Investigación

21 herramientas de SysInternals (7 días de clases)

1. AccessChk: Permite saber qué tipo de acceso tienen los usuarios o grupos específicos a los recursos, incluidos archivos, directorios, claves de registro, objetos globales y servicios de Windows.
   Uso: *accesschk [-s] [- e] [- u] [- r] [- w] [- n] [- v] - [f <account>, ...] [[- a] | [- k] | [-p [-f] [-t]] | [-h] [- o [-t <tipo de objeto>]] [- c] | [-d]] [[-l [-i]] | [nombre de usuario]] <archivo, directorio, clave de registro, proceso, servicio, objeto>*

Parámetro	Descripción
-una	El nombre es un derecho de cuenta de Windows. Especifique "*" como nombre para mostrar todos los derechos asignados a un usuario. Tenga en cuenta que cuando especifica un derecho específico, solo se muestran los grupos y cuentas asignados directamente a la derecha.
-do	El nombre es un servicio de Windows, por ejemplo, ssdpsrv. Especifique "*" como nombre para mostrar todos los servicios y "scmanager" para verificar la seguridad del Administrador de control de servicios.
-re	Sólo procesar directorios o claves de nivel superior
-mi	Mostrar solo explícitamente los niveles de integridad establecidos (solo Windows Vista y superior)
-F	Si sigue -p, muestra la información completa del token de proceso, incluidos los grupos y privilegios. De lo contrario, hay una lista de cuentas separadas por comas para filtrar desde la salida.
-h	El nombre es un archivo o una impresora compartida. Especifique '*' como nombre para mostrar todos los recursos compartidos.
-yo	Ignore los objetos que solo tengan entradas de control de acceso heredadas al descargar listas de control de acceso completo.
-k	El nombre es una clave de registro, por ejemplo, hklm \ software
-l	Mostrar descriptor de seguridad completo. Agregue -i para ignorar las ACE heredadas.
-norte	Mostrar solo objetos que no tienen acceso

Parámetro	Descripción
-o	Nombre es un objeto en el espacio de nombres del Administrador de objetos (el valor predeterminado es raíz). Para ver el contenido de un directorio, especifique el nombre con una barra diagonal inversa o agregue -s. Agregue -t y un tipo de objeto (por ejemplo, sección) para ver solo objetos de un tipo específico.
-pag	Nombre es un nombre de proceso o PID, por ejemplo, cmd.exe (especifique "*" como nombre para mostrar todos los procesos).Agregue -f para mostrar la información completa del token de proceso, incluidos los grupos y privilegios. Agregue -t para mostrar los hilos.
-q	Omitir Banner
-r	Mostrar solo objetos que tengan acceso de lectura
-s	Recuento
-t	Filtro de tipo de objeto, por ejemplo, "sección"
-u	Suprimir errores
-v	Verbose (incluye el nivel de integridad de Windows Vista)
-w	Mostrar solo objetos que tienen acceso de escritura

2. AccessEnum: Ofrece una vista completa de su sistema de archivos y la configuración de seguridad del Registro en segundos
   Funcionamiento: AccessEnum utiliza las API de seguridad estándar de Windows para completar su vista de lista con información de acceso de lectura, escritura y denegación.
3. Active Directory Explorer (AdExplorer): Es un visor y editor avanzado de Active Directory (AD). Puede usar AdExplorer para navegar fácilmente por una base de datos de AD, definir ubicaciones favoritas, ver propiedades y atributos de objetos sin tener que abrir cuadros de diálogo, editar permisos, ver el esquema de un objeto y ejecutar búsquedas sofisticadas que puede guardar y volver a ejecutar.
   AD Explorer también incluye la capacidad de guardar snapshots de una base de datos de AD para verlas y compararlas fuera de línea. Cuando carga una instantánea guardada, puede navegar y explorarla como lo haría

con una base de datos activa. Si tiene dos instantáneas de una base de datos de AD, puede usar la funcionalidad de comparación de AD Explorer para ver qué objetos, atributos y permisos de seguridad han cambiado entre ellos.

