HackOn 2024

THREAT HUNTING Y EL MODELADO DE AMENAZAS

Enlaces de interés, ejercicios y práctica final.

ÁNGEL LUIS VELOY MORA

1.- Una brevísima introducción al Threat Hunting

- **Slide 4.**
  - Definición TRELLIX: What Is Cyber Threat Hunting? | Trellix
  - Libro TH: Practical Threat Intelligence and Data-Driven Threat Hunting | Packt (packtpub.com)
- **Slide 7.**
  - Pyramid of Pain: Enterprise Detection & Response: The Pyramid of Pain (detect-respond.blogspot.com)
  - ATP: Advanced persistent threat - Wikipedia
  - RaaS: Ransomware as a service - Wikipedia
  - Zero day: Zero-day (computing) - Wikipedia
  - Insider: Defining Insider Threats | CISA
  - Dwell Time: What is Dwell Time for Cybersecurity? | ConnectWise
- **Slide 10.**
  - IoC vs IoA: IOA vs IOC: Understanding the Differences - CrowdStrike

2.- Modelado de amenazas. Árboles de ataque/amenaza

- **Slide 12.**
  - Attack Tree: Attack tree - Wikipedia
- **Slide 13.**
  - Attack Tree. Bruce Schneier: Academic: Attack Trees - Schneier on Security
- **Slide 22.**
  - Unified Kill Chain: Unified Kill Chain: Raising Resilience Against Cyber Attacks
  - Cyber Kill Chain: Cyber Kill Chain® | Lockheed Martin
- **Slide 23.**
  - Mitre ATT&CK: MITRE ATT&CK®
- **Slide 24.**
  - Lateral Movement: Lateral Movement, Tactic TA0008 - Enterprise | MITRE ATT&CK®
  - Lateral Tool Transfer: Lateral Tool Transfer, Technique T1570 - Enterprise | MITRE ATT&CK®
  - PsExec: PsExec, Software S0029 | MITRE ATT&CK®
- **Slide 25.**
  - BlackCat: BlackCat, Software S1068 | MITRE ATT&CK®
  - Navigator ATT&CK BlackCat: ATT&CK® Navigator (mitre-attack.github.io)
- **Slide 26.**
  - BlackCat BCSC-Malware-BlackCat: bcsc-malware-blackcat-tlpwhite.pdf (ciberseguridad.eus)
  - The many lives of BlackCat ransomware. Microsoft: The many lives of BlackCat ransomware | Microsoft Security Blog
  - Ransomware Spotlight. BlackCat: Ransomware Spotlight: BlackCat - Security News (trendmicro.com)

3.- Cazando PsExec: Un caso práctico

3.1.- Entender qué es PsExec

- **Slide 29.**
  - PsExec v2.43: PsExec - Sysinternals | Microsoft Learn
  - Server Message Block: Server Message Block - Wikipedia
  - The Classic: What is PsExec?: Threat hunting for PsExec and other lateral movement tools (redcanary.com)
  - What Is PsExec and How to Protect Against Lateral Movement: How to Detect PsExec Misuse with ExtraHop
  - Threat Hunting for PsExec, Open-Source Clones, and Other Lateral Movement Tools: Threat hunting for PsExec and other lateral movement tools (redcanary.com)
  - Hunting for PsExec artifacts in your enterprise: Hunting for PsExec artifacts in your enterprise (logpoint.com)
  - Windows Lateral Movement with smb, psexec and alternatives: Windows Lateral Movement with smb, psexec and alternatives | nv2lt - Scratching the Surface
  - Introducing PsExec for Python: Introducing PsExec for Python – Blogging for Logging
  - PsExec Demystified: PSExec Demystified | Rapid7 Blog (archive.org)
- **Slide 30.**
  - ATTC&CK Navigator: ATT&CK® Navigator (mitre-attack.github.io)
- **Slide 31.**
  - Administrative share: Administrative share - Wikipedia
  - Service Control Manager: Service control manager - Win32 apps | Microsoft Learn
  - Remote procedure call (RPC): Remote procedure call (RPC) - Win32 apps | Microsoft Learn

