Seguridad informática con PowerShell

Introducción

Confidencialidad

[crayon-6a9d4f52bbb1c516229079/]

Integridad

[crayon-6a9d4f52bbb22356516378/]

Seguridad física

Analizar el hardware de los equipos de la empresa

[crayon-6a9d4f52bbb25935117662/]

Ver dispositivos conectados (móviles, almacenamiento USB, etc.)

[crayon-6a9d4f52bbb26228225563/]

Seguridad lógica

Usuarios

Ver información sobre usuarios y grupos (usuario que ha iniciado sesión)

[crayon-6a9d4f52bbb28182922730/]

Crear usuarios y grupos (procedimiento de creación)

[crayon-6a9d4f52bbb2a788626921/]

Software

Analizar el software de los equipos de la empresa

[crayon-6a9d4f52bbb2b418390195/]

Actualizaciones

Ver las actualizaciones instaladas en el sistema

[crayon-6a9d4f52bbb2d319533681/]

Procesos

Procesos que se están ejecutando

[crayon-6a9d4f52bbb2e097442772/]

Ruta de ejecución de los procesos

[crayon-6a9d4f52bbb30912958452/]

Procesos y usuarios

[crayon-6a9d4f52bbb32088210760/]

Procesos y conexiones de red (UDP)

[crayon-6a9d4f52bbb33141985569/]

Procesos y conexiones de red (TCP)

[crayon-6a9d4f52bbb35882836401/]

Servicios

- https://www.jesusninoc.com/11/10/analizar-servicios-con-powershell/

Analizar los programas que están instalados en los equipos de la empresa y ver la relación que tienen con los procesos y servicios

[crayon-6a9d4f52bbb36214652386/]

Analizar los programas que están instalados en los equipos de la empresa y ver la relación que tienen con los procesos y servicios (también se pueden analizar hilos)

[crayon-6a9d4f52bbb38231192075/]

Servicios y conexiones de red (UDP)

[crayon-6a9d4f52bbb39638411294/]

Servicios y conexiones de red (TCP)

[crayon-6a9d4f52bbb3f957848353/]

Antivirus

Analizar

[crayon-6a9d4f52bbb43059470615/]

Definiciones

[crayon-6a9d4f52bbb44598403894/]

Copias de seguridad

Realizar y restaurar copias de seguridad

[crayon-6a9d4f52bbb46212806108/]

Red

Escanear equipos

[crayon-6a9d4f52bbb47138996077/]

Monitorizar

- https://www.jesusninoc.com/05/01/analisis-de-conexiones-de-red/
- https://www.jesusninoc.com/2015/11/13/cmdlets-for-tcpip-model-layers/

[crayon-6a9d4f52bbb49975373014/]

Wifi

- https://www.jesusninoc.com/10/14/ejecutar-airodump-ng-en-linux-realizando-una-conexion-ssh-desde-powershell-en-windows/

Canales encubiertos

- https://www.jesusninoc.com/03/11/enviar-datos-a-un-formulario-de-google-docs-desde-powershell/

Logs

[crayon-6a9d4f52bbb4a187691391/]

Ofuscación

- https://www.jesusninoc.com/12/01/ofuscacion-en-powershell/

Memoria

- https://www.jesusninoc.com/02/16/cargar-en-memoria-y-ejecutar-un-payload-de-ejecucion-de-comandos-arbitrarios-en-powershell/
- https://www.jesusninoc.com/03/20/analizar-con-cheat-engine-un-payload-de-ejecucion-de-comandos-arbitrarios-para-ejecutar-powershell/

Criptografía

- https://www.jesusninoc.com/02/01/criptografia-en-powershell/

Cifrar y descifrar

Cifrar

[crayon-6a9d4f52bbb4e124743669/]

Descifrar

[crayon-6a9d4f52bbb50091345726/]

Forense

Analizar sistema de archivos (rutas, fechas, etc.)

[crayon-6a9d4f52bbb51990955279/]

Artefactos

[crayon-6a9d4f52bbb55151231430/]

Crear un fichero de volcado de memoria de un proceso

[crayon-6a9d4f52bbb57267216723/]

Pentesting

Fuerza bruta

[crayon-6a9d4f52bbb58435049876/]

Post exploitation

- https://www.jesusninoc.com/10/09/windows-post-exploitation-cmdlets-execution-powershell/