4. Contig: Es un desfragmentador de un solo archivo que intenta hacer que los archivos sean contiguos en el disco. Es perfecto para optimizar rápidamente los archivos que se fragmentan continuamente, o que desea asegurarse de que estén en el menor número de fragmentos posible.
   Uso:
   \ src \ Contig \ Release \ Contig.exe [-a] [-s] [-q] [-v] [archivo existente]

   o \ src \ Contig \ Release \ Contig.exe [-f] [-q] [-v] [unidad:]

   o \ src \ Contig \ Release \ Contig.exe [-v] [-l] -n [nuevo archivo] [longitud del nuevo archivo]

Parámetro	*Descripción*
-a	Analizar fragmentacion
-f	Analizar la fragmentación del espacio libre.
-l	Establezca la longitud de datos válida para la creación rápida de archivos (requiere derechos de administrador)
-q	Modo silencioso
-s	Subdirecciones de recurse
-v	Verboso

   Contig también puede analizar y desfragmentar los siguientes archivos de metadatos de NTFS:

   $ Mft
   $ LogFile
   $ Volumen
   $ AttrDef
   $ Bitmap
   $ Arranque
   $ BadClus
   $ Seguro
   $ Mayúsculas
   $ Extender
5. DiskView: Le muestra un mapa gráfico de su disco, lo que le permite determinar dónde se encuentra un archivo o, al hacer clic en un clúster, ver qué archivo lo ocupa. Haga doble clic para obtener más información sobre un archivo al que se asigna un clúster.

6. DiskExt: Demuestra el uso del comando **IOCTL_VOLUME_GET_VOLUME_DISK_EXTENTS** que devuelve información sobre en qué discos están ubicadas las particiones de un volumen (los discos de múltiples particiones pueden residir en varios discos) y en qué lugar del disco están ubicadas las particiones.
7. Autologon: Permite configurar fácilmente el mecanismo de inicio de sesión integrado de Windows. En lugar de esperar a que un usuario ingrese su nombre y contraseña, Windows usa las credenciales que ingresa con Autologon, que están cifradas en el Registro, para iniciar sesión automáticamente en el usuario especificado.
   Uso: *autologon usuario domain contraseña.*
8. Coreinfo: Es una utilidad de línea de comandos que muestra la asignación entre los procesadores lógicos y el procesador físico, el nodo NUMA y el socket en el que residen, así como la memoria caché asignada a cada procesador lógico. Utiliza la función **GetLogicalProcessorInformation** de Windows para obtener esta información y la imprime en la pantalla, representando una asignación a un procesador lógico con un asterisco, por ejemplo, "*". Coreinfo es útil para obtener información sobre la topología de procesador y caché de su sistema. Para cada recurso, muestra un mapa de los procesadores visibles para el SO que corresponden a los recursos especificados, con '*' representando los procesadores aplicables.
   Uso:

   coreinfo [-c] [- f] [- g] [- l] [- n] [- s] [- m] [- v]

Parámetro	*Descripción*
-c	Volcar la información en los núcleos.
-f	Volcar la información de la función principal.
-g	Volcar la información en grupos.
-l	Volcar la información en cachés.
-n	Volcar la información en los nodos NUMA.
-s	Volcar la información en los zócalos.
-m	Volcar el costo de acceso NUMA.
-v	Volcar solo las funciones relacionadas con la virtualización, incluida la compatibilidad con la traducción de direcciones de segundo nivel.

   Todas las opciones excepto -v están seleccionadas de forma predeterminada.
9. DiskMon: Es una aplicación que registra y muestra toda la actividad del disco duro en un sistema Windows. También puede minimizar DiskMon en la bandeja del sistema donde actúa como luz de disco, presentando un icono verde cuando hay actividad de lectura de disco y un icono rojo cuando hay actividad de escritura de disco.

