Hacker Highschool

SECURITY AWARENESS FOR TEENS



LECCIÓN 8
ANÁLISIS Y CONTRAMEDIDAS FORENSES

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

WARNING

The Hacker Highschool Project is a learning tool and as with any learning tool there are dangers. Some lessons, if abused, may result in physical injury. Some additional dangers may also exist where there is not enough research on possible effects of emanations from particular technologies. Students using these lessons should be supervised yet encouraged to learn, try, and do. However ISECOM cannot accept responsibility for how any information herein is abused.

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool Project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license, including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the HHS web page at http://www.hackerhighschool.org/licensing.html.

The Hacker Highschool Project is an open community effort and if you find value in this project, we ask that you support us through the purchase of a license, a donation, or sponsorship.

AVISO

El proyecto Hacker Highschool es una herramienta de aprendizaje, y como tal existen riesgos. El mal uso de algunas lecciones puede terminar en daño físico. Existen riesgos adicionales ya que no existen estudios suficientes sobre los posibles efectos de las emisiones en algunas tecnologías. Los estudiantes que sigan estas lecciones deberían ser supervisados y motivados a aprenderlas, probarlas y utilizarlas. No obstante, ISECOM no acepta responsabilidad alguna por el mal uso de la información presentada.

Las siguientes lecciones y cuadernos de trabajo son abiertos y accesibles al público bajo los siguientes términos y condiciones de ISECOM:

Todas las obras del proyecto Hacker Highschool se proporcionan para su uso no comercial con estudiantes de escuelas primarias, secundaria y bachillerato ya sea en centros públicos, instituciones privada, o educación en casa. Este material no puede ser reproducido para su venta bajo ningún concepto. Impartir cualquier clase, formación o actividad con estos materiales cobrando por ello está expresamente prohibido sin la adquisición de una licencia, incluyendo cursos en escuelas, clases universitarias, cursos comerciales, cursos de verano, campamentos de informática, y similares. Para adquirir una licencia, visite la sección LICENCIA en la página web de Hacker Highschool en www.hackerhighschool.org/licensing.html.

El proyecto HHS es resultado del esfuerzo de una comunidad abierta. Si encuentra útil este proyecto, le pedimos que nos apoye mediante la compra de una licencia, una donación o patrocinio.

Table of Contents

WARNING.... 2
Contributors.... 5
Introducción.... 6
Alimenta tu mente: ¿Qué necesitas para ser en Investigador Forense Digital?.... 8
El truco mágico de la desaparición de los datos (Dónde y cómo ocultarlos).... 8
Lo primero es lo primero: Grandes conjuntos de datos.... 8
Alimenta tu mente: ¿Por dónde comienzan los investigadores forenses?.... 9
No puedes ir directamente de 'A' hasta 'B'.... 10
Herramientas.... 10
Cavando el túnel.... 11
Pasar la pelota.... 11
Trabajando desde casa.... 12
Siguiente paso – Bocaditos de Bytes.... 12
Intercambia en el intercambiador.... 12
Tú déjale sitio.... 13
Reformando archivos.... 13
Alimenta tu mente: ¿Qué tipo de pruebas electrónicas reúnen los investigadores?.... 15
Dispositivos.... 15
Su impresora les delata.... 15
Backups.... 15
Pruebas digitales.... 16
Pero antes, has de conocer las leyes.... 16
El truco mágico de la desaparición de datos (Hacer los datos irrecuperables).... 16
Lavar, aclarar y repetir.... 17
Más herramientas software.... 17
Boot and Nuke.... 17
Eraser.... 18
Sderase.... 18
Martillear, taladrar y machacar.... 18
Planta un jardín.... 19
Sembrando el jardín.... 19
Alimenta tu mente: Principios de la Ciencia Forense Digital.... 20
Metodología para forenses digitales.... 20
Proceso digital forense.... 21
¡Las pruebas se pierden constantemente!.... 21
Ejercicio exclusivo para agentes de los cuerpos de Policía.... 22
Estar lejos de casa: cuando lo profesional se mezcla con lo personal.... 23
Herramientas y colecciones de software.... 24
Análisis de los soportes de datos.... 24
La hora de la cita.... 25
Llegar a tiempo... con Offset.... 25
Datos EXIF.... 25
Herramientas para imágenes.... 26
¡Trata de arrancarlo!.... 26
Datos borrados.... 26
Alimenta tu mente: un vídeo puede absolverte... o condenarte.... 27
Formateo de soportes.... 27
Precauciones a tener en cuenta cuando recopiles pruebas de un soporte de datos.... 28
Esteganografía: Una mirada a las controversias de la seguridad.... 28
Esteganografía: Es real, es fácil y funciona.... 29
La esteganografía es un timo.... 31

Análisis forense en Windows 32
Los portátiles son como cofres del tesoro 32
Información volátil 32
Herramientas para recopilar información volátil en Windows 33
Información no volátil 34
¿Preparados? Luces, cámaras... ¡Acción! 34
Localización y edición del registro de eventos de Windows Server 2008 35
Análisis forense en Linux 35
El Slack en Linux 36
Cadenas simples 36
Grep 36
Más herramientas en línea de comandos 36
Cómo encontrar un pajar en una aguja 37
Cifrado, descifrado y formatos de archivo 37
Alimenta tu mente: algunos casos reales 39
Análisis forense de móviles 39
Conecta el cable azul al conector rojo 40
Requiere desmontaje 40
Tantos dispositivos, tan poco tiempo 41
Ejemplo de análisis forense de un iPhone 42
Herramientas software para teléfonos 42
¿Y ahora qué? 43
Análisis forense de la red 43
Registros del firewall 44
Packet Sniffers 44
Sistemas de detección de intrusos, o Intrusion Detection Systems (IDS) 44
Registros en los Routers y Administración de red 45
Herramientas para el tráfico de las redes 45
Cabeceras del E-Mail 45
Comienza el juego: Boca abajo y sucia 46
Comencemos con la diversión 49
Reconocimiento 49
Vulnerabilidades software y hardware 49
OpenVAS 49
Armas para hackear redes 50
El juego continúa: Arreglándose para el “Gran Pestazo” 53
Contramedidas forenses 56
Quién tiene ventaja 56
Tienes que ser social 57
Con la cabeza en las nubes 57
Problemas con los análisis forenses en la nube 57
Conclusiones 59

Contributors

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Bob Monroe, ISECOM
Simone Onofri, ISECOM
Greg Playle, ISECOM
Willy Nassar
Ken Withey
Alfonso Arjona, ISECOM
Adrian Crespo, madrid.crespo@gmail.com

ISECOM

Introducción

Si estás pasando por todo el proceso de aprender hacking y te gustaría practicarlo, necesitarás saber cómo ocultar tus huellas. Es muy razonable pensar que serás objeto de una investigación si consigues ejecutar un hackeo realmente bueno. No importan los "por qué" y "cómo" del hack: los investigadores buscarán pruebas para localizarte y relacionarte con el crimen. Y estos profesionales que tanto se interesan por ti son los "Investigadores forenses digitales" o "Digital Forensic Examiners" (en inglés). La verdad es que ese nombre da un poco de miedo. Pero no te preocupes: esta lección te explicará todo lo que debes saber sobre ellos.

Cada una de las lecciones de Hacker Highschool no es más que una muestra de un vasto océano de información. Algo así como una degustación de la enorme cantidad de materias que te abrirá el apetito por el hacking. Esta lección, concretamente, te proporcionará conocimientos avanzados que te ayudarán a mantenerte a salvo. Saber cómo usarlos depende por completo de ti. Te indicaremos lugares donde mantener tus datos a salvo y la forma de mantener esos tesoros ocultos, lejos del alcance de miradas indiscretas. ¿Qué habría de bueno en hackear un sistema y obtener información vital si no puedes guardarla en un lugar seguro?

Cuando lleves algún tiempo siendo un hacker, estarás saturado con toda clase de soportes de almacenamiento de los que necesitarás deshacerte. Posiblemente ya no te interese conservar esa memoria USB de 256 megabytes; o quizás esa tarjeta SD de 16 megabytes sea demasiado pequeña como para que darle otra utilidad aparte de usarla como marcapáginas. Sea cual sea el caso, no es buena idea tirarlos a la basura. Por ejemplo, tu viejo disco duro; si, el que usaste para hacer un XSS en el departamento de lencería de una tienda on-line: no puede terminar sus días en el cubo de la basura en su estado actual. Te enseñaremos cómo hacer que esos datos desaparezcan. Aprenderás métodos, con garantías, de hacer que nadie pueda volver a leer los datos de esos dispositivos. Las pruebas tienen que desaparecer.

Cuando hayas eliminado todo lo innecesario, probablemente volverás a explorar nuevos dominios. Cuando alguien accede a un sistema ilegalmente deja huellas de su entrada al sistema, de sus exploits y de su salida. Lo delincuentes saben que estas pistas digitales se quedan en el sistema, y llamarán la atención de las autoridades locales. Y no te gustaría que pasara eso ¿verdad?

Es parecido a limpiar tu habitación: necesitas saber cómo hacerlo por ti mismo. Todo, desde ocultar tu localización, cambiar los métodos de entrada, modificar las fechas del registro del sistema, copiar datos sin que nadie se dé cuenta o abrir puertas traseras debe planificarse y ejecutarse conforme avanzas. Analizaremos las mejores técnicas para ello.

