Programación para Ciberseguridad

Evidencia 7

Automatización de tareas forenses con PowerShell en Windows

Nombre: Manuel de Jesús Puente Martínez

Matricula: 1895776

Nombre: Rogelio de Llano Salazar

Matricula: 2067433

Docente: Osvaldo Habib Gonzales Gonzales

Grupo: 061

Introducción

La automatización de tareas forenses en sistemas Windows representa una herramienta fundamental para los analistas de ciberseguridad. Mediante scripts y módulos en PowerShell, es posible recopilar evidencias, detectar comportamientos sospechosos y correlacionar eventos de manera eficiente. El **Script principal** integra cinco funciones que permiten identificar actividades anómalas, examinar procesos en ejecución y revisar conexiones de red, consolidando así un marco práctico de análisis forense.

1. Función Get-SuspiciousEvents

Su propósito es extraer eventos sospechosos del **Visor de eventos de Windows** y guardarlos en un archivo CSV.

Parámetros

- **MaxEvents**: número máximo de eventos a analizar.
- **OutputPath**: ruta del archivo CSV para guardar los resultados.
- **DontSaveReport**: muestra los resultados en consola sin guardarlos en archivo.

Comandos utilizados

- **Get-WinEvent**: obtiene registros de eventos de Windows.
- **Where-Object**: filtra eventos con IDs sospechosos (ej. 4625 = inicio de sesión fallido, 6008 = apagado inesperado), niveles críticos (*Error*, *Warning*, *Critical*) y palabras clave como *malware* o *attack*.
- **Select-Object**: organiza los resultados con campos relevantes.
- **Export-Csv**: exporta los datos para análisis externo.
- **Write-Warning**: muestra advertencias si no se puede acceder a los registros.

Funcionamiento

Recorre los logs de *System*, *Application* y *Security*, filtra los eventos relevantes y genera un informe que facilita la detección de incidentes.

2. Función Get-InternetProcesses

Busca correlacionar procesos en ejecución con **conexiones TCP activas**.

Parámetro

- **DontSaveReport**: evita guardar en archivo.

Comandos utilizados

- **Get-NetTCPConnection**: obtiene todas las conexiones de red.
- **Where-Object State -eq 'Established'**: filtra las que están activas.
- **Get-Process -Id**: obtiene el proceso dueño de la conexión.
- **Select-Object**: estructura la información (proceso, PID, IP local/remota, puertos).
- **Export-Csv**: exporta el reporte en CSV.

Funcionamiento

Permite identificar qué aplicaciones están comunicándose con redes externas, lo cual ayuda a detectar software sospechoso.

3. Función Get-UnsignedProcesses

Analiza procesos activos y detecta cuáles **no tienen firma digital**, lo cual puede ser indicio de software malicioso.

Comandos utilizados

- **Get-Process**: lista todos los procesos en ejecución.
- **Get-AuthenticodeSignature**: revisa la firma digital de cada ejecutable.
- **Where-Object Status -ne 'Valid'**: filtra los procesos con firma inválida o inexistente.
- **Select-Object**: organiza información clave (nombre del proceso, ruta del archivo, estado de la firma).
- **Export-Csv**: exporta los resultados.

Funcionamiento

Verifica la legitimidad de los procesos en ejecución. Un proceso sin firma digital válida puede ser sospechoso y requiere mayor análisis.

4. Función Get-SuspiciousInternetProcesses

Combina la lógica de **conexiones de red** con la verificación de **firmas digitales**.

Comandos utilizados

- **Get-NetTCPConnection** + **Get-Process**: obtiene procesos con conexiones activas.
- **Get-AuthenticodeSignature**: revisa la validez de la firma de dichos procesos.
- **Where-Object Status -ne 'Valid'**: filtra solo los que no tienen firma confiable.
- **Export-Csv**: guarda la información.

Funcionamiento

Permite identificar procesos que, además de tener comunicación externa, no cuentan con firma digital válida. Esto los convierte en candidatos prioritarios a revisar, ya que pueden ser malware en ejecución.

5. Función Get-FullForensicAnalysis

Es una función integradora que ejecuta las cuatro funciones anteriores en conjunto.

Comandos utilizados

- Llama internamente a:
  - **Get-SuspiciousEvents**
  - **Get-InternetProcesses**
  - **Get-UnsignedProcesses**
  - **Get-SuspiciousInternetProcesses**

Funcionamiento

Genera un análisis forense completo en una sola ejecución, entregando reportes detallados de eventos sospechosos, procesos en red, procesos sin firma y procesos de red sin firma digital. Con esto, el analista obtiene un panorama integral del estado de seguridad del sistema.