10. DebugView: Es una aplicación que le permite controlar la salida de depuración en su sistema local o en cualquier computadora de la red a la que pueda acceder a través de TCP / IP. Es capaz de mostrar tanto la salida de depuración del modo kernel como la de Win32, por lo que no necesita un depurador para capturar la salida de depuración que generan sus aplicaciones o controladores de dispositivo, ni tampoco necesita modificar sus aplicaciones o controladores para usar una depuración no estándar APIs de salida.
11. Disk Usage: Informa el uso de espacio en disco para el directorio que especifique. Por defecto, recurre en los directorios para mostrar el tamaño total de un directorio y sus subdirectorios.
    Uso: du [-c [t]] [-l <levels> | -n | -v] [-u] [-q] <directorio>

Parámetro	Descripción
-c	Imprimir la salida como CSV. Utilice -ct para delimitar pestañas.
-l	Especifique la profundidad de la información del subdirectorio (el valor predeterminado es todos los niveles).
-n	No lo hagas.
-v	Mostrar tamaño (en KB) de directorios intermedios.
-u	Cuente cada instancia de un archivo enlazado.
-q	Tranquilo (sin banner).

    La salida CSV está formateada como:
    Ruta, CurrentFileCount, CurrentFileSize, FileCount, DirectoryCount, DirectorySize
12. NTFSInfo: Es un pequeño applet que muestra información sobre los volúmenes NTFS. Su volcado incluye el tamaño de las unidades de asignación de una unidad, donde se encuentran los archivos clave de NTFS y los tamaños de los archivos de metadatos de NTFS en el volumen, muestra dónde se encuentra la MFT en el disco (en términos de clústeres) y qué tan grande es, además de especificar qué tan grandes son los clústeres del volumen y los registros de MFT. Para proteger la MFT de la fragmentación, NTFS reserva una parte del disco alrededor de la MFT que no se asignará a otros archivos a menos que el espacio en el disco se agote. Esta área se conoce como MFT-Zone y NTFSInfo le indicará dónde se encuentra la zona MFT en el disco y qué porcentaje de la unidad está reservado para ella. Para que NTFSInfo funcione, debe tener privilegios administrativos.
    Uso: NTFSInfo x

Parámetro	Descripción
x	La letra de unidad del volumen NTFS que desea examinar.

13. EFSDump: Windows 2000 introduce el Sistema de archivos de cifrado (EFS) para que los usuarios puedan proteger sus datos confidenciales. Varias API nuevas hacen su debut para admitir este servicio, incluido one-QueryUsersOnEncryptedFile, que le permite ver quién tiene acceso a los archivos cifrados. Este applet usa la API para mostrarle qué cuentas están autorizadas para acceder a archivos encriptados.
14. FindLinks: Informa sobre el índice de archivos y los enlaces duros (rutas de archivo alternativas en el mismo volumen) que existen para el archivo especificado. Los datos de un archivo permanecen asignados siempre que tengan al menos un nombre de archivo que haga referencia a ellos.

    Uso: findlinks <nombre de archivo>

15. Hex2dec: Pude convertir hexadecimal a decimal y viceversa con esta sencilla utilidad de línea de comandos.
    Uso: hex2dec [hex | decimal]
16. Desktops: Permite organizar sus aplicaciones en hasta cuatro escritorios virtuales. Lea el correo electrónico en uno, navegue por Internet en el segundo y trabaje en su software de productividad en el tercero, sin el desorden de las ventanas que no está utilizando. Después de configurar las teclas de acceso rápido para cambiar de escritorio, puede crear y cambiar de escritorio haciendo clic en el ícono de la bandeja para abrir una ventana de vista previa y de cambio del escritorio, o usando las teclas de acceso rápido. Sysinternals Desktops utiliza un objeto de escritorio de Windows para cada escritorio. Las ventanas de la aplicación están vinculadas a un objeto de escritorio cuando se crean, por lo que Windows mantiene la conexión entre las ventanas y los escritorios y sabe cuáles mostrar cuando se cambia un escritorio. Eso hace que los escritorios de Sysinternals sean muy ligeros y libres de errores, por lo que el otro enfoque es propenso a que su visión de las ventanas activas se vuelva inconsistente con las ventanas visibles.
17. Whois: Realiza el registro de registro para el nombre de dominio o la dirección IP que especifique. El nombre de dominio puede ser un nombre DNS o una dirección IP.
    Uso: whois [-v] domainname [whois.server]

Parámetro	Descripción
-v	Imprimir información whois para referencias.