Si alguna vez la policía te pide ayuda para resolver un crimen, deberías saber que los delincuentes emplean trucos sencillos pero efectivos para desviar o ralentizar la investigación. Posiblemente tendrán un abogado... o puede que no. Hay formas de permanecer un paso por delante de los investigadores, e incluso existen muchas más de divertirse con los forenses.

Las contramedidas forenses son precisamente lo que su nombre indica, y es que el análisis forense es parecido a jugar al gato y al ratón: hay que moverse incluso antes que la otra persona comience. La forma de usar las contramedidas depende de lo que quieran obtener. Pueden borrar pruebas para ralentizar tu trabajo como investigador, alterarlas para hacer que no sean fiables, o incluso divertirse con los guardias de la

puerta. Este capítulo te mostrará una visión general de todos los temas que hemos presentado y le dará, posiblemente, sentido a todo.

Pocos hackers trabajan en solitario. Hoy día, el hacking es un negocio. Las organizaciones de hackers tienen oficinas, estructuras de gestión y pagan nóminas. Uno sólo puede imaginarse qué tipos de planes de jubilación y salud ofrecen a sus empleados. Los negocios de hacking tienen sistemas bastante buenos de comunicaciones, gracias en parte a la encriptación. Tú también necesitarás usar una tecnología que te proteja de escuchas no autorizadas para comunicarte con tu interlocutor. Cualquiera con quien vayas a trabajar, te enseñará métodos para protegerte mejor. Si tu teléfono se convierte en el objetivo, te diremos cómo evitar que te localicen o intercepten tu tarjeta SIM. También te enseñaremos a modificar la SIM y a utilizar AES (Advanced Encryption Standard) para realizar llamadas seguras por VoIP con tu terminal.

Te mostraremos las armas que se utilizan en este campo de batalla. ¿A que no te gustaría entrar en combate con una cuchara de plástico para defenderte? En este capítulo te enseñaremos las mejores y últimas herramientas de análisis forense, tanto comerciales como Open Source. Durante tu entrenamiento te enseñaremos las técnicas que se emplean para eludir los cortafuegos comerciales, IDS, análisis de actividades y muchos otros obstáculos que encontrarás en el camino. Lo que necesitas es saber cómo los criminales consiguen no dejar apenas rastros de sus actividades, o incluso algo más importante: aprender cómo consiguieron traspasar esos carísimos sistemas. Son conocimientos muy útiles para aprender las debilidades de las herramientas forenses y saber cómo aprovecharlas.

Y para terminar esta lección, te enseñaremos a usar las técnicas más eficaces que utilizan los delincuentes para penetrar sistemas sin ser detectados, ejecutar sus actividades, dejar una puerta trasera, limpiar los registros del sistema y salir de allí sin que nadie se dé cuenta.

Con estos conocimientos ¡sólo tú serás capaz de atraparlos!

Alimenta tu mente: ¿Qué necesitas para ser en Investigador Forense Digital?

Saber cómo encontrar cosas es lo mismo que saber cómo esconderlas. Si te interesa convertirte en investigador forense necesitarás tener unos buenos conocimientos sobre informática general: hardware, software, varios sistemas operativos, aplicaciones y redes. Te hará falta tener curiosidad y ser capaz de explorar zonas de una red que volverían loco a cualquier otro. La capacidad de tomar decisiones y dar respuestas rápidas deben equilibrarse con la paciencia, para poder hace frente a dos tareas fundamentales del análisis forense:

Examen en vivo: sucede cuando las pruebas digitales todavía están en funcionamiento, no se han desconectado, y el dispositivo para recuperarlos es accesible para ser examinado.

Post Mortem: el crimen ya se ha cometido. Las pruebas pueden encontrarse en cualquier sitio, así que tu trabajo será mucho más difícil dado que los criminales pueden haber utilizado contramedidas forenses para complicar la investigación. Post-mortem (que en latín significa "una vez muerto") normalmente implica que los dispositivos electrónicos que pudieran contener las pruebas se han apagado antes de que llegaras.

Y dado que eres un forense muy capacitado, ya sabes que debes seguir un proceso perfectamente definido para recopilar, analizar y proteger las pruebas digitales.

Muchos investigadores buscan obtener certificaciones profesionales o asistir a cursos de capacitación que están disponibles en diversos sitios. Esto puede mejorar su credibilidad como ṕeritos expertos, pero no es un requisito imprescindible ya que no hay nada mejor que la experiencia adquirida con el tiempo.

El truco mágico de la desaparición de los datos (Dónde y cómo ocultarlos)

Imagina por un momento que trabajas como asesor externo para una agencia secreta del gobierno, dedicada a proteger a menores de ciberacosadores (bulling). Mientras investigabas una red de la que procedían mensajes contra alguien que necesitaba protección, te has encontrado (lo has hackeado) con un sistema que tiene una información muy especial. Deja volar tu imaginación con el concepto de "información muy especial". Sea lo que sea esa información, supongamos que has conseguido hacerte con una copia de la misma. ¡Buen trabajo!

Bien... así que ahora tienes varios megabytes de información en tu ordenador. ¿Dónde tienes pensado guardarla? No es nada recomendable dejarla en tu equipo. Y ya que estamos imaginando, ¿qué tal si ese sistema es propiedad de una organización criminal? ¿Y si añadimos a la historia ochenta y cinco sicarios de la mafia calabresa que, armados hasta los dientes, se dirigen a tu casa? Estos sicarios tienen perros de presa, un helicóptero con armamento pesado... y están todos de mal humor porque no tuvieron tiempo de desayunar en condiciones. Tienes que hacer desaparecer esa "información especial" como por arte de magia ¡y rápido!

Lo primero es lo primero: Grandes conjuntos de datos

Puedes mantener los datos (prestados) en tu equipo (no es muy inteligente hacer eso), siempre y cuando utilices un cifrado fuerte, de forma que no se almacenen en texto claro. Una idea algo mejor sería guardar esa información incriminatoria tras una puerta oculta en una estantería.

Porque, por supuesto, tendrás un cuarto secreto detrás de una estantería

¡Ah! ¿Que no tienes? Bueno, dado que eres el único que no lo tiene, vamos a traspasar esos datos encriptados a otro lugar. Por cierto, esas estanterías están a la venta. Yo, en tu lugar, yo compraría al menos dos.

Un truco muy viejo para almacenar información incriminatoria es guardarla en el ordenador de otra persona, preferiblemente sin que lo sepa. Muchos hackers usan esta técnica, ya que les permite hacer que sean otros los que carguen con las culpas a ojos de las fuerzas y cuerpos de seguridad del Estado . Es difícil inculpar a alguien de un crimen si no hay pruebas contra él.

Volvamos con los sicarios, sus perros rabiosos y el helicóptero armado que van camino de tu casa. Antes de que localizaras ese sitio con información especial, habrás encontrado otros que no te interesaron en absoluto; por ejemplo, los tres servidores de "Pañales S.A." que tenían poca seguridad, mucho espacio libre y casi sin uso (Hay un chiste por algún lado en este comentario, créenos)

Volvamos a "Pañales S.A." y démosle un vistazo a su conjunto de servidores. Si algo huele mal, sal de allí pitando. En caso contrario, busca un directorio que se use frecuentemente... o que no se use en absoluto. Ambos tienen sus ventajas e inconvenientes.

En un directorio con actividad podrás crear varios subdirectorios para almacenar tus datos sin que se note mucho la transferencia. El volumen de los datos transferidos no debería disparar ninguna alarma, ya que el directorio principal se usa constantemente. Las malas noticias es que ese directorio puede estar siendo vigilado de cerca porque contiene cosas muy valiosas para la organización. Además, a un lugar con tanta actividad se le suelen hacer backups con regularidad, y no querrás que haya copias extra de tan valiosa información. ¡Son pruebas!

Los directorios inactivos o muertos son sitios muy populares a la hora de esconder datos. Estos pueden haber sido de utilidad para la organización en algún momento.

Ahí es donde podrás crear un laberinto de subdirectorios, o incluso hacer uno oculto. Si eliges hacer el laberinto, hazte un mapa y memorízalo para saber dónde ir cuando navegues por él a la hora de guardar tus datos. La idea es construir un entramado en el que alojar los datos encriptados. Ese entramado debe confundir a cualquiera que localice tu escondite, mientras que tú sabrás donde ir exactamente. Por ejemplo, si construyes un directorio unos niveles por debajo de otros, comienza por añadir subniveles extra. Por cada subnivel, añade más subniveles. El patrón que debes seguir debe ser algo sencillo como "subnivel izquierdo" -> "subnivel derecho" -> "derecha" -> "derecha" -> "izquierda" (5).

Alimenta tu mente: ¿Por dónde comienzan los investigadores forenses?