Estos serían unos ejemplos de lo que te mostraría cada función:

1. Función Get-SuspiciousEvents

LogName	TimeCreated	Id	LevelDisplayName	Message
System	10/09/2025 19:03	1796	Error	La actualización de arranque seguro no pudo actualizar una variable de arranque seguro con el error Unknown HResult Error code: 0x800700c1. Para obtener más información, consulte https://go.microsoft.com/fwlink/?linkid=2169931
System	10/09/2025 19:03	10317	Error	Minipuerto Microsoft Wi-Fi Direct Virtual Adapter #2, {ef60c33c-1c07-43ff-b5d6-1ad56cdcb3a5}, tuvo el evento Fatal error: The miniport has failed a power transition to operational power
System	08/09/2025 17:57	20	Error	Error de instalación: error de Windows al instalar la siguiente actualización, error 0x80073D02: 9NHT9RB2F4HD-Microsoft.Copilot.
System	08/09/2025 17:56	20	Error	Error de instalación: error de Windows al instalar la siguiente actualización, error 0x80073D02: 9N3RK8ZV2ZR8-Microsoft.WidgetsPlatformRuntime.
System	08/09/2025 17:26	1796	Error	La actualización de arranque seguro no pudo actualizar una variable de arranque seguro con el error Unknown HResult Error code: 0x800700c1. Para obtener más información, consulte https://go.microsoft.com/fwlink/?linkid=2169931
System	08/09/2025 17:26	10317	Error	Minipuerto Microsoft Wi-Fi Direct Virtual Adapter #2, {ef60c33c-1c07-43ff-b5d6-1ad56cdcb3a5}, tuvo el evento Fatal error: The miniport has failed a power transition to operational power
System	05/09/2025 09:56	1796	Error	La actualización de arranque seguro no pudo actualizar una variable de arranque seguro con el error Unknown HResult Error code: 0x800700c1. Para obtener más información, consulte https://go.microsoft.com/fwlink/?linkid=2169931
System	05/09/2025 09:16	10317	Error	Minipuerto Microsoft Wi-Fi Direct Virtual Adapter #2, {ef60c33c-1c07-43ff-b5d6-1ad56cdcb3a5}, tuvo el evento Fatal error: The miniport has failed a power transition to operational power
System	05/09/2025 08:36	1796	Error	La actualización de arranque seguro no pudo actualizar una variable de arranque seguro con el error Unknown HResult Error code: 0x800700c1. Para obtener más información, consulte https://go.microsoft.com/fwlink/?linkid=2169931
System	05/09/2025 08:36	10317	Error	Minipuerto Microsoft Wi-Fi Direct Virtual Adapter #2, {ef60c33c-1c07-43ff-b5d6-1ad56cdcb3a5}, tuvo el evento Fatal error: The miniport has failed a power transition to operational power
System	04/09/2025 19:56	10317	Error	Minipuerto Microsoft Wi-Fi Direct Virtual Adapter #2, {ef60c33c-1c07-43ff-b5d6-1ad56cdcb3a5}, tuvo el evento Fatal error: The miniport has failed a power transition to operational power
System	04/09/2025 10:08	10317	Error	Minipuerto Microsoft Wi-Fi Direct Virtual Adapter #2, {ef60c33c-1c07-43ff-b5d6-1ad56cdcb3a5}, tuvo el evento Fatal error: The miniport has failed a power transition to operational power
System	04/09/2025 09:56	1796	Error	La actualización de arranque seguro no pudo actualizar una variable de arranque seguro con el error Unknown HResult Error code: 0x800700c1. Para obtener más información, consulte https://go.microsoft.com/fwlink/?linkid=2169931
System	04/09/2025 09:13	1796	Error	La actualización de arranque seguro no pudo actualizar una variable de arranque seguro con el error Unknown HResult Error code: 0x800700c1. Para obtener más información, consulte https://go.microsoft.com/fwlink/?linkid=2169931
System	04/09/2025 09:13	10317	Error	Minipuerto Microsoft Wi-Fi Direct Virtual Adapter #2, {ef60c33c-1c07-43ff-b5d6-1ad56cdcb3a5}, tuvo el evento Fatal error: The miniport has failed a power transition to operational power
System	02/09/2025 18:43	1796	Error	La actualización de arranque seguro no pudo actualizar una variable de arranque seguro con el error Unknown HResult Error code: 0x800700c1. Para obtener más información, consulte https://go.microsoft.com/fwlink/?linkid=2169931
System	02/09/2025 18:43	10317	Error	Minipuerto Microsoft Wi-Fi Direct Virtual Adapter #2, {ef60c33c-1c07-43ff-b5d6-1ad56cdcb3a5}, tuvo el evento Fatal error: The miniport has failed a power transition to operational power
System	01/09/2025 19:46	1796	Error	La actualización de arranque seguro no pudo actualizar una variable de arranque seguro con el error Unknown HResult Error code: 0x800700c1. Para obtener más información, consulte https://go.microsoft.com/fwlink/?linkid=2169931
System	01/09/2025 19:46	10317	Error	Minipuerto Microsoft Wi-Fi Direct Virtual Adapter #2, {ef60c33c-1c07-43ff-b5d6-1ad56cdcb3a5}, tuvo el evento Fatal error: The miniport has failed a power transition to operational power
