
- **Threat Detection:**
  - provides visibility into low-level system activities that are not typically logged by default Windows logging.
- **Hash Calculation:**
  - calculates cryptographic hash values for files involved in certain events

Malicious Activity Indications – Sysmon

Sysmon Events

Category	Event ID
Sysmon Service Status Changed	0
Process Create	1
File Creation Time Changed	2
Network Connection	3
Sysmon Service State Change	4
Process Terminated	5
Driver Loaded	6
Image Loaded	7
CreateRemoteThread	8
RawAccessRead	9

Category	Event ID
Process Access	10
File Create	11
Registry Object CreateDelete	12
Registry Value Create	13
Registry Object Rename	14
File Create Stream Hash	15
Sysmon Configuration Changed	16
Pipe Created	17
Pipe Connected	18
Error	255

v6

Malicious Activity Indications – Sysmon

Sysmon Events:

- **Event ID 1: Process Create**
  - **Indicators:**
    - More detailed information than Windows Event ID 4688.
    - Capture image, command line, hash, and signature verification status.
- **Event ID 3: Network Connection**
  - **Indicators:**
    - Unusual outbound connections from a process.
    - Check for connections to known malicious IP addresses.
- **Event ID 7: Image Loaded**
  - **Indicators:**
    - Detect loading of DLLs by processes.
    - Check for DLLs associated with known malware.
- **Event ID 8: CreateRemoteThread (Injection)**
  - **Indicators:**
    - Detects code injection techniques used by malware.
    - Check for processes injecting code into others.

Malicious Activity Indications – Sysmon

Sysmon Events:

- **Event ID 10: Process Access**
  - **Indicators:**
    - Logged when a process opens another process
    - Enables detection of hacking tools that read the memory contents of processes
- **Event ID 11: File Create**
  - **Indicators:**
    - Logged when a file is created or overwritten
    - Check for suspicious files.
- **Event ID 12, 13, 14: Registry Events**
  - **Indicators:**
    - Detect creation, deletion or modification of Windows Registry.
    - Also provides the process that did the modifications.

Thank you for your patience!