Si te llaman para acudir a la escena de un delito informático en calidad de investigador forense, tus primeros pasos harán que las pruebas que recojas sean de válidas o no. Analicemos dos ejemplos de crímenes:

En el primer caso, tienes que recuperar pruebas de un ordenador en funcionamiento conectado a la red de la organización. Hay sospechas de que un usuario utilizó este equipo para organizar y cometer un delito contra un competidor. Para recuperar las pruebas no puedes apagar el equipo hasta que hayas generado una imagen de las

memorias volátiles y no volátiles. Debes obtener una imagen del disco de forma que no se altere el contenido del mismo. La parte difícil de esto es: ¿qué hacemos con la red a la que está conectada el equipo? Puede que existan pruebas en los servidores de red, pero no puedes desconectar al resto de usuarios para recuperarlas. La respuesta es ejecutar un análisis en vivo en cada servidor, y analizar las imágenes en otro lugar.

El segundo caso trata de un equipo que ha sido apagado antes de tu llegada. ¿Quién apagó el sistema? ¿Por qué? Si fue el sospechoso ¿cuándo se utilizó por última vez? Aquí es donde se necesita tu experiencia, dado que el sospechoso puede haber utilizado contramedidas forenses.

Con otra clase de dispositivos, como cámaras de vídeo, teléfonos móviles y tabletas necesitarás herramientas especiales y una formación adecuada si quieres recuperar las pruebas. Tu curiosidad y experiencia con dispositivos digitales te ayudarán a comprender cómo se almacenan los datos en cada equipo.

No puedes ir directamente de 'A' hasta 'B'

Sin duda hay una pregunta que te está rondando la cabeza desde hace tiempo:
¿Cómo puedo evitar que mis calcetines huelan tan mal?

Lo sentimos señor P. Estoso, no podemos ayudarte en eso, pero podemos enseñarte a mover grandes volúmenes de información desde tu equipo a "Pañales S.A." sin que nadie se dé cuenta. El protocolo ICMP (Internet Control Message Protocol), un protocolo muy denostado, cuenta con poderes mágicos... si sabemos hackearlo un poco.

Cuando escaneas un puerto estás enviando una petición TCP SYN (layer 4) para ver si este responde. Un ping correctamente ejecutado utiliza ICMP, que no usa puertos. Aunque ICMP está en lo alto del Protocolo de Internet (IP), no es un protocolo de la capa 4. Y esto resulta muy útil cuando tenemos que lidiar con los registros del firewall y del tráfico de la red.

Los firewalls trabajan en varios niveles del modelo OSI, restringiendo o permitiendo el flujo de datos en función de un criterio dado. Cuanta más alta sea la capa de la pila, más profundamente debe inspeccionar el firewall el contenido de cada paquete. En las capas inferiores, el firewall aún puede interceptar y controlar los datos, pero no puede averiguar tanto sobre ellos como hacen las capas superiores. Y aquí es donde los paquetes ICMP entran en escena para hacer cosas muy divertidas.

Esta técnica se conoce como "ICMP Tunneling." Pero antes de poder hacer algo con estas comunicaciones encubiertas, necesitaremos algunas herramientas.

Herramientas

- Wireshark - www.wireshark.org/
- Hping - http://www.hping.org/
- BackTrack www.backtrack-linux.org/

Los paquetes ICMP tienen mucho espacio tras la cabecera para almacenar datos (alrededor de 41k por paquete). La idea es generar a mano paquetes ICMP cargados con tus datos y enviarlos camuflados a través de un túnel ICMP al destino que desees. Puedes generar paquetes ICMP con hping o nping (otra creación de los chicos de nmap) e incorporar la carga al mismo tiempo. Con estas herramientas puedes personalizar el encabezado Ethernet, la cabecera IP y la carga útil.

Cavando el túnel

¿Por qué tendrías que hacer todo el trabajo? ¿Qué tal si hacemos que el servidor al otro lado haga todo el trabajo por ti? Necesitarás establecer un túnel entre tu equipo y el servidor en el que vas a almacenar las cosas. Es el momento de pensar como un hacker.

Ejercicios

8.1 Lo primero que necesitas es aprender cómo funciona esta técnica. Ha llegado el momento de aprender el valor de uno de los recursos para hackers más interesantes que encontrarás en Internet: Youtube. Dada la velocidad a la que se dan los cambios en la web, puede que haya una nueva web de vídeos cuando leas esto, pero es más que razonable pensar que Youtube seguirá siendo tu fuente principal.

Para ver una demostración de cómo funcionan los túneles ICMP, mira este video http://www.youtube.com/watch?v=ADHtjwwkErI

8.2 Un túnel tiene dos lados: el del cliente y el del servidor. Comprobarás que el creador del vídeo prometió publicar el código fuente, pero que nunca lo hizo a pesar de las súplicas de los visitantes.

Necesitarás encontrar el código fuente que, por cierto, ya se ha publicado en Internet. Búscalo. Una pista: el nombre del autor.

8.3 Ahora necesitarás colocar el código de servidor en tu objetivo y ejecutarlo para que funcione. ¿Cómo colocarías ese código en el servidor?

Cuando ambos demonios estén en ejecución conectando ambos hosts, el servidor empezará a hacer sniffing de los paquetes ICMP. Estarás enviando comandos a través del túnel al servidor utilizando ping, y a su vez el servidor te responderá con otro ping. El demonio del servidor comenzará a recoger tus paquetes y a colocar los datos donde le hayas indicado. Si el flujo de datos es grande, el servidor iniciará pings adicionales. Por su parte, el demonio en el cliente recibirá las actualizaciones de la transmisión mediante el mismo tipo de sniffer que estamos empleando en el servidor.

Pasar la pelota

Los discos portátiles son cada vez más pequeños y su capacidad aumenta, lo que te permite esconder fácilmente gran cantidad de datos en su interior; esconde el dispositivo en un lugar seguro lejos de tu casa y tu ordenador. Cuando los sicarios de la mafia y sus perros aparezcan por la puerta, puedes estar seguro de que buscarán en todos los sitios imaginables, incluso en el cajón de la ropa interior. Ten en cuenta que, en su trabajo, estas personas se dedican a entrar y buscar en las casas de los demás como forma de vida. Conocen todos los escondites. Y no le des el dispositivo a un amigo para que te lo guarde: eso, simplemente no sería divertido.

Antes de que empieces a pensar en lugares donde esconder tu tesoro, encripta el dispositivo, los datos o ambos. Prueba con TrueCrypt, www.truecrypt.org

Pon el dispositivo dentro de una bolsa de plástico sellada, para que sea resistente a la intemperie. Usa una pajita para aspirar el aire de la bolsa y reducir tanto la humedad del interior, como el tamaño del paquete. No hagas un agujero en el suelo cerca de tu casa para esconder el dispositivo, porque la tierra suelta resulta sospechosa para cualquiera. En su lugar, busca escondites que se encuentren en alto. Por algún motivo, la gente rara vez busca las cosas en sitios elevados. Asegúrate de que puedes llegar al escondrijo

cuando lo necesites. Utiliza algún método para sujetar la bolsa y evitar que se caiga. Puedes usar precinto, bridas, cordones de zapatos, cuerda o cualquier otra cosa que te garantice que la bolsa no se suelte y se pierda.

Un escondite muy bueno es cualquier lugar cerca de edificios públicos, o incluso dentro de los mismos. Hay escondrijos muy buenos en su interior, pero tienes muchos más en el exterior. Usa tu imaginación, pero actúa con lógica, para pensar donde colocar, cómo recuperar y cómo dejar la zona sin llamar la atención. Tus actividades serán menos sospechosas de día, ya que hacerlo en la oscuridad suele llamar la atención de más personas. Dejar una bolsa a plena luz del día, alrededor de media tarde, no llamará tanto la atención como hacerlo de noche.

Trabajando desde casa

Muchas empresas ofrecen almacenamiento gratuito en la nube sin otro requisito que proporcionar una dirección de correo válida. Algunos sitios como www.Adrive.com te dan 50 GB de almacenamiento en línea gratis. Google, Apple, Microsoft y otros muchos también dan cuentas con almacenamiento de forma gratuita. Estos servicios de cloud, si usas una cuenta de correo de un sólo uso, pueden ser muy útiles para almacenar datos. Todo lo que tienes que hacer es limpiar la caché de tu navegador cada vez que te conectes a ellas, o bien usar el modo "Incógnito" de Chrome, de forma que no dejes huellas de tus visitas en el ordenador. Algunos de estos servicios en la nube te permiten sincronizar los archivos de tu equipo con los que almacenas en línea. Desactiva esta opción y elimina todas las entradas que se refieran a esas cuentas. Es más fácil y seguro examinar tus datos mediante un navegador web, que hacerlo usando la herramienta del cloud.

Siguiente paso – Bocaditos de Bytes

Si tienes una cantidad de datos pequeña, como contraseñas, claves privadas o tu receta secreta para una exquisita sopa, puedes introducirlos en lugares donde no se vean. No intentes esconderlo en tu ADN: ya lo hemos intentado nosotros y como efecto secundario nos hemos quedado con este sentido del humor tan espantoso. Además, ahora tenemos un tic nervioso. Hay mejores formas de hacerlo.

Los autores de Malware saben desde hace tiempo que hay sitio para almacenar cosas en el sector de arranque (MBR) de Windows. No es mucho, pero si el suficiente para esconder una clave privada o una DLL. Por cierto, la fiambrera con tu almuerzo no cabe; ya lo intentamos nosotros.