System	29/08/2025 18:25	1796	Error	La actualización de arranque seguro no pudo actualizar una variable de arranque seguro con el error Unknown HResult Error code: 0x800700c1. Para obtener más información, consulte https://go.microsoft.com/fwlink/?linkid=2169931
System	27/08/2025 21:51	22	Error	El servicio de inicio de sesión de eventos detectó un error al inicializar recursos de publicación para el canal Microsoft-Windows-USBVideo/Analytic. Si el tipo de canal es Analítico o Depurador, podría indicar también un error de inicialización de recursos de registro.
System	27/08/2025 21:50	10010	Error	El servidor {B91D5831-B1BD-4608-8198-D72E155020F7} no se registró con DCOM dentro del tiempo de espera requerido.
System	27/08/2025 21:49	7023	Error	El servicio Servicio orquestador de actualizaciones se cerró con el siguiente error: %%2149884192
System	27/08/2025 21:48	7023	Error	El servicio Servicio orquestador de actualizaciones se cerró con el siguiente error: %%2149884192
System	27/08/2025 21:47	22	Error	El servicio de inicio de sesión de eventos detectó un error al inicializar recursos de publicación para el canal Microsoft-Windows-USBVideo/Analytic. Si el tipo de canal es Analítico o Depurador, podría indicar también un error de inicialización de recursos de registro.
System	27/08/2025 20:22	10010	Error	El servidor {BCFC164F-4BE5-4FDD-94E9-E2AF73ED4A19} no se registró con DCOM dentro del tiempo de espera requerido.
System	27/08/2025 19:29	20	Error	Error de instalación: error de Windows al instalar la siguiente actualización, error 0x80073D02: 9MSSGKG348SP-MicrosoftWindows.Client.WebExperience.
System	27/08/2025 19:29	20	Error	Error de instalación: error de Windows al instalar la siguiente actualización, error 0x80073D02: 9NMPJ99VJBWV-Microsoft.YourPhone.
System	27/08/2025 19:28	20	Error	Error de instalación: error de Windows al instalar la siguiente actualización, error 0x80073D02: 9WZDNCRFJBMP-MICROSOFT.WINDOWSSTORE.
Application	10/09/2025 19:55	1022	Error	.NET Runtime version 4.0.30319.0 - Error al inicializar la infraestructura de asociación de la API de generación de perfiles. Este proceso no permitirá que se asocie un generador de perfiles. HRESULT: 0x80004005. Id. de proceso (decimal): 13780. Id. de mensaje: [0x2509].
Application	10/09/2025 19:43	1022	Error	.NET Runtime version 4.0.30319.0 - Error al inicializar la infraestructura de asociación de la API de generación de perfiles. Este proceso no permitirá que se asocie un generador de perfiles. HRESULT: 0x80004005. Id. de proceso (decimal): 17884. Id. de mensaje: [0x2509].
Application	10/09/2025 19:38	1022	Error	.NET Runtime version 4.0.30319.0 - Error al inicializar la infraestructura de asociación de la API de generación de perfiles. Este proceso no permitirá que se asocie un generador de perfiles. HRESULT: 0x80004005. Id. de proceso (decimal): 16760. Id. de mensaje: [0x2509].
Application	10/09/2025 19:34	1022	Error	.NET Runtime version 4.0.30319.0 - Error al inicializar la infraestructura de asociación de la API de generación de perfiles. Este proceso no permitirá que se asocie un generador de perfiles. HRESULT: 0x80004005. Id. de proceso (decimal): 22948. Id. de mensaje: [0x2509].
Application	10/09/2025 19:16	1022	Error	.NET Runtime version 4.0.30319.0 - Error al inicializar la infraestructura de asociación de la API de generación de perfiles. Este proceso no permitirá que se asocie un generador de perfiles. HRESULT: 0x80004005. Id. de proceso (decimal): 12676. Id. de mensaje: [0x2509].
Application	10/09/2025 19:12	1022	Error	.NET Runtime version 4.0.30319.0 - Error al inicializar la infraestructura de asociación de la API de generación de perfiles. Este proceso no permitirá que se asocie un generador de perfiles. HRESULT: 0x80004005. Id. de proceso (decimal): 13460. Id. de mensaje: [0x2509].
Application	10/09/2025 19:03	1022	Error	.NET Runtime version 4.0.30319.0 - Error al inicializar la infraestructura de asociación de la API de generación de perfiles. Este proceso no permitirá que se asocie un generador de perfiles. HRESULT: 0x80004005. Id. de proceso (decimal): 2388. Id. de mensaje: [0x2509].
Application	08/09/2025 19:25	1022	Error	.NET Runtime version 4.0.30319.0 - Error al inicializar la infraestructura de asociación de la API de generación de perfiles. Este proceso no permitirá que se asocie un generador de perfiles. HRESULT: 0x80004005. Id. de proceso (decimal): 4236. Id. de mensaje: [0x2509].
Application	08/09/2025 18:36	1022	Error	.NET Runtime version 4.0.30319.0 - Error al inicializar la infraestructura de asociación de la API de generación de perfiles. Este proceso no permitirá que se asocie un generador de perfiles. HRESULT: 0x80004005. Id. de proceso (decimal): 10068. Id. de mensaje: [0x2509].