18. PsPasswd: Es una herramienta que le permite cambiar la contraseña de una cuenta en los sistemas locales o remotos, lo que permite a los administradores crear archivos por lotes que ejecutan PsPasswd en las computadoras que administran para realizar un cambio masivo de la contraseña del administrador. PsPasswd utiliza las API de restablecimiento

de contraseña de Windows, por lo que no envía las contraseñas a través de la red de forma clara.

Uso: pspasswd [[\\ computer[, computer[, ..] | @file [-u user [-p pssswd]]] Username [NewPassword]

Parámetro	Descripción
computer	Ejecute el comando en la computadora remota o en las computadoras especificadas. Si omite el nombre del equipo, el comando se ejecuta en el sistema local y si especifica un comodín (\\ *), el comando se ejecuta en todos los equipos del dominio actual.
@file	Ejecute el comando en cada computadora listada en el archivo de texto especificado.
-u	Especifica el nombre de usuario opcional para iniciar sesión en la computadora remota.
-p	Especifica la contraseña opcional para el nombre de usuario. Si omite esto, se le pedirá que ingrese una contraseña oculta.
Username	Especifica el nombre de la cuenta para el cambio de contraseña.
NewPassword	Nueva contraseña. Si se omite se aplica una contraseña NULA.

19. RegDelNull: Esta utilidad de línea de comandos busca y le permite eliminar claves de registro que contienen caracteres nulos incrustados y que de otra manera no se pueden borrar con las herramientas estándar de edición de registros. Nota: la eliminación de las claves de registro puede hacer que las aplicaciones a las que están asociadas fallen.

    Uso: regdelnull <path> [-s]

Parámetro	Descripción
-s	Recurso dentro de las sub-llaves.

20. VMMap: es un proceso de utilidad de análisis de memoria virtual y física. Muestra un desglose de los tipos de memoria virtual comprometidos de un proceso, así como la cantidad de memoria física (conjunto de trabajo) asignada por el sistema operativo a esos tipos. Además de las representaciones gráficas del uso de la memoria, VMMap también muestra información resumida y un mapa detallado de la memoria del proceso. Las potentes funciones de filtrado y actualización le permiten identificar las fuentes de uso de la memoria de proceso y el costo de memoria de las funciones de la aplicación. Además de las vistas flexibles para analizar procesos en vivo, VMMap admite la exportación de datos en múltiples formas, incluido un formato nativo que conserva toda la información para que pueda volver a cargarla. También incluye opciones de línea de

comandos que permiten escenarios de scripting. VMMap es la herramienta ideal para los desarrolladores que desean comprender y optimizar el uso de los recursos de memoria de sus aplicaciones.