Intercambia en el intercambiador

Los archivos **Swap** (o archivos de intercambio) son lugares de un dispositivo de almacenamiento que se usan temporalmente como memoria RAM. El archivo swap permite que tu equipo siga funcionando, o que incluso lo haga más rápido, cuando te quedas sin memoria RAM para ejecutar programas. UNIX y Linux utilizan permanentemente un bloque de un dispositivo de almacenamiento para el swap. Incluso si tu ordenador está apagado, el fichero de swap en el disco aún contiene datos de lo que ha ocurrido anteriormente.

Los archivos de intercambio de Windows (**page files**) pueden ser muy grandes y conservar fragmentos de archivos recientes. Esto puede ser aún más peligroso si estás conectado a un servidor Windows. Los servidores Windows almacenan una cantidad muy significativa de datos de los usuarios, que pueden resultar muy útiles a un forense. Dale un vistazo a los directorios "temp" y busca archivos swap.

Tú déjale sitio...

Los archivos se almacenan en **clusters**. Los clusters tienen distinto tamaño, dependiendo del sistema operativo. Si has creado un archivo en tu ordenador, ese archivo puede necesitar sólo el 50% del espacio del cluster. Esto deja al cluster con espacio disponible. Este espacio disponible dentro de un cluster se denomina **file slack** o **slack**. Si borras un archivo que ocupaba parcialmente un cluster, esa información sigue estando disponible.

Ese 50% del espacio del cluster que estaba ocupado por un archivo conservará los datos intactos, y permanecerán allí hasta que otra información los sobrescriba. Windows crea automáticamente slack cuando un archivo se ve, modifica, guarda o se crea.

Reformando archivos

Algunos de los mejores lugares para esconder información es ocultarlos simple vista. "Modificar un archivo" es sólo una forma elegante de decir que le hemos cambiado el nombre, la extensión o sus atributos. A estas alturas del curso, ya sabrás cómo cambiar el nombre de un archivo. Anteriormente creaste un archivo llamado "Planes Malignos"; bien, ahora toca ser algo más creativos. ¿Pondrías todas tus contraseñas en un archivo que se llamase "Passwords"? Por supuesto que no. Nunca debes almacenar tu trabajo en archivos que puedan ser identificados fácilmente.

Cuando buscas archivos modificados, lo primero que compruebas es la extensión. Comprimir archivos es una forma muy sencilla de eliminar pistas y ahorrar espacio, pero es lo primero que comprobará un analista forense. Así que necesitas cambiar la extensión del archivo. Puedes hacerlo simplemente cambiando los tres últimos caracteres del nombre.

Cambiar la extensión .doc de un archivo a .gif es tan sencillo como hacerlo de .odt a .avi. Crear archivos modificados tiene su truco y lleva tiempo. Comprueba el tamaño de los ficheros, fecha de creación y modificación para tener una idea de cómo personalizarlos. Un archivo .odt no debería tener un peso de 1 gigabyte, así como un .avi tampoco debería ser de apenas un par de kilobytes: estos archivos pueden ocupar varios gigabytes.

Comprueba también la fecha de los archivos. Los ficheros que hayan sido creados o accedidos en el plazo de una semana de la comisión del delito harán sonar las alarmas. Modifica esas fechas a cualquier otra que sea, al menos, un año anterior de al hack. Si te quieres divertir un poco, cambia las fechas a valores imposibles, como el 30 de Febrero o el 21 de Marzo de 2112. Tampoco te olvides del "Día de Pi": con esa fecha y hora sabrás quién sabe de matemáticas y quién no.

Ejercicios

8.1 La fecha es 21 de Diciembre de 2012. Mientras estás realizando un análisis forense, localizas varios archivos. Junto a ellos, puedes ver el tipo de fichero y su tamaño. Si continúas investigando, te darás cuenta de que aparece la fecha de cuando fueron abiertos o modificados. Investiga cada uno de los siguientes archivos para ver si alguno resulta sospechoso.

Nombre del archivo	Tipo de archivo	Tamaño del archivo	Fecha de creación	Último acceso o modificación
Passwords.exe	ejecutable	13KB	05/01/08	12/19/12
Vacaciones verano 2012.jpg	Imagen	12948KB	06/01/09	12/19/12
PlanesParaMatarAlJefe.doc.	Documento de word	2KB	12/01/12	12/20/12
Canciones amor.mp3	Música	7985340KB	Desconocido	Desconocido

¿Cuáles de estos archivos te resultan sospechosos?
¿Qué archivos analizarías antes?
¿Cuáles pueden ser un fake?
¿En qué basas tus respuestas para cada archivo?

Muchas veces a lo largo de tu vida te verás en situaciones en las que tendrás claro que usar un martillo te ayudaría a resolver tus problemas con el hardware del ordenador. Una tienda de bricolaje muy conocida vendía hace tiempo un juego de herramientas que llamaron "El juego de herramientas definitivo", que consistía en una caja con diez tipos de martillo diferentes. En el campo forense, los martillos no te ayudarán a resolver ningún caso. Al usar un martillo puedes causar otros problemas, y posiblemente convertirte en sospechoso.

Alimenta tu mente: ¿Qué tipo de pruebas electrónicas reúnen los investigadores?

La clave de analizar dispositivos de almacenamiento es la siguiente: cuando se borra un archivo, en realidad no desaparece. Sigue ahí, en el dispositivo de almacenamiento; sólo se ha borrado la entrada en el sistema del fichero: los datos siguen en la unidad. ¡Con un programa de recuperación de datos puedes leer el espacio no asignado o el de slack para ver qué datos se borraron! Los creadores de software malicioso suelen ocultar sus programas en el espacio de slack. Curiosamente muchos criminales piensan que borrando sus "archivos delictivos" no dejan pruebas de sus actos. La mayoría de ellos ahora se encuentran en prisión.

Cuando estemos realizando una **investigación digital forense**, tenemos que saber dónde mirar, cómo proteger, qué es importante y qué relación tiene con el delito. Estos son los lugares habituales en los que debemos buscar pruebas electrónicas:

Dispositivos

- Equipos de sobremesa y estaciones de trabajo
- Servidores de red
- Ordenadores personales/unidades USB/cdroms/dvds/unidades portátiles
- Laptops, netbooks
- PDAs, tablets, reproductores
- teléfonos móviles/smartphones/hot spots portátiles
- Equipos de fax, fotocopiadoras

Su impresora les delata

Los faxes y fotocopiadoras tienen una memoria interna. Un fax tendrá, normalmente, memoria RAM mientras que las fotocopiadoras dispondrán de RAM y de un gran disco duro. Estas dos máquinas almacenan la fecha y hora del evento junto con otra información. Las copiadoras tienen discos duros que almacenan una copia digitalizada de todos los documentos que han pasado por ella. Hoy en día, las fotocopiadoras pueden escanear, enviar un fax e imprimir, y se encuentran conectadas a la red para ser fácilmente accesibles.

Y todos estos datos se encuentran almacenados en su disco duro interno.

Backups

- Copias de seguridad del sistema (mensuales/semanales/incrementales)
- Copias para usar en caso de desastre (almacenadas en otro lugar)
- Copias personales (busca CDs/DVDs, memorias USB y otros dispositivos similares)
- Cuentas de almacenamiento en la nube

Pruebas digitales

Las pruebas digitales se definen como cualquier información con validez en un juzgado que se hayan almacenado o enviado en formato digital. Se trata de la información recuperada desde dispositivos de almacenamiento, información de la red, o copias de los datos encontrados en una investigación forense. Las pruebas digitales incluyen archivos como:

- Archivos de imagen
- Ficheros de audio y vídeo
- Historial de los navegadores
- Registros de seguridad, eventos y auditoría de sistemas y servidores
- Archivos de Word y hojas de cálculo
- Email
- Registros
- Datos del sistema de un teléfono móvil
- Archivos de registro de Firewall, router, e IDS

Los datos y dispositivos que encuentres como prueba son los mismos que se pueden manipular para ocultarte información.

Finalmente, las pruebas digitales deben cumplir ciertos requisitos para ser aceptadas en un juicio. Estos son:

Admisible: la prueba debe estar relacionada con el acto que se quiere demostrar.

Autentica: la prueba debe ser real y debe estar relacionada con el incidente de forma adecuada.

Completa: la prueba debe demostrar la actividad al completo.

Confiable: la prueba debe probar ser auténtica y veraz.

Creíble: la prueba debe ser clara e inteligible para los jueces.

Pero antes, has de conocer las leyes

Hay requisitos legales que deben cumplirse antes de poder comenzar a recuperar pruebas. Consulta con el departamento jurídico de tu organización, o la legislación vigente en tu país.

Bien: ya es hora de ir poniéndose la ropa de trabajo porque en breve veremos técnicas de ocultación de datos y anti forenses.

El truco mágico de la desaparición de datos (Hacer los datos irrecuperables)

Tras la puerta 1 tenemos una limpieza digital, y tras la puerta 2, la destrucción física del soporte de almacenamiento. Cada opción tiene sus ventajas, pero eres tú el que debe decidir qué método prefieres. A los miembros de Hacker Highschool nos encanta escuchar el sonido que hace un taladro eléctrico mientras perfora un viejo disco duro. Si le añades música a esos sonidos ¡obtendrás un remix increíble! Pero si no soportas ese

sonido o no te gusta ver cómo se destroza el hardware, siempre te queda la limpieza del medio para eliminar los datos no deseados. Es una forma más amable de hacer desaparecer todos esos bits indeseables.

