www.eysglobal.com

MÓDULO 1
TEMA 6: VERTIENTES DE UN ANALISIS FORENSE

VERTIENTES DE UN ANALISIS FORENSE

V1: PREPARACIÓN PARA EL ANÁLISIS

Se puede utilizar software como VMware5, que permitirá crear una plataforma de trabajo con varias máquinas virtuales. También se puede utilizar una versión LIVE de sistemas operativos como Caine6, que permitirá interactuar con las imágenes montadas pero sin modificarlas. Si se está muy seguro de las posibilidades y de lo que va a hacer, se puede conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para intentar hacer un análisis en caliente del sistema, se deberá tomar la precaución de montar los dispositivos en modo sólo lectura, esto se puede hacer con sistemas anfitriones UNIX/Linux, pero no con entornos Windows.

V2 : RECONSTRUCCIÓN DEL ATAQUE

Si ya se tienen montadas las imágenes del sistema atacado en una estación de trabajo independiente y con un sistema operativo anfitrión de confianza, se procede con la ejecución de los siguientes pasos:

•

Crear una línea temporal o timeline de sucesos.

•Ordenar los archivos por sus fechas MAC, esta primera comprobación, aunque simple, es muy interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los ficheros nuevos, fechas MAC muy distintas a las de los ficheros más antiguos.

V3: DETERMINACIÓN DEL ATAQUE

Una vez obtenida la cadena de acontecimientos que se han producido, se deberá determinar cuál fue la vía de entrada al sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el

atacante para aprovecharse de tal brecha. Estos datos, al igual que en el caso anterior, se deberán obtener de forma metódica, empleando una combinación de consultas a archivos de logs, registros, claves, cuentas de usuarios.

V4: IDENTIFICACIÓN DEL ATACANTE.

Si ya se logro averiguar cómo entraron en el sistema, es hora de saber quién o quiénes lo hicieron. Para este propósito será de utilidad consultar nuevamente algunas evidencias volátiles que se recopiló en las primeras fases, revisar las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además buscar entre las entradas a los logs de conexiones. También se puede indagar entre los archivos borrados que se recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

V5 : PERFIL DEL ATACANTE.

Otro aspecto muy importante es el perfil de los atacantes y sin entrar en muchos detalles se podrá encontrar los siguientes tipos:

V6 : EVALUACIÓN DEL IMPACTO CAUSADO AL SISTEMA

Para poder evaluar el impacto causado al sistema, el análisis forense ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron al sistema. Esto permitirá evaluar el compromiso de los equipos y realizar una estimación del impacto causado. Generalmente se pueden dar dos tipos de ataques:

DELITOS INFORMATICOS

Delito informático, delito cibernético o ciberdelito es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet.

DELITOS INFORMATICOS - MODALIDADES

NUEVAS TENDENCIAS DEL CIBERCRIMEN ORGANIZADO PORNOGRAFÍA INFANTIL

La corrupción de menores y la pornografía infantil, que utilizan como víctimas a niños y niñas destruye vidas porque el circuito que apela a la inhumanidad para cernirse sobre ellos en pro de la mercantilización, de la distribución de material pornográfico, así como el reclutamiento de víctimas de explotación sexual comercial, tiene garantizada su permanencia, y aún su incremento, en tanto y en cuanto los seres humanos insistan en valorizar lo humano, mediante la apropiación y destrucción de vidas infantiles y adolescentes. Este modelo horroroso impregna la cotidianeidad de los países denominados civilizados, y viola todos y cada uno de los derechos, de esos niños y jóvenes, sus derechos, y sus personas.

SUPLANTACIÒN DE SIM CARD

Modalidad en la que el ciberdelincuente aprovechando que el titular de una línea telefónica se encuentra de viaje o no puede atender llamadas, se presenta en oficinas de empresas de operadores de telefonía móvil para obtener una simcard nueva a partir de la suplantación del titular.

TRÁFICO DE DATOS FINANCIEROS PERSONALES

Modalidad de estafa en la que los ciberdelincuentes aplican técnicas de ingeniería social vía telefónica, para obtener acceso a información personal y financiera de sus víctimas, con el fin de realizar operaciones fraudulentas y obtener beneficios económicos.

FRAUDE POR FALSO WHATSAPP

Después del nacimiento de WhatsApp Web se crearon otros sitios fraudulentos que imitaban al original. La utilización de aplicaciones alojadas en las tiendas virtuales oficiales, son usadas para la creación de conversaciones falsas por parte de personas inescrupulosas que utilizan los datos públicos como la foto de perfil y el número de celular de las víctimas para simular chats y enviar pantallazos de las conversaciones para obtener información y cometer delitos vinculados a la afectación de la reputación de las personas, estafas, extorsión.

CIBERINDUCCIÓN AL DAÑO FÍSICO Y MENTAL A MENORES DE EDAD

Si un niño no cuenta con las habilidades necesarias para discriminar qué información es cierta y que información es falsa o para interactuar de forma segura en internet, es muy fácil que pueda verse comprometido en uno de estos grupos que promocionan un modelamiento de interacción a base de retos con fines de autolesión, cuya acción criminal atenta en contra de la vida y la integridad de los mismos. Un ejemplo de este tipo de cibercrimen es el conocido como “La Ballena Azul” o “El reto del Hada de Fuego”, que ha ocasionado suicidios y serias lesiones físicas y mentales de adolescentes y jóvenes,

CIBERPIRÁMIDES

Con la incertidumbre y a su vez el gran auge de las criptomonedas como el Bitcoin, el Ripple o el Ethereum, los ciberdelincuentes por medio de las denominadas ciberpirámides lograron captar la atención de incautos inversionistas en once ciudades del país con el ofrecimiento de esas monedas virtuales. Miles personas reportaron haber sido estafadas,

ESTAFAS POR INTERNET