3.2.- CTI aplicada a PsExec

- **Slide 35.**
  - PsExec. Techniques Used. ATT&CK: PsExec, Software S0029 | MITRE ATT&CK®
  - Navigator ATT&CK. PsExec: ATT&CK® Navigator (mitre-attack.github.io)
- **Slide 36.**
  - Groups That Use This Software. ATT&CK: PsExec, Software S0029 | MITRE ATT&CK®
  - Campaigns. ATT&CK: PsExec, Software S0029 | MITRE ATT&CK®
- **Slide 37.**
  - Lateral Movement. Mitre ATT&CK: Lateral Movement, Tactic TA0008 - Enterprise | MITRE ATT&CK®
  - Understanding the cyber kill chain: The threat landscape | Microsoft Press Store

3.3.- Detección de uso de PsExec

- **Slide 44.**
  - Security Auditing: Security auditing - Windows Security | Microsoft Learn
  - Sysmon v15.14: Sysmon - Sysinternals | Microsoft Learn
- **Slide 45.**
  - Use Windows Event Forwarding to help with intrusion detection: Use Windows Event Forwarding to help with intrusion detection - Windows Security | Microsoft Learn
  - Windows Event Log: Windows Event Log - Win32 apps | Microsoft Learn
  - Appendix L: Events to Monitor: Appendix L - Events to Monitor | Microsoft Learn
  - Security auditing: Security auditing - Windows Security | Microsoft Learn
  - Windows Security Log Events: Randy's Windows Security Log Encyclopedia (ultimatewindowssecurity.com)
  - Windows Security Log Event ID 4624: Windows Security Log Event ID 4624 - An account was successfully logged on (ultimatewindowssecurity.com)
  - 4624(S): An account was successfully logged on.: 4624(S) An account was successfully logged on. - Windows Security | Microsoft Learn
- **Slide 46.**
  - 4688(S): se ha creado un nuevo proceso.: 4688(S) Se ha creado un nuevo proceso. (Windows 10) - Windows security | Microsoft Learn
- **Slide 47.**
  - SwiftOnSecurity/sysmon-config: sysmon-config/sysmonconfig-export.xml at master · SwiftOnSecurity/sysmon-config · GitHub
- **Slide 48.**
  - Id. de evento 1: Creación del proceso: Sysmon - Sysinternals | Microsoft Learn
  - Procesos y subprocesos: Procesos y subprocesos - Win32 apps | Microsoft Learn
  - Processes, Threads, and Jobs in the Windows Operating System: Processes, Threads, and Jobs in the Windows Operating System | Microsoft Press Store
- **Slide 50.**
  - Create processes: Create processes - Win32 apps | Microsoft Learn
  - CreateProcessA function (processthreadsapi.h): CreateProcessA function (processthreadsapi.h) - Win32 apps | Microsoft Learn
  - Sysmon Event ID 1: Sysmon Event ID 1 - Process creation (ultimatewindowssecurity.com)
  - SYSMON Playbook – Event ID 1: SYSMON Playbook - Event ID 1 - Relative Security
  - Understanding Sysmon Events using SysmonSimulator: Understanding Sysmon Events using SysmonSimulator | RootDSE
- **Slide 51.**
  - Defense Evasion. ATT&CK: Defense Evasion, Tactic TA0005 - Enterprise | MITRE ATT&CK®
- **Slide 52.**
  - PsExec. STRONTIC: PsExec.exe | Execute processes remotely | STRONTIC