21. CacheSet: Es un applet que le permite manipular los parámetros del conjunto de trabajo de la caché de archivos del sistema. A diferencia de CacheMan, CacheSet se ejecuta en todas las versiones de NT y funcionará sin modificaciones en las nuevas versiones de Service Pack. Además de proporcionarle la capacidad de controlar el tamaño mínimo y máximo de los conjuntos de trabajo, también le permite restablecer el conjunto de trabajo del caché, obligándolo a crecer según sea necesario desde un punto de inicio mínimo. Además, a diferencia de CacheMan, los cambios realizados con CacheSet tienen un efecto inmediato en el tamaño de la memoria caché. Use CacheSet para ajustar el rendimiento del tamaño del caché del sistema de una manera que no sea posible sin ajustar las variables internas como lo hace CacheMan. CacheSet usa una llamada **NtQuerySystemInformation** para obtener información sobre la configuración de la memoria caché y **NtSetSystemInformation** para establecer nueva información de tamaño. La información del conjunto de trabajo para un proceso sirve como guía para el Administrador de memoria de NT con respecto a cuántas páginas de memoria física deben asignarse a la aplicación. Debido a que son pautas, las condiciones pueden resultar en que el Administrador de memoria haga crecer un conjunto de trabajo a un tamaño mayor que el máximo, o lo reduzca a menos del mínimo. Sin embargo, las configuraciones son factores que afectarán la asignación general y, por lo tanto, la capacidad de respuesta de una aplicación. En el caso de CacheSet, la aplicación es el sistema de archivos Caché. Internamente, **NtSetSystemInformation** llama a **MmAdjustWorkingSetSize**, que aumenta el conjunto de trabajo de una aplicación o lo recorta. Si el tercer parámetro pasado a **MmAdjustWorkingSetSize** es 1, el conjunto de trabajo del caché del sistema se ajusta, de lo contrario, el ajuste se realiza en el proceso actual (las llamadas de información del sistema afectan solo al caché del sistema). Pasar un mínimo y un máximo de -1 hace que **MmAjustWorkingSetSize** realice una operación de borrado de conjuntos de trabajo, liberando todas las páginas del conjunto de trabajo de la aplicación.

Tres distribuciones de análisis forense

1. SIFT - SANS Investigative Forensic Toolkit: La estación de trabajo SIFT es un grupo de respuestas forenses de código abierto y herramientas forenses diseñadas para realizar exámenes forenses digitales detallados en una variedad de configuraciones.
   Puede coincidir con cualquier respuesta a incidentes actual y conjunto de herramientas forenses. SIFT demuestra que las capacidades avanzadas de respuesta a incidentes y las técnicas forenses digitales de inmersión profunda a intrusiones pueden lograrse utilizando herramientas de código abierto de vanguardia que están disponibles de forma gratuita y se actualizan con frecuencia.
2. Security Onion: Security Onion es una distribución de Linux gratuita y de código abierto para la detección de intrusiones, el monitoreo de seguridad empresarial y la administración de registros.
   Incluye Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, Wazuh, Sguil, Squert, CyberChef, NetworkMiner y muchas otras herramientas de seguridad.
3. NST - Network Security Toolkit: La intención principal de desarrollar este conjunto de herramientas fue proporcionar al profesional de la seguridad y al administrador de la red un conjunto completo de herramientas de seguridad de red de código abierto.
   En el mundo virtual, NST se puede utilizar como una herramienta de análisis, validación y monitoreo de seguridad de red en servidores virtuales empresariales que alojan máquinas virtuales.
4. DEFT - Digital Evidence & Forensics Toolkit: El sistema DEFT se basa en GNU Linux, puede ejecutarse en vivo (a través de DVDROM o USB pendrive) o ejecutarse como un dispositivo virtual en VMware. DEFT trabaja actualmente en varios lugares y por varias personas, tales como: Militares, Funcionarios de Gobierno, Cumplimiento de la Ley, Investigadores, Testigos Expertos, Auditores de TI, Universidades e Individuos.

The Sleuth Kit (TSK)

The Sleuth Kit® (TSK) es una biblioteca y una colección de herramientas de línea de comandos que le permiten investigar imágenes de disco. La funcionalidad principal de TSK le permite analizar el volumen y los datos del sistema de archivos. El marco de complemento le permite incorporar módulos adicionales para analizar el contenido de los archivos y construir sistemas automatizados. La biblioteca se puede incorporar a herramientas forenses digitales más grandes y las herramientas de línea de comandos se pueden usar directamente para encontrar evidencia.

Permite examinar los sistemas de archivos de una computadora sospechosa de una manera no intrusiva. Debido a que las herramientas no dependen del sistema operativo para procesar los sistemas de archivos, se muestra el contenido eliminado y oculto. Se ejecuta en plataformas Windows y Unix.

Las herramientas del sistema de volumen (gestión de medios) le permiten examinar el diseño de los discos y otros medios. El kit Sleuth es compatible con particiones DOS, particiones BSD (etiquetas de disco), particiones Mac, segmentos de Sun (tabla de contenidos de volumen) y discos GPT. Con estas herramientas, puede identificar dónde están ubicadas las particiones y extraerlas para poder analizarlas con las herramientas de análisis del sistema de archivos.

Autopsy

Autopsy® es una plataforma forense digital y una interfaz gráfica para The Sleuth Kit® y otras herramientas forenses digitales. Es utilizado por los inspectores de las fuerzas del orden, militares y corporativos para investigar lo que sucedió en una computadora. Incluso puede usarlo para recuperar fotos de la tarjeta de memoria de su cámara. Fue diseñada para ser una plataforma de extremo a extremo con módulos que vienen con ella fuera de la caja y otros que están disponibles de terceros. Algunos de los módulos proporcionan:

- Análisis de la línea de tiempo: interfaz de visualización gráfica avanzada de eventos (video tutorial incluido).
- Filtrado de hash: marca los archivos mal conocidos e ignora los buenos.
- Búsqueda por palabra clave: búsqueda por palabra clave indexada para encontrar archivos que mencionan términos relevantes.
- Artefactos web: extraiga el historial, los marcadores y las cookies de Firefox, Chrome e IE.
- Talla de datos: recupere archivos eliminados de un espacio no asignado utilizando PhotoRec.
- Multimedia: extraer EXIF de imágenes y ver videos.
- Indicadores de compromiso: escanear una computadora utilizando STIX.

Comentario

Para el análisis forense es necesario, conocer las herramientas que nos permitan realizarlo tanto para Windows como Linux, es necesario conocer las herramientas que cuenta Windows SysInternals, ya que cuenta con una gran variedad de herramientas que nos ofrecen información del equipo, conocer distribuciones que nos ayudan para el análisis forense es de ayuda ya que vienen instaladas herramientas para el análisis forense, Sleuth Kit nos ofrece una variedad de

herramientas para el análisis del sistema de archivos y Autopsy nos permite recuperar datos, lo que nos permite la realización de un análisis forense.

Referencias

https://docs.microsoft.com/en-us/sysinternals/downloads/accessenum

https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk

https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer

https://docs.microsoft.com/en-us/sysinternals/downloads/autologon

https://resources.infosecinstitute.com/category/computerforensics/introduction/free-open-source-tools/overview-of-computer-forensics-linux-distributions/#gref

https://itsfoss.com/linux-hacking-penetration-testing/

https://www.yeahhub.com/6-linux-distributions-forensics-investigation/

https://www.sleuthkit.org/autopsy/

https://www.sleuthkit.org/sleuthkit/

https://www.sleuthkit.org/sleuthkit/desc.php

https://docs.microsoft.com/en-us/sysinternals/downloads/diskmon

https://docs.microsoft.com/en-us/sysinternals/downloads/diskext

https://docs.microsoft.com/en-us/sysinternals/downloads/desktops

https://docs.microsoft.com/en-us/sysinternals/downloads/debugview

https://docs.microsoft.com/en-us/sysinternals/downloads/bginfo

https://docs.microsoft.com/en-us/sysinternals/downloads/cacheset

https://docs.microsoft.com/en-us/sysinternals/downloads/diskview

https://docs.microsoft.com/en-us/sysinternals/downloads/du

https://docs.microsoft.com/en-us/sysinternals/downloads/efsdump

https://docs.microsoft.com/en-us/sysinternals/downloads/findlinks

https://docs.microsoft.com/en-us/sysinternals/downloads/hex2dec

https://docs.microsoft.com/en-us/sysinternals/downloads/vmmap

https://docs.microsoft.com/en-us/sysinternals/downloads/pspasswd

https://docs.microsoft.com/en-us/sysinternals/downloads/regdelnull

https://docs.microsoft.com/en-us/sysinternals/downloads/ntfsinfo