2. Función Get-InternetProcesses

ProcessName	PID	LocalAddress	LocalPort	RemoteAddre	RemotePort	State
mc-fw-host	5852	2806:2f0:40a	58759	2806:2f0:429	443	Established
servicehost	5892	2806:2f0:40a	58758	2806:2f0:429	443	Established
WINWORD	14932	2806:2f0:40a	58757	2603:1036:24	443	Established
msedge	11560	2806:2f0:40a	58752	2620:1ec:33:	443	Established
WINWORD	14932	2806:2f0:40a	58751	2603:1036:24	443	Established
WINWORD	14932	2806:2f0:40a	58750	2603:1036:24	443	Established
msedge	11560	2806:2f0:40a	58748	2620:1ec:33:	443	Established
explorer	23424	2806:2f0:40a	58705	2603:1036:31	443	Established
explorer	23424	2806:2f0:40a	58703	2603:1036:31	443	Established
WINWORD	14932	2806:2f0:40a	58680	2603:1036:24	443	Established
svchost	6140	2806:2f0:40a	58669	2603:1030:40	443	Established
msedge	11560	2806:2f0:40a	58667	2a06:98c1:31	443	Established
msedgewebvi	23128	2806:2f0:40a	58656	2603:1063:16	443	Established
WINWORD	14932	2806:2f0:40a	58646	2603:1063:22	443	Established
ms-teams	20084	2806:2f0:40a	58631	2603:1063:33	443	Established
ms-teams	20084	2806:2f0:40a	58620	2603:1063:16	443	Established
WINWORD	14932	192.168.100.	58760	13.107.42.12	443	Established
msedge	11560	192.168.100.	58755	20.42.65.94	443	Established
WINWORD	14932	192.168.100.	58753	13.107.42.12	443	Established
svchost	18720	192.168.100.	58745	173.46.81.20	80	Established
mc-fw-host	5852	192.168.100.	58742	52.24.70.109	443	Established
mc-fw-host	5852	192.168.100.	58741	186.96.40.9	443	Established
OneDrive	13200	192.168.100.	58740	13.89.179.8	443	Established
OneDrive	13200	192.168.100.	58737	52.104.80.25	443	Established
svchost	18720	192.168.100.	58729	173.46.81.20	80	Established
hp-one-agent	4512	192.168.100.	58696	52.2.61.126	443	Established
msedge	11560	192.168.100.	58676	20.169.174.2	443	Established
OneDrive	13200	192.168.100.	58623	104.208.203.	443	Established
NVDisplay.Cc	3816	127.0.0.1	49708	127.0.0.1	49707	Established
NVDisplay.Cc	3816	127.0.0.1	49707	127.0.0.1	49708	Established
WUDFHost	1820	127.0.0.1	49705	127.0.0.1	49704	Established
WUDFHost	1820	127.0.0.1	49704	127.0.0.1	49705	Established

3. Función Get-UnsignedProcesses

	A	B	C	D	E	F
1	Timestamp	ProcessName	PID	RemoteAddre	AbuseConfide	TotalReports
2	2025-09-10T2	OneDriveStan	16628	20.189.173.1(	20	4
3	2025-09-10T2	OneDrive	13200	13.89.179.8	20	3

5. Función Get-FullForensicAnalysis

	A	B	C	D	E
1	ProcessName	PID	HasInternet	Unsigned	SuspiciousIP
2	explorer	23424	True	False	False
3	msedge	11560	True	False	False
4	msedgewebvi	23128	True	False	False
5	ms-teams	20084	True	False	False
6	NVDisplay.Co	3816	True	False	False
7	OneDrive	13200	True	False	False
8	svchost	6140	True	False	False
9	WINWORD	14932	True	False	False
10	WUDFHost	1820	True	False	False