- **Slide 57.**
  - SIGMA: GitHub - SigmaHQ/sigma: Main Sigma Rule Repository
  - Rule Creation Guide: Rule Creation Guide · SigmaHQ/sigma Wiki · GitHub
  - How to Write Sigma Rules: How to Write Sigma Rules - Nextron Systems (nextron-systems.com)
  - SIGMA. Rules: sigma/rules at master · SigmaHQ/sigma · GitHub
  - SIGMA Detection Format: Sigma - SIEM Detection Format | The shareable detection format for security professionals. (sigmahq.io)
  - Getting Started: Getting Started | Sigma Website (sigmahq.io)
  - sigconverter.io: sigconverter.io - sigma rule converter
- **Slide 59.**
  - SPL: Splexicon:SPL - Splunk Documentation
  - Welcome to BOTS: Splunk Boss of the SOC
- **Slide 61.**
  - Red Team: Red Team - Glossary | CSRC (nist.gov)
- **Slide 62.**
  - Atomic Test #2 - Use PsExec to execute a command on a remote host: atomic-red-team/atomics/T1569.002/T1569.002.md at master · redcanaryco/atomic-red-team · GitHub
  - Atomic Test #3 - Copy and Execute File with PsExec: atomic-red-team/atomics/T1021.002/T1021.002.md at master · redcanaryco/atomic-red-team · GitHub
  - Atomics. Atomic Red Team: Atomics - Explore Atomic Red Team
  - Atomic Red Team: Learn More - Explore Atomic Red Team
- **Slide 65.**
  - SOAR: Security orchestration - Wikipedia
- **Slide 66.**
  - ¿Qué es la tecnología del engaño?: ¿Qué es la tecnología de engaño? Importancia y ventajas | Zscaler
- **Slide 68.**
  - Resource Hacker™: Resource Hacker (angusj.com)
- **Slide 70.**
  - Cybersecurity Framework CSF. NIST: Cybersecurity Framework | CSRC (nist.gov)
  - Software Restriction Policies: Software Restriction Policies | Microsoft Learn
  - AppLocker: AppLocker - Windows Security | Microsoft Learn
  - User Account Control settings and configuration: User Account Control settings and configuration - Windows Security | Microsoft Learn
  - Privileged Access Management for Active Directory Domain Services: Privileged Access Management for Active Directory Domain Services | Microsoft Learn
- **Slide 71.**
  - Intrusion detection system: Intrusion detection system - Wikipedia
  - Endpoint detection and response: Endpoint detection and response - Wikipedia

EJERCICIO 1

ENUNCIADO: Buscar actores que hagan uso de **PsExec** o alguna de sus variantes y documentar la forma en que usan esta herramienta (los llamados *procedure*).

OBJETIVO DEL EJERCICIO: Este ejercicio está pensado para analizar y entender qué podemos detectar a través de la metodología **OSINT**, qué medidas de protección podemos implementar en nuestras empresas, …

Ejemplo de fuentes a consultar:

- Windows Threat Hunting: Processes of Interest (Part 2) | by Pratinav Chandra | InfoSec Write-ups (infosecwriteups.com)
- En este documento podemos ver varias capturas de pantalla con los eventos de detección: 48498 (exploit-db.com)

TIP. Usabilidad vs Seguridad → Usar un nombre personalizado para el uso de las herramientas (ejecutable, nombre del servicio, …) de **PsExec** dentro de la organización y de este modo, filtrar su uso dentro del **SIEM**. También podríamos hacer que se usan desde una cuenta determinada, …

Ejemplo: `PsExec.exe \\$Computer -r TrustedAdmin cmd.exe`

Fuente: PsExec. I thought we were friends - In.security

EJERCICIO 2

ENUNCIADO: Crear una alerta correlada (*o una simple consulta*) que detecte la creación del servicio y la operación u acción sobre un objeto con privilegios (4674 [1] [2]).

PISTAS:

- Evento 7045 – Nuevo servicio. Filtros
- Detectar que el proceso o ImagePath contenga la extensión EXE
- ServiceName sea *InstalledService*.
- Evento 4674 en que se busca la eliminación del servicio.
- El campo AccessMask con valor "%%1537" indicando la acción de borrado.
  Extraido de: What the Heck PsExec! - In.security

PREGUNTA: ¿qué ventajas o desventajas encuentras en esta consulta?

EJERCICIO 3

ENUNCIADO: Crea una alerta que detecte la ejecución de la herramienta PsExec (que esté renombrada).

PISTA:

- ¿Qué campo es más probable que no pueda ser modificado dentro de los que encontramos en el evento de **Sysmon 1**?

FUENTES:

- Detect Renamed PsExec - Splunk Security Content
- Suspicious Process Execution via Renamed PsExec Executable | Elastic Security Solution [8.12] | Elastic

Los eventos 7036 también pueden ser usados para detectar el servicio de **PsExec**.

- *Event ID 7036: The PSEXESVC service entered the running state.*
- *Event ID 7036:The PSEXESVC service entered the stopped state.*

EJERCICIO 4

ENUNCIADO: Un posible indicativo de compromiso es cuando en un período corto de tiempo se detecta la **creación, ejecución, parada y eliminación de un servicio remoto**.

Realiza una consulta que detecte este comportamiento.