Después de un tiempo de haber estado usando un disco duro, o cualquier otro tipo de soporte de almacenamiento, es posible que haya llegado el momento en el que no te resulta útil. Lo cierto es que es una mala idea tirarlo a la basura o dárselo a otra persona que pueda sacarle partido sin haber eliminado primero esa información. ¿Seguro que quieres que alguien pueda encontrar esa foto tuya del año pasado disfrazado de Batman? ¿Y qué hay de los recibos de tu último trabajo? ¿A que no te gustaría que esos videos caseros que te hiciste bailando en ropa interior terminasen en Youtube? Bien, vamos e eliminar todos esos recuerdos digitales comprometedores del soporte antes de que se lo des a otra persona.

Lavar, aclarar y repetir

Limpiar los soportes es barato (aunque no es muy divertido) y te permite destruir de forma segura los datos sensibles. Puedes borrar esos datos, eliminando esos bits de la faz de la tierra, usando software libre. Una de las formas más sencillas de encriptar el soporte es usar True Crypt. Cuando tengas completamente encriptado el dispositivo de almacenamiento puedes tirarlo a la basura. La razón de esto es que esa información no puede descifrarse a menos que tengas la contraseña. Sencillo ¿no? Si esos ochenta y cinco sicarios le ponen las manos encima a tus viejos soportes, les resultarán inútiles dado que tú eres la única persona del mundo capaz de desbloquear la información. Si otra persona se hace con esos soportes, no le quedará más remedio que reparticionarlos y formatearlos de nuevo para poder usarlos.

Grosso modo hay dos estándares para asegurar una destrucción adecuada de los soportes. El primero de ellos es emplear US DOD 5220.22-M, y el otro el algoritmo de Gutmann. El DOD 5220.22 es parte del documento "*US National Industrial Security Program Operating Manual*" y contiene instrucciones acerca de cómo destruir los datos. Al Departamento de Defensa de EE.UU. también le gusta destruir cosas, así que sólo admiten y autorizan la destrucción completa como mecanismo para eliminar datos.

El algoritmo de Gutmann, que recibe este nombre por el Dr. Peter Gutmann y Colin Plumb, es algo distinto a la destrucción del hardware. Este algoritmo consiste en escribir en el soporte treinta y cinco patrones específicos. Distintas unidades precisan de distintos patrones. Aunque este método es una técnica excelente de investigación del backend, en la actualidad es obsoleta debido al tamaño de las nuevas unidades de disco y a las configuraciones de los controladores integrados.

Más herramientas software

En la comunidad de software libre existen herramientas excelentes que conseguirán que tus datos sean imposibles de recuperar. El software no dañará el medio de soporte, pero hará que los datos almacenados sean irreparables. Cuando ejecutes el programa y pulses el botón "start", ya puedes despedirte de ellos: no volverás a verlos nunca. Ni siquiera en el más allá.

Boot and Nuke

http://www.Dban.org

Boot and Nuke se distribuye como una imagen ISO para grabar en un CD, y que utilizarás para iniciar tu sistema. Una vez que el software esté en ejecución, solamente tendrás que seleccionar qué disco quieres limpiar (Nuked). Dban es un estándar industrial para la destrucción masiva de datos y situaciones de emergencia. Una vez que hayas usado Dban en una unidad, no hay recuperación posible. Los datos han desaparecido ¡Hasta nunca!

Eraser

http://sourceforge.net/projects/eraser/files/latest/download

Este programa sólo funciona en Windows. A pesar de que desde Windows Vista se tiene la posibilidad de formatear y escribir "1" en todo el dispositivo, Eraser formatea la unidad y escribe datos aleatorios en ella varias veces. El programa ejecuta el proceso de formateo y escritura repetidamente hasta que se complete el patrón.

Sderase

http://sourceforge.net/projects/sderase/?source=directory

SD es un recién llegado al campo de la limpieza de discos, y su primera versión apareció el 28 de Agosto de 2012. El autor del programa hace un interesante comentario en su web: SDerase afirma que cumple con los requisitos de limpieza de datos descritos en la norma US DOD 5220.22-M. Pero según esta normativa, el único método aceptable para eliminar los datos de un dispositivo es su destrucción física. Aún está por ver si hay algún software capaz de hacer eso.

Martillear, taladrar y machacar

Sólo existe un mecanismo que ha resistido el paso del tiempo a la hora de hacer desaparecer la información; un método en el que todos los expertos están de acuerdo en considerarlo como el más eficaz: la destrucción física del medio. Aplástalo, golpéalo, tritúralo o destrózalo. Usa tu imaginación para encontrar formas de destruir el soporte. Un imán sólo afectará a materiales magnéticos, así que si colocas un altavoz sobre una unidad flash será inútil. El soporte no podrá parar de reírse de ti hasta que, tras unos momentos de espera, aparezcas con un martillo.

Un típico martillo de carpintero puede hacer bastante daño a cualquier objeto sólido que golpee. Un martillo de mayor tamaño causará daños mayores, ¡y es más divertido! Pero ten cuidado de no machacarte un dedo. Una piedra puede hacer el mismo trabajo que un martillo, tanto en un soporte de datos como en tus dedos. Y además, visto desde el punto de vista del Retorno de Inversión (ROI, en inglés), una piedra es bastante más barata, aunque puede que tengas que ir renovándola conforme pasa el tiempo.

Así mismo, un taladro eléctrico equipado con una broca grande puede dar excelentes resultados en una demolición. La mejor forma de destruir algo con un taladro es hacer varios agujeros en distintas partes del soporte de almacenamiento.
Hay algunas medidas de seguridad que debes seguir a la hora de usar un taladro:

- Usa gafas de seguridad, u otra medida de protección equivalente para los ojos.
- Ni se te ocurra sujetar el soporte en tu regazo mientras lo taladras.
- Tampoco lo sujetes en la mano mientras lo perforas.
- No le pidas a un amigo o familiar que te lo sostenga en las manos o entre las piernas mientras lo taladras.

- Para evitar dañar el taladro o la broca, coloca unos cartones o tablas de madera bajo el soporte de almacenamiento antes de empezar a taladrar.

Una vez hayas terminado de transformar el soporte de almacenamiento en un montón de piececitas, lo siguiente que debes hacer es tirar los restos repartiéndolos entre varios cubos de basura. Busca un tirachinas y practica tu puntería disparando a latas vacías con los fragmentos. O crea una obra de arte con lo que te quede. Existen toda clase de formas de repartir pequeños fragmentos en un área extensa. ¡Y es divertido!

Planta un jardín

Para sobrevivir en este trabajo tienes que ser un poco paranoico. Bueno, en realidad bastante paranoico. Estar alerta y hacer planes para el futuro siempre es una buena idea y no debes tomártelo a la ligera (este consejo también es válido si quieres jubilarte anticipadamente). En el mundo real, dejamos cabellos, fibras de nuestras ropas, huellas dactilares, pisadas y otras pruebas de nuestra presencia. Pero al contrario que en el mundo real, es posible estar en un mundo digital, jugar en el durante un rato y salir sin dejar ni una sola huella. Piensa en cómo puede usarse esto para bien o para mal, y lo peligroso que puede ser estar en el lado equivocado.

Más adelante explicaremos el proceso completo, pero por ahora nos centraremos en esconder tus huellas. En las redes existen dos clases de dispositivos. El primer tipo es, básicamente, un dispositivo "tonto", lo que significa que no mantiene un registro de actividades. Algunos de esos dispositivos tontos son los switches, hubs, bridges, y similares: sólo saben hacer aquello para lo que están diseñados y nada más.

Por otra parte, también tenemos dispositivos "inteligentes" que mantienen registros de ciertas actividades y pueden tomar decisiones en base a los filtros y configuraciones que tienen instalados. En esta categoría se encuentran los firewalls, routers, extensores de rango, servidores, y todo el hardware de red que mantenga un registro del flujo de datos. A estos son a los que hay que prestarles atención porque son los que monitorizarán, grabarán y posiblemente interrumpirán tu hack. Estos obstáculos en la red se describen más detalladamente en otras lecciones de HHS.

Necesitas saber cómo enfrentarte a estos dispositivos para ocultar tus huellas y, si es necesario, despistar a esos ochenta y cinco sicarios. Establecer una "línea de tiempo" puede ser muy útil para tus planes. Te permitiría planificar cuanto tiempo estarás en esa red y minimizar las probabilidades de que te pillen, controlando el tiempo que estarás expuesto.

Sembrando el jardín

Tendrás que pensar en varias formas de cubrir tus huellas antes de salir de la red que atacas. Si sólo conoces una forma de hacerlo, como borrar los registros del sistema, te estas exponiendo a ser detectado por otros métodos. Borrar los registros del sistema puede parecer una idea estupenda pero ¿qué pasa si existen registros redundantes escondidos? ¡Ups! Tenemos que emplear varias líneas de acción que se complementen entre ellas pero que no interfieran con tus planes. Piensa en esto tanto desde el punto de vista del investigador... como del agresor.

