Taller Forense Básico Windows

OpenWebinars

¡BIENVENIDOS!

Soy Jordi Ubach Manau

Me dedico a Ciberseguridad & Forensic

https://www.linkedin.com/in/jordi-ubach-9971a1a5/

ÍNDICE

- Ubicando bases de datos de miniaturas
- Captura de la memoria volátil
- Captura de la memoria de paginación
- Captura de servicios en ejecución
- Captura de lista de usuarios iniciado sesión
- Captura de estado de red
- Captura MBR

COOKIES

- Varias cookies sin fecha o con fecha de vencimiento por ej.: año 25000 será persistente siempre, se utiliza para verificar conjunto Usuario, navegador, etc. Hoy existen las llamadas supercookies:
- Además, hay aplicativos que son capaces de recolectar cookies de otros portales.

  - Podemos tener accesos a sitios no controlados, “mega upload” ….
  - Utilizaremos “historian” permite recoger datos, índices, etc recogiendo día, hora, usuario
  - Corte búsqueda en CMD:
  - cd .. cd.. → directorio raíz
  - dir cookie*.* /s /p (depende de la versión de windows se guarda en diferente sitios
  - Revisamos las ubicaciones mostradas por pantalla.

- Nos mostrara alguna info, usuario, dominio, si lo editamos veremos que esta ofuscada la información. Guardaremos info en el pendrive forense con el hash
- Lo importante de HISTORIAN, nos permite ver la información más digerida y detecta que tipo de info se trata, RAM, historial, etc
- Abrimos la aplicación y vamos a los paths encontrados.
- Podemos seleccionar todas las cookies de golpe
- Seleccionamos las cookies → un archivo o varios → export (lo exporta a la misma carpeta
- Pasamos al pendrive forense, abrimos y veremos los datos (fecha, hora, etc). HASH importante.

Ver sitios donde se ha navegado (posibles fugas información)

- Ejecutar un corte de búsqueda cd .. cd .. dir index.dat /s /p /a
- Como son varios, los iremos copiando a una carpeta Index1, index2,….
- Siempre con privilegios de administrador sino una distro linux
- Grabamos a un fichero + HASH y Utilizaremos HISTORIAN

Descubrir qué aplicaciones se han ejecutado

dir *.pf /s /a /p

- listara los prefetch
- veremos que están todos en el directorio Prefetch
- Abrimos HISTORIAN y vamos a la carpeta prefetch
- Exportamos como ExportAPP abrimos
- Buscamos algo sospechoso (TPVCGATEWAY)

Listado Cache Mui

- Cada vez que se ejecuta un programa se escribe una clave en el registro de windows.
- Ejecutaremos Muicache view
- rastreamos los procesos

    ojo!!! hh.exe /

Ubicando bases de datos de miniaturas (WFA THUMB.exe)

    dir thumb*.db /s /p /a

- encontrará un montón de tablas de miniaturas
- Copiar todas las bases i llevarlas al pendrive forense
- Ejecutaremos la herramienta WFATHUMB.exe sirve para varios (mostrar)
- Pero seleccionamos “analizar la base de datos de miniaturas”
- Hacemos la prueba con la que tenemos en carpeta “thumbs.db”

CAPTURA DE LA MEMORIA VOLATIL

- También nombrada memoria de intercambio o swap, el elemento más volátil es la memoria RAM.
- Dumpit (se crea un fichero donde se ejecuta)
- Ejecutamos
- la herramienta realiza un volcado.
- Realiza el volcado de todas las versiones de windows
- Saca un fichero en formato RAW
- Guardamos el archivo en la carpeta de evidencias junto con el HASH (botón derecho y suma de comprobación que deseamos)

- Para visualizar no podemos utilizar notepad, etc
- Abrimos Disk investigator y puede leer en crudo, revisamos la información.

CAPTURA DE LA MEMORIA DE PAGINACIÓN (SHADOWCOPY)

- Denominada pagefile.sys, generalmente en c: pero se debe buscar debido a que puede estar ubicada en otros entornos. Permite buscar usuarios, contraseñas….
- Sí que es cierto que clonando el disco podríamos tener este fichero, pero debemos saber que existe una opción para borrar este archivo cada vez que se apaga la maquina
- Presenta un desafío importante, ya que windows protege en modo de ejecución

  ej.: cmd dir /a

  copy pagefile.sys C:/forense pf.sys → no deja ni como administrador debido a limitaciones del Kernel.

- Hay pocas herramientas que puedan realizar una copia en caliente.
- Instalamos la herramienta shadow copy y “ejecutamos como administrador”
- La herramienta utiliza BSS (servicio copia sombra de windows)
- Casilla FILEMASK “*.sys” para que no copie lo demás
- Ruta directorio i HASH
- Desactivar casilla “copiar subdirectorios”
- Le damos a “copy”

CAPTURA SERVICIOS EN EJECUCIÓN (PS service)

- Es interesante capturar en tiempo real los servicios en ejecución, ya que es posible que haya en funcionamiento algún RAT.
- Un servicio es transparente al usuario, y no necesita interacción con el usuario. Debemos utilizar aplicaciones que no sean del sistema operativos, podríamos utilizas el services.msc, podrían estar comprometidos por un rootkit.

  Psservice.exe > servicios.txt

- Enviar el fichero al pendrive forense
- podemos editarlo y buscar “remoto”, u otros servicios. Los servicios pueden estar stoped o running.
- Repasar un poco todos los servicios.

CAPTURA PROCESOS EN EJECUCIÓN (PS list)

- Un proceso a diferencia del programa es el acto y administración de un recurso del programa, como en una receta de cocina el proceso serio (hacerlo, hornearlo, etc. Como otras ocasiones, el s.o tienes aplicaciones, pero no las utilizaremos

  Pslist.exe > procesos.txt

- pasamos a pendrive y HASH
- Verificar proceso Idle= 0 (proceso de tiempo muerto) sino tenemos un problema (rootkit, etc)
- Repasamos el resto de procesos para ver que tenemos (svhost, spool)

CAPTURA LISTA USUARIOS INICIADO SESIÓN (PSLOGGEDON)

- Toma una instantánea de los usuarios del sistema, podemos tener usuarios máquina y personas, pero existe un Superuser SYSTEM, puede desencriptar cualquier volumen, ciertos archivos del sistema, solo podrán ser borrados por este usuario. Es importante tener una toma de todos los usuarios que han iniciado sesión, y si hay posible pivoting. Existen aplicaciones del s.o. pero vamos a utilizar otros.

  PsLoguedon.exe > Loggued.txt

  Guardamos evidencia + hash

  Podríamos usar “net users” pero no recomendable

  “net accounts”

  “net session” si da error debemos iniciar terminal como administrador

CAPTURA estado de red. (Promiscuous Detect)

- Entre la información volátil que debe ser adquirida, se encuentra el estado de toda la red, tablas de netbios, caché de dns, dominios permitidos, estado dhcp

  promisdetect.exe > estadored.txt (verificamos los roles “direct, multicast 224,0,x,x, promiscuous”

  Netviewx.exe >> estadored.txt no da información del tipo de máquina que es, si un atacante le hubiera dado un rol más, se mostraría

  arp -a >>estadored.txt liga todas las direcciones ip con las mac (MIM)

  nbtstat -c >> estadored.txt (tabla netbios de todo lo que conoce)

  ipconfig /a >> estadored.txt muestra mucha info sobre los adaptadores podemos comprobar la mac con la tarjeta por si se está haciendo macspoofing

  ipconfig /displaydns >> estadored.txt

  netstat -an >> estadored.txt

CAPTURA MBR(MbrUtil)

- La parte mínima de una unidad es un sector (512b), y son agrupados en clusters, el sector 0 se encuentra el MBR. Es lo primero que lee la Rom bios (CMOS), le dirá al CMOS que disco y cuantas particiones tiene. Otra cosa que almacena es en qué sector inicia cada partición, y cuál es la partición activa.

- Ciertos virus de MBR, modifican el acceso al Bootstrap i se inician ellos en memoria.

  Mbrutil.exe /S=mbr.evi

  como se ve? Sin ningún formato

  Este archivo podemos subirlo a virus total o symantec y analizarán MBR y nos dirán si hay algún tipo de amenaza.

  Guardamos report y fichero, en pendrive + HASH