FUENTE: Endpoint Detection of Remote Service Creation and PsExec - F-Secure Blog

Campos destacados del evento 5145 [3] [4]:

- Share folder es IPC$
- El servicio es PSEXECSVC-*
- También se debe mirar accesos a ADMIN$ donde se copia herramientas/archivos.

EJERCICIO 5

ENUNCIADO: ¿Cómo sería el código del movimiento lateral usando **PsExec** y realizando un **Pass-the-Hash (*PtH*)**?

FUENTES:

- Threat Hunting · GitHub
- Defeating pass-the-hash attacks with two-factor authentication

Más info sobre *Lateral Movement*:

- Lateral Movement. Red Team Cheat Sheet.
- Find_Evil - Threat Hunting | SANS@MIC Talk
- Find Evil Threat Hunting Lateral Movement
- Cómo detectar PtH

Laboratorio: PsExec Hunt Blue Team Lab → Ejemplo de laboratorio de **BlueTeam** y **PsExec**.

PRACTICA FINAL

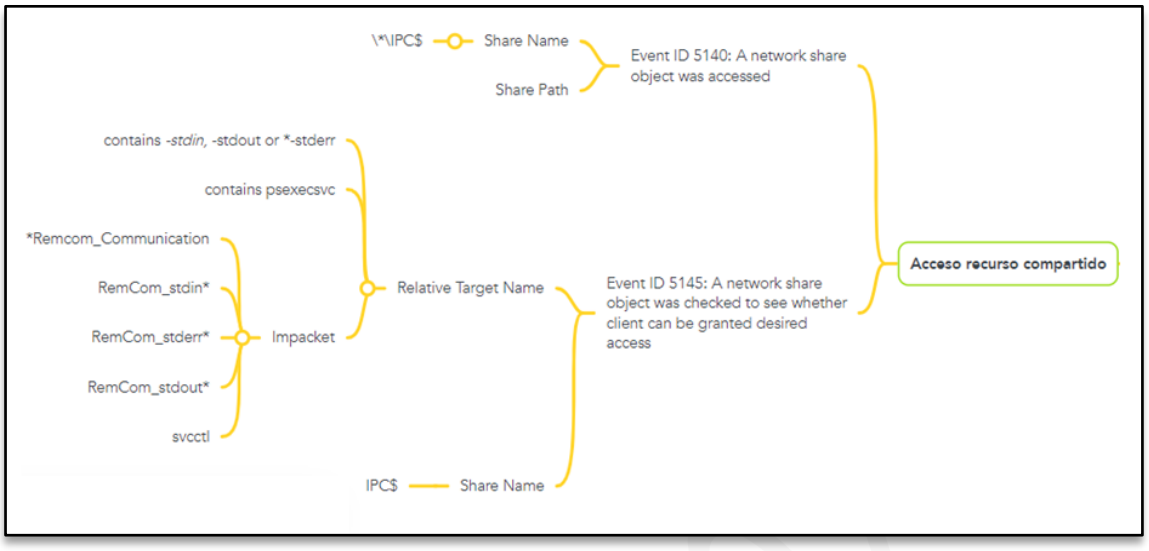

Ilustración 1 Posibles métodos detección Acceso a recursos compartidos

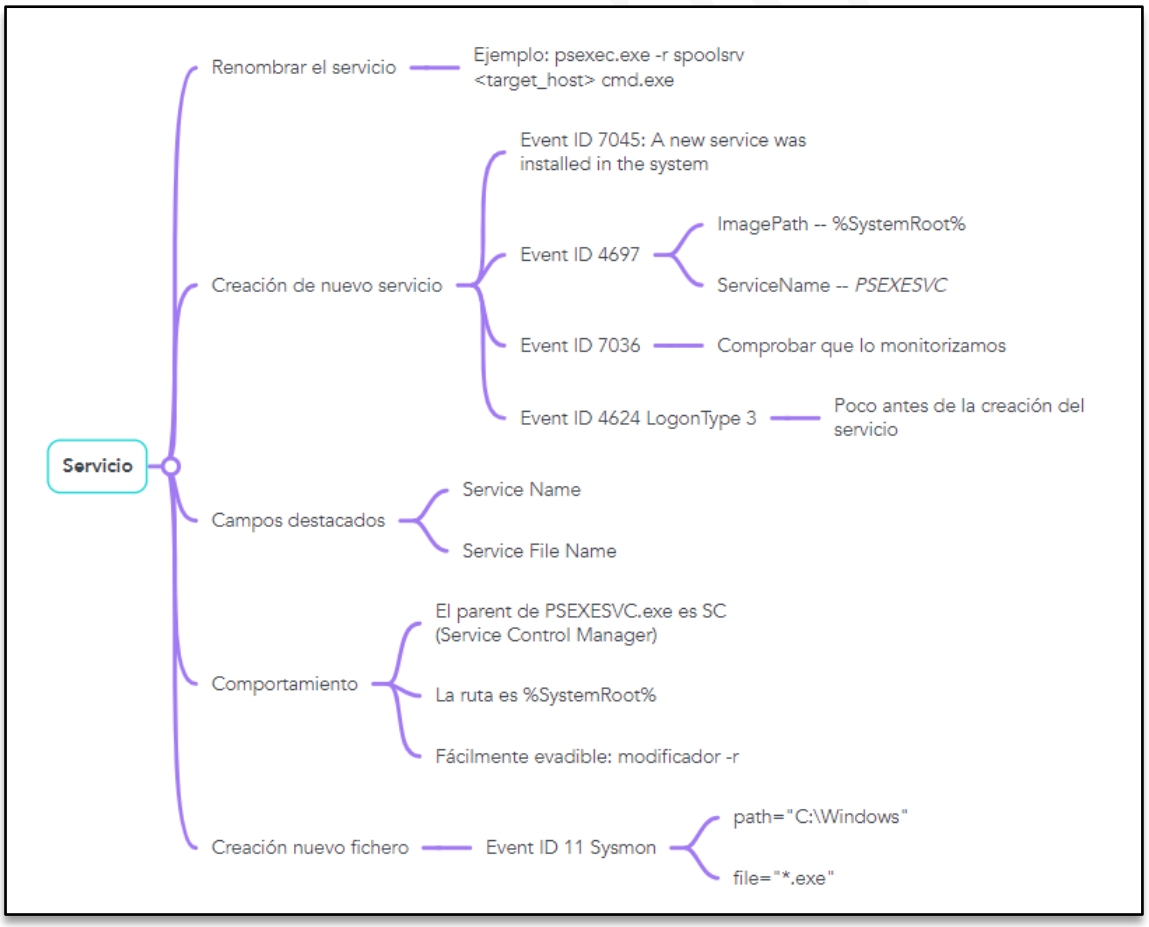

Ilustración 2 Posibles métodos de detección entre PsExec y los Servicios

¿Qué vamos a hacer?

- Vamos a **elegir una** de las dos opciones propuestas en la página anterior.
- Lo primero que tenemos que hacer es **entender cómo funciona lo que queremos detectar**. *Busca información sobre cómo funciona **PsExec**.*
- *¿Qué **evento o eventos** vamos a usar para **detectar** este **comportamiento**?*
