



Los procedimientos seguidos son la clave para realizar el análisis forense con completa seguridad y éxito, ya que la captura de la información puede haber sido tediosa o compleja en función del escenario encontrado, sin embargo el mayor problema que nos encontramos cuando ya disponemos de la información es la detección, clasificación y correlación de los mismos, ya que como indicabamos en el anterior tema, se puede disponer de mucha información pero si carecemos de los conocimientos o herramientas necesarios para su descubrimiento poco o nada extraeremos de los mismos. De ahí la importancia de los procedimientos ya que al seguir un patrón fijado previamente evitaremos que nos saltemos un paso.

La norma UNE 71506:2013 de Sistema de Gestión de Evidencias Electrónicas describe dichos procedimientos que nos ayudarán a no olvidar ningún elemento de análisis y correlación. Además su estandarización a nivel comercial la convierten en imprescindible para aquellos profesionales que deseen dedicarse al mundo del analisis forense.

Por otra parte en el entorno de la AGE - Administración General del Estado la norma-tipo implementada es la publicada por el CCN - Centro Criptológico Nacional CCN-STIC ENS 818 que nos mostrará de forma más o menos pormenorizada los puntos de interés a analizar y no perder eventos o elementos que nos ayuden al esclarecimiento del incidente de seguridad. Aunque como acostumbra a ser normal dado el retraso tecnológico de implementación de ésta tecnología, otros países nos llevan la delantera, dado que muchas de nuestras normas se basan en manuales, normas y guías de terceros.

¿Qué es la correlación de eventos?

Entendemos la correlación de eventos como el proceso de analizar los datos de eventos para identificar patrones, causas comunes y causas iniciales. La correlación de eventos analiza los eventos entrantes para estados predefinidos mediante reglas predefinidas y para relaciones predefinidas.

El fin y la meta de la correlación de eventos en el entorno forense es la detección de las acciones practicadas por un atacante en un sistema vulnerado. Dicho de otro modo, pretendemos unir las piezas de un rompecabezas, analizando su patrón y a la vez determinando el momento en el que fueron reunidos. Solo desde la comprensión y unificación de los elementos u acciones detectadas podremos conocer el qué, el cómo y el cuando del ataque y de la información o acciones que se realizaron en la maquina o sistema comprometido.

Así pues la correlación se muestra igual de vital en el esclarecimiento de las actividades sospechosas detectadas como la causa y el objetivo del mismo. A modo de ejemplo y como explicación del mismo.

Para introducirse en el PC de nuestra casa, un atacante debería conocer la IP de nuestro ISP (Proveedor de Internet) y vulnerar previamente como primer paso el router-router wifi de nuestro domicilio. La primera actividad que realizará será buscar la marca, modelo y credenciales por defecto de nuestro router, una vez detectado el mismo procederá a intentar validarse contra el mismo si la administración WAN y las credenciales por defecto no han sido modificadas; hay que recordar que además de la contraseña de administrador los routers disponen de una clave para soporte que con frecuencia no es cambiada para que desde el ISP nos controlen el router; una vez superado ese primer escollo procederá a buscar en nuestra red domestica bajo las IP's de clase 3, determinar cuantas máquinas (PC, portátiles, tablets, etc.) tenemos conectados. Analizará las IPs, Sistemas Operativos, versiones de software y puertos abiertos para determinar el mejor vector de ataque y usará el más productivo para sus fines, Java, Flashplayer y navegador (Internet Explorer 0 a 9 son vulnerables) son el vector de ataque siempre y tienen multiples vulnerabilidades, en el caso de Java al ser multiplataforma, permite el ataque a máquinas bajo otros Sistemas Operativos como UNIX, Mac, Solaris, etc. Y una vez infectado nos extraera la información, contraseñas guardadas en los navegadores, cookies para secuestro de sesión, etc.

Una vez que hemos detectado el comportamiento anomalo de nuestro PC, ralentización, IP ajena conectada a nuestro router, etc. empezamos a mirar que está pasando, con frecuencia procedemos a buscar herramientas instaladas o programas que antes iban bien y ahora van "de pena". Miramos los "logs" y descubrimos que nuestro PC se conecta a paginas web raras o que por tener el Wake On LAN se arrancó a las 5 de la mañana mientras dormiamos, resultado descubrimos que aquel PDF que nos descargamos el otro día estaba infectado y nos han atacado el PC al abrirnos dicho PDF una puerta desde el navegador.

Para seguirle los pasos al atacante habrá que hacer el análisis de dentro hacia fuera, primero determinar lo extraño e ir hacia fuera para ver los logs del router finalmente e identificar la IP atacante que se conecto a nuestro router. Cuando juntasemos todas las piezas podriamos conocer la hora a las que se produjeron y los ficheros alterados o consultados, conociendo el objetivo de sus actividades.

La seguridad perimetral de nuestros sistemas es vital para evitar este tipo de situaciones, por lo que para construir un eficiente sistema de defensa debemos construirlo desde dentro hacia fuera. Osea instalación Sistema Operativo mas actualizado, parcheado, antivirus, firewall, sustitución de credenciales por

defecto en elementos de red (router, switch, impresora, escaner de red, etc.), filtrado por MAC, fortalecimiento de contraseñas con al menos 12 caracteres mezclando numeros, letras mayusculas y minusculas, y finalmente eliminar la autorización de conexión desde la WAN, además de los servicios Telnet y SSH al router.

Así pues solo mediante la correlación podremos determinar el cuándo, cómo y el que nos han robado. Con frecuencia todo el mundo piensa que no es una victima potencial, cuando la idoneidad para convertirse en victima es tener un sistema vulnerable y fácil. Los atacantes siempre eludirán las complicaciones si no tienen un objetivo definido y prefijado.