Sembrar bombas lógicas es algo que se usa desde hace tiempo por proveedores subcontratados que no han cobrado por su trabajo, administradores furiosos, y gente que no anda muy bien de la cabeza. Todos ellos colocan bombas lógicas donde se pueda provocar el mayor daño posible a la información. No es que sea precisamente una buena idea destruir una red de datos al completo si quieres pasar desapercibido tras

penetrar en ella. Una bomba lógica que sólo elimine o corrompa los registros del sistema, y se active cuando se realice una auditoría, u horas o días después de haber salido, funcionará muy bien para cubrir tus huellas y no alarmará a mucha gente.

CCleaner (http://www.ccleaner.com/) es un programa gratuito de Windows que resulta muy útil tanto para usuarios domésticos como en empresas (al principio se llamaba "Crap Cleaner", el "Limpia mierda", pero sus autores tuvieron un momento de lucidez y decidieron que necesitaban un nombre algo más respetable). Con esta herramienta de 332 KB, puedes seleccionar qué archivo de logs quieres editar o borrar de cualquier máquina en la que tengas privilegios de administrador. Incluso puedes limpiar el historial de navegación y borrar tus huellas una vez que haya concluido tu trabajo. CCleaner intentará crear un punto de restauración en el sistema antes de cambiar nada. Tus opciones son permitirlo o no, aunque si lo haces siempre puedes buscar en el directorio raíz del disco una carpeta con un nombre similar a "cc_20110928_203957". Elimina este archivo antes de desconectarte, incluso si este se encuentra en tu unidad.

Los Root kits ocultan la actividad, y son muy útiles en sistemas basados en Linux, que no tienen demasiados agujeros de seguridad.

Alimenta tu mente: Principios de la Ciencia Forense Digital

Como en otros campos de la ciencia, la forense digital se basa en métodos bien definidos, que se ocupan fundamentalmente de mantener las pruebas intactas. Tiene su lógica: si pierdes el control de la prueba, aunque sólo sea un minuto, ya no sirve porque puede haber sido alterada.

Los archivos de datos pueden alterarse sin aparentarlo. Es muy fácil cambiar la hora, la suma de control y la fecha del último acceso cuando alguien haya editado un archivo o registro. Una de las tareas más importantes de un investigador forense es demostrar que la prueba adquirida no ha sufrido modificaciones en forma alguna. Básicamente, tendrás que demostrar que no le ha ocurrido nada a los datos cuando los recogiste, analizaste, y que además los custodiaste todo el tiempo.

Por eso es importante utilizar procedimientos seguros para recopilar, inspeccionar y trabajar con los datos. Un pequeño error puede hacer que tu trabajo resulte inútil. Aquí es donde entran juego las técnicas de confianza. Llevar a cabo cada investigación de la misma forma y usar los mismos procedimientos para documentar tus acciones es lo que te permitirá demostrar que nada ha alterado las pruebas.

Metod

La trata
sob e. Esto
imp estar
fisg ostrará
los

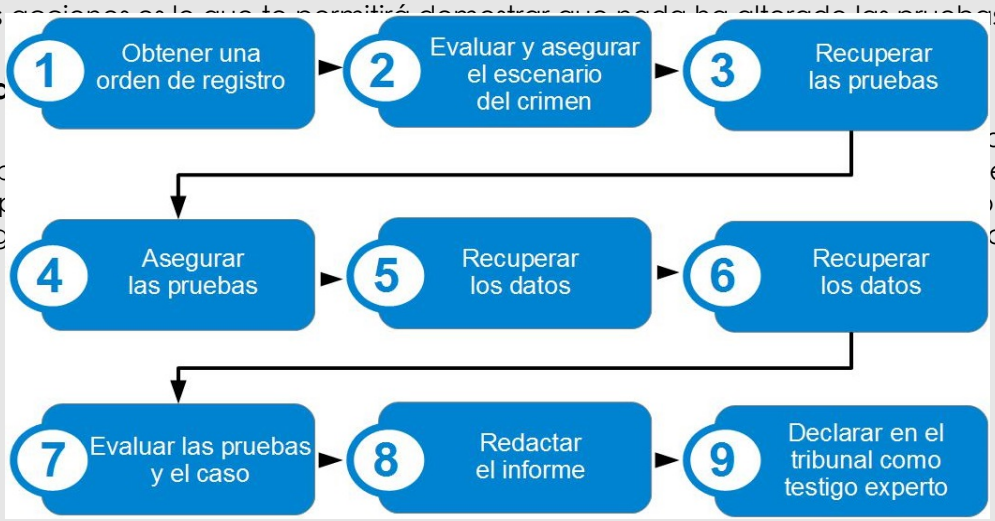

Figura 8.1: Método para forenses digitales

Proceso digital forense

Cuando estés investigando un delito informático, tendrás que fundamentar tu trabajo en un proceso, con una política, procedimientos y listas de comprobación. Tu procedimiento forense debe ser reproducible y soportar el análisis de otro experto. Tendrás que desarrollar un proceso de investigación que precise de documentar continuamente cada acción que se realice sobre las pruebas. Si algo no está documentado, nunca ha ocurrido.

Un ejemplo de esto:

1. Identificación de las pruebas (debe estar documentado)
2. Recuperación de las pruebas (debe estar documentado en la cadena de custodia)
3. Conservación de las pruebas (debe estar documentado en la cadena de custodia)
4. Análisis o interpretación (por supuesto, documentado)
5. Comunicación de tus hallazgos y documentación

Posiblemente, el documento más importante sea la **Cadena de custodia**, que debe indicar claramente qué se recuperó como prueba, por quien y a quien se le entregó en custodia. Perder la custodia de la prueba, aunque sólo sea por unos minutos, hará que la prueba no tenga validez legal.

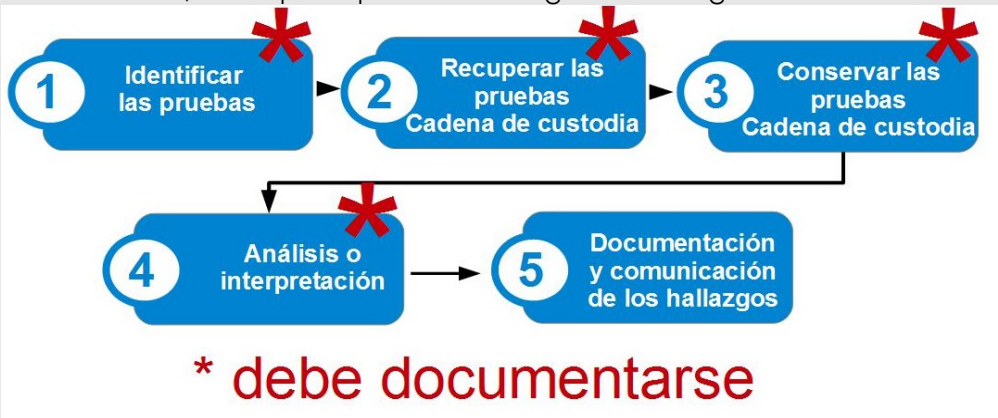

Figura 8.2: Proceso Digital forense

¡Las pruebas se pierden constantemente!

No dejes que todo tu trabajo sea vuelva inútil porque una parte vital de la información no fuera etiquetada o no se siguiera correctamente la cadena de custodia. Al contrario que tus profesores, los jueces nunca aceptarán que te disculpes por perder una prueba diciéndoles que "el perro se comió mis pruebas"

Aunque por otra parte, el que se pierda una prueba puede ser fantástico para alguien: depende de la perspectiva.

Ejercicio exclusivo para agentes de los cuerpos de Policía

Los expedientes criminales se almacenan en servidores locales, los cuales se encuentran en distintas comisarías de policía, y cuentan con una copia de seguridad que se aloja en alguna subestación de policía. En la base de datos principal existen varios subtipos para catalogar la información. Es en estos subtipos donde se guarda la información obtenida en las investigaciones diarias, información sobre los criminales (órdenes de arresto, delitos recientes) o resultados de las pruebas forenses.

En todos los sistemas de las fuerzas y cuerpos de seguridad, como el FBI, no existe forma alguna de conectarse a través Internet, aunque las estaciones de trabajo sí pueden hacerlo. Los enlaces de comunicaciones están disponibles usando estaciones de trabajo dentro de los edificios de la policía, con un sistema de privilegios que se conceden según las necesidades del trabajo. Además de esto, los coches de policía cuentan con ordenadores portátiles cifrados para las comunicaciones a distancia. Estos ordenadores de a bordo son muy potentes y tienen acceso a la mayoría de las bases de datos policiales y a Internet.

Estos equipos permanecen conectados incluso cuando el motor del coche está apagado, aunque sólo sea por breves instantes. En Estados Unidos de América, las comunicaciones se llevan a cabo mediante redes de datos inalámbricas que trabajan según la "Sección 90: Comunicaciones públicas y privadas de estaciones de radio terrestres (LMR) de dos vías operando en banda ancha (25 kHz) para la transmisión de voz o datos; control o transmisión de datos por sistemas de radio en las frecuencias 150-174 MHz (VHF) y 421-512 MHz (UHF)".
La FCC ha ordenado que estas frecuencias deben migrarse a tecnología de banda estrecha (12.5 kHz o inferior) antes de Enero de 2013.

Ejercicios

8.2 Este cambio a banda estrecha está teniendo un coste económico bastante alto para muchos cuerpos de seguridad, ya que la mayoría de ellos había comprado sistemas de radio con saltos de frecuencia. Estos sistemas permitían que las emisoras "saltaran" a otras frecuencias, haciendo bastante difícil interferirlas o escucharlas. Cada radio se configura pasa "saltar" en base a una emisora principal (o Master) y un tiempo alrededor de tres segundos. Cuando una radio esclava (o Slave) se sincroniza con la Master, todas las transmisiones se escuchan a la perfección, incluso en aquellos modelos que cambian de frecuencia 70 veces por minuto. El pasar a banda estrecha elimina esta posibilidad, ya que las radios se encuentran limitadas al uso de un par de canales. ¿Puedes averiguar cuáles son las frecuencias de la zona donde vives? Pero antes de hacer nada, asegúrate de que obtener esa información sea legal donde vives. ¡No te gustaría aprender esa lección por el lado difícil!

Los cuerpos de policía tienen contratos de servicio público con los principales proveedores de telefonía móvil, para cubrir todas las zonas bajo su jurisdicción. Las frecuencias de radio son las mismas que utilizan para los datos tus dispositivos móviles, EDGE, 2G, 3G, and 4G LTE. La diferencia está en que los datos transmitidos emplean el cifrado SSL entre los servidores y los equipos portátiles. Hay programas como Snort y Wireshark que permiten capturar fácilmente los paquetes de datos, sin embargo, el sistema que quieras espiar debe estar quieto... o en el coche del mafioso al que investigas. ¡Y necesitas una autorización judicial para poder hacerlo!

Los criminales lo saben y por eso utilizan los mismos sistemas para que a la policía le resulte más difícil detenerlos.

Anteriormente hablamos acerca de cómo ocultar tus cosas cerca de edificios públicos. Hay una buena razón por la que los criminales suelen "pasar el rato" en los alrededores de los estacionamientos de la policía, donde están aparcados los patrulleros. Es un sitio perfecto para capturar paquetes de datos con las credenciales de acceso. Cuando alguien prepara un coche policía para salir a patrullar, el ordenador de abordo tiene que autenticarse y sincronizarse con los servidores. Esto ocurre en cada cambio de turno, dado que cada policía está relevando a otro policía. Pero lo que ellos no saben es que los alrededores están fuertemente vigilados, e incluso cuentan con sistemas de **Jamming** para impedir que, desde cierta distancia, puedan interceptarse los datos. Más de un delincuente ha aprendido la lección desde su nueva residencia habitual para los próximos años... y ya puedes imaginarte de lo que estamos hablando ¿Sabes lo que es el Jamming? Investiga un poco sobre este asunto: te encantará.

Un nuevo añadido a los equipos portátiles es la VoIP. El propósito principal es impedir que los malos y los reporteros chismosos intercepten las transmisiones de radio. Pero la VoIP es un sistema que también tiene sus vulnerabilidades.

Estar lejos de casa: cuando lo profesional se mezcla con lo personal

Una de las mayores debilidades que encontramos en la comunidad de las Fuerzas y Cuerpos de Seguridad es el uso que hacen del correo, tanto cuando están de servicio como no. Usar el teléfono del trabajo para hacer llamadas personales, enviar correos a sus cuentas particulares, entrar en Facebook y otro tipo de comunicaciones diluyen la línea que separa lo profesional de lo personal. Los agentes del FBI se llevan trabajo a casa con frecuencia, y los policías suelen hacer lo mismo. Tener acceso a la información del trabajo dentro y fuera de la oficina es sencillo para cualquier persona capaz de hacer clic con el ratón.

Piensa en esto: la mayor parte de los nombres de usuario de correo son una combinación del nombre y apellidos, separados por un punto y seguidos por el nombre del organismo. Algo así como nombre.apellidos@policía.gov. Por ejemplo, supongamos que quieres contactar con el agente Dean Martin del Departamento de Policía de Nueva York. Su dirección de correo sería D.Martin@troopers.ny.gov. Todos los departamentos de policía muestran su URL en su sitio web, normalmente en las secciones "Contacto" o "Reclamaciones".

En muchos casos, la primera parte de la dirección del correo será el nombre del agente. Esto resulta muy útil para compartir información abiertamente entre departamentos de los cuerpos de seguridad. Pero una vez que hayas conseguido acceder a una de las cuentas de correo, será muy sencillo interceptar las comunicaciones y acceder a la base de datos que contiene las investigaciones en curso.

El problema sería cómo acceder a las bases de datos. Este tipo de accesos está muy controlado, se concede sólo a determinados departamentos y siempre según las necesidades que requiera la investigación que lleve a cabo un oficial. Si alguien se conectara como si fuera un agente e intentase acceder a una sección de la base de datos a la cual el investigador no tuviera acceso, saltarían las alarmas. Todo esto entra en la fase de reconocimiento de un hack: aprender todo lo que puedas acerca de quien está haciendo qué con el caso.

Existen muchas versiones de distribuciones Linux especializadas en seguridad y análisis forense disponibles en Internet. Te recomendamos visitar **www.securitydistro.com** y probar algunas de ellas. Pero antes de probar los kits que vienen en ellas, lee detenidamente la documentación. Cada paquete de software incluye herramientas muy potentes que, mal configuradas, pueden hacerte pasar un mal rato. Ten cuidado, se educado y nunca

olvides que tus acciones pueden tener consecuencias nada deseables sobre otras personas. Algún día TÚ puedes ser la "otra persona", y debes estar preparado por si se da el caso.

Herramientas y colecciones de software

Las herramientas libres u Open Source más comunes para análisis forense y pruebas de seguridad que incluyen esos kits son:

- **Kali Linux** (www.kali.org/)
- **Sleuthkit** (www.sleuthkit.org)
- **Katana** (sourceforge.net/projects/katana-usb/)
- **CAINE** (www.caine-live.net/)
- **Wireshark** (www.wireshark.org/)
- **DEFT** (www.deftlinux.net/)
- **HELIX**(https://www.e-fense.com/store/index.php?_a=viewProd&productId=11)

Ejercicios

8.3 Elige alguna de las distribuciones de software forense que te hemos presentado antes. Sigue las instrucciones para grabar un "Live CD". Estos discos te permiten arrancar el ordenador y cargar ese sistema operativo sin necesidad de tener que utilizar aquel que tengas instalado en el equipo.

8.4 A continuación, haz una memoria USB arrancable con el mismo software forense. Recuerda que estas herramientas se ejecutan bajo muchas distribuciones de Linux, así que no tienes que preocuparte por la compatibilidad con el sistema operativo que estés usando en el equipo de prueba.

8.5 Dale un vistazo a las herramientas y lee la documentación. Mientras lo haces, monta tu disco duro e intenta recuperar algún archivo que puedas haber borrado recientemente. Una vez que lo hayas hecho, renómbralo a "Planes malignos" manteniendo la extensión original. Usaremos el archivo "Planes malignos" un poco más adelante.

8.6 Gran parte del software incluido dispone de una Interfaz gráfica de usuario (GUI), mientras que otros funcionan en línea de comandos. Fíjate en cómo los switches (/s) al final de cada comando constituyen por si mismos unas herramientas muy potentes.

Análisis de los soportes de datos

Los investigadores forenses emplean diversas herramientas para analizar y recuperar datos en distintos soportes. Hay dos motivos fundamentales para realizar un análisis forense: para reconstruir un ataque después de haberse producido, y para examinar un dispositivo que podría haberse utilizado para cometer un crimen.

El primer paso antes de proceder al análisis de cualquier dato es realizar una imagen exacta de la prueba y trabajar exclusivamente con ella. Las herramientas que mencionamos antes permiten a los investigadores realizar las siguientes tareas... y muchas otras más:

- Buscar texto en los espacios de archivo, de slack y no asignados de un dispositivo físico.
- Encontrar y recuperar datos de ficheros que han sido borrados u ocultados.
- Encontrar datos en archivos encriptados.
- Reparar tablas de partición FAT (FAT16, FAT32, eFAT) y sectores de arranque.
- Recuperar datos de particiones NTFS dañadas (Si Windows no puede hacerlo, Linux es capaz de recuperarlos casi siempre)
- Unir y dividir archivos.
- Analizar y comparar ficheros.
- Clonar dispositivos que contengan datos.
- Hacer backups e imágenes de datos.
- Borrar de forma segura ficheros confidenciales.
- Editar archivos con un editor hexadecimal.
- Crackear ciertos tipos de archivos y directorios encriptados.
- Cambiar los atributos de los ficheros, o eliminar permisos restrictivos (como "read" or "write only")

La hora de la cita

Llegar a tiempo... con Offset

El momento en el que sucedió el evento es fundamental, y por tanto también lo es la necesidad de registrar la **diferencia** (offset) de tiempo entre la hora en la que se obtuvo la prueba y la hora atómica (¡no te olvides de la zona horaria!). Normalmente esto se hace DESPUÉS de salvaguardar la prueba, ya que esto implica volver a iniciar el sistema.

Conocer cuando tuvo lugar (o no) un determinado evento es algo crucial que debe establecerse para todas y cada una de las pruebas. Si un sospechoso declara que "nunca envió un email con amenazas" a la víctima, tu trabajo consistirá en localizar ese correo y confirmar cuando se envió y por quién. A lo largo de esta lección vamos a repetir esta idea hasta que creamos que la has escuchado suficientes veces. Y luego la repetiremos una vez más, sólo para estar seguros de que estás harto de escucharla.

Datos EXIF

Las fotos digitales se codifican con unos **metadatos** llamados EXIF, o *Exchangeable File Image File Format*. El objetivo original de usar EXIF era facilitar a los fotógrafos información precisa de cada foto, como la velocidad de obturación, balance de color, o la fecha y hora en que se tomó cada foto. Esa increíble cantidad de información contendría aún más datos si la cámara tuviera el GPS activado, incluyéndose los servicios de localización.

La mayoría de las cámaras que incluyen esta información de rastreo son de teléfonos móviles. Y estas cámaras incluyen en los datos EXIF información personal, como el nombre del usuario; si el GPS estaba activado, en los datos EXIF se incluirán las coordenadas del lugar en el que se tomó la foto.

Por supuesto, esa información puede falsificarse, pero pocas personas comprueban primero esos datos. Y una foto publicada en una red social puede ser suficiente para localizar al sospechoso.

Herramientas para imágenes

Al igual que ocurre con los discos duros, a cualquier soporte de datos que pudiera ser una prueba se le debe sacar una imagen y almacenarla, de modo que tu análisis se realice exclusivamente en esta. Nunca deberías trabajar directamente sobre las pruebas originales, ya que hacer esto podría alterar la información en el soporte. Todas las herramientas forenses que te mencionamos antes pueden sacar una imagen de la mayoría de soportes. Si tu ordenador para análisis forense puede leer el soporte, estas herramientas podrán sacar una imagen de él.

Calcula el hash para garantizar que la imagen binaria es una copia exacta bit a bit del original. Obtén el hash del original, crea la imagen y calcula el hash de esta última. Si los dos hash son iguales, entonces tienes una copia exacta. Todo esto puede hacerse con el mismo software que vimos antes. No tiene sentido trabajar con una imagen que no sea exactamente igual a la prueba original.

¡Trata de arrancarlo!

El arranque es el proceso en el cual un pequeño programa inicia el sistema operativo instalado en un ordenador o dispositivo de arranque. Parte de este proceso incluye comprobar el sector de arranque para encontrar dónde se encuentra el sistema operativo. Las unidades USB también pueden ser dispositivos de arranque tal y como lo son los CD, DVD, ZIP, tarjetas flash e interfaces de red (mediante PXE).

El que un CD/DVD/USB (u otro soporte) tengan el apellido "live", significa que el dispositivo es capaz de arrancar el ordenador. En tanto la BIOS del ordenador permita arrancar desde otros dispositivos, estos soportes pueden contener toda clase de sistemas operativos, incluyendo máquinas virtuales o arranque dual.

La capacidad de arrancar desde distintos tipos de soportes permite que un atacante arranque un ordenador con su propio sistema operativo y almacene en el soporte todas las pruebas que desee. Este tipo de arranque no dejará pruebas de su actividad en el ordenador de la víctima y hará que tu trabajo sea más difícil.

Datos borrados

Un asesino intentará deshacerse del cadáver y el arma empleada tan rápidamente como le sea posible tras cometer el crimen. Además, querrá destruir todas las pruebas que puedan relacionarle con el homicidio. Un sospechoso de cometer un delito informático hará exactamente lo mismo. Las pruebas digitales pueden eliminarse rápida y fácilmente si el sospechoso sabe lo que está haciendo.

No te tomes esto como una invitación a cometer "el crimen perfecto". Te garantizamos que tal cosa no existe: terminaríamos por saberlo y tendrá consecuencias.

Para eliminar los restos de archivos eliminados, en Linux se utiliza el comando **dd**

```
dd if=/dev/zero of=/home/filename
synch
rm /home/filename
synch
```

Para borrar archivos y eliminar los restos de estos en Windows:

1. Abre el explorador, selecciona los archivos o ficheros y pulsa la tecla "Supr".
2. Borra todos los archivos del directorio temporal, o usa un software como CCleaner.
3. Una vez que se han eliminado los archivos, selecciona la Papelera de reciclaje.
4. Haz clic con el botón derecho en la papelera, y selecciona "Vaciar papelera de reciclaje"
5. En "Sistema", crea un nuevo punto de restauración y borra los puntos anteriores que pudiera haber.
6. Reinicia.

CCleaner te permite seleccionar que archivos de log quieres borrar o editar en cualquier máquina en la que tengas privilegios de administrador. Un sospechoso puede incluso borrar el historial de navegación para eliminar sus huellas una vez que haya terminado con su trabajo. CCleaner intentará crear un punto de restauración del sistema antes de modificar nada. Tus opciones son no permitir crear ese punto de restauración, o buscar un archivo en el directorio raíz con un nombre parecido a "cc_20110928_203957". Un sospechoso eliminará ese archivo antes de salir, incluso si se encuentra en un disco duro portátil.

Alimenta tu mente: un vídeo puede absolverte... o condenarte

¿Una videocámara podría resolver un crimen y, a la vez, ser parte de otro? Si.
El 5 de Agosto de 2012 dos turistas chocaron con sus motos de agua en Waikiki, Hawaii. El accidente mató a una chica de 16 años de California. La policía de Honolulu tenía dificultades para conseguir pruebas dado que sólo había unos pocos testigos. Uno de los pilotos declaró que estaba sentado en su moto y que no vio a la víctima hasta el incidente.

Pero otro testigo declaró a la policía que alguien tenía una cámara de vídeo y estaba filmando la escena cuando ocurrió todo esto. La cámara estaba siendo utilizada por la novia del perpetrador, grabando a su novio en la moto de agua.

Cuando la policía de Honolulu consiguió la cámara de vídeo, se encontraron con que el video del incidente había desaparecido. El análisis forense recuperó el fragmento de vídeo borrado, en el cual se veía al novio conduciendo la moto de forma peligrosa y temeraria, pilotando de pie y acelerando cuando golpeó a la fallecida por detrás.

La novia admitió más tarde que había borrado el vídeo para sacar a su novio del problema. El sospechoso se declaró "No culpable" de los cargos, mientras que su novia está acusada de "manipulación de pruebas" y "obstrucción a la justicia".

Formateo de soportes

La mayoría de los soportes de datos necesitan formatearse antes de poder ser utilizados con un sistema operativo en concreto. Por lo general, el formateo destruye toda la información que estuviera almacenada en el dispositivo. Si alguna vez te encuentras con un disco duro u otro dispositivo que haya sido formateado recientemente, puede que este contuviera información que el sospechoso quisiera hacer desaparecer. Pero con las

herramientas que te hemos indicado antes, tendrás la posibilidad de recuperar los archivos y carpetas de ese soporte.

Existen algunos programas que formatean los soportes, escriben datos al azar en ellos, vuelven a formatear y así tantas veces como quieras. Bajo estas condiciones tan extremas, resulta bastante difícil recuperar los archivos y carpetas. La clave para recuperar algo está en descubrir el evento y recuperar el soporte lo más rápido posible.

Precauciones a tener en cuenta cuando recopiles pruebas de un soporte de datos.

Estas son las reglas que debes seguir cuando te encuentres en el lado de "los buenos": es decir, cuando tengas que recuperar información para un análisis forense. Esta vez no necesitarás un martillo o un taladro: tendrás que ir con cuidado y procurar no romper nada.

- Sostén el soporte por los bordes para evitar arañarlo o dejarlo caer.
- Usa rotuladores no permanentes para escribir en la prueba.
- Almacena las pruebas en una bolsita hermética y etiquétala.
- Ten mucho cuidado cuando trabajes con soportes que estén rotos o dañados.
- No limpies con agua el soporte para eliminar el polvo, grasas o aceites: usa siempre guantes.
- No uses ningún tipo de limpiador con base orgánica o de petróleo cerca de la prueba.
- Haz una imagen del dispositivo y trabaja con ella para evitar dañar los datos originales.

Ejercicios

8.7 Mientras estás analizando una tarjeta XD de 4Gb de un sospechoso, te das cuenta de que en la misma sólo aparece una partición de 2.5 Gb... y nada más. En esa tarjeta encuentras fotos familiares, documentos corrientes y otros datos sin importancia. Pero te das cuenta que hay un archivo encriptado con un cifrado AES de 192 bits en una carpeta llamada "fotos de los niños"

¿Por qué la tarjeta sólo tiene espacio para 2,5 Gb cuando debería tener 4 Gb?

¿Te preocupa que haya un archivo encriptado en esa carpeta tan extraña?

¿Qué sabes de AES, y qué te indica un cifrado de bloques de 192 bits? ¿Es importante para la investigación?

¿Puedes crackear ese archivo?

Esteganografía: Una mirada a las controversias de la seguridad

El tema de la esteganografía te dará una oportunidad de ver lo