- *¿Sobre qué **máquina** o **máquinas realizaríamos el Hunt**?* En estos dos últimos eventos, debemos asegurarnos de que estamos recibiendo los eventos que queremos usar. *¿Cómo haríamos esto?*
- Debemos **crear la consulta** que utilizaremos. Para ello realizaremos lo siguiente:
    - Crearemos la consulta en un *pseudocódigo*.
    - Posteriormente, crearemos la *regla* dentro de ***SIGMA***.
    - Finalmente, crearemos la *consulta* dentro del lenguaje ***SIEM*** que queramos.
    - En caso de que **detectásemos** algo **sospechoso**, *¿qué haríamos?*
    - Se nos indica que debemos crear una regla **SIEM** del hunt realizado. *¿Qué tendríamos que considerar a la hora de crearla para que sea lo **más eficiente posible**? ¿Qué **metadatos** debería tener?*
    - Si estuvieras en el lado del atacante, ¿**cómo evadirías esta detección**? En caso de indicar un método válido, *¿cómo cambiarias tu **consulta para detectar** este nuevo escenario?*
    - *¿Qué **recomendaciones** a nivel de **protección** realizarías a tu organización?*

OPCIONAL: Crea un **Playbook** tanto para el **análisis de la alerta** (destinado a los analistas del **SOC**), como de **respuesta ante incidentes**, intentando realizar en ambos casos, **procesos de automatización**. Se deben poseer conocimientos de automatización en SOAR/EDR, … para poder realizar esta última parte de este enunciado.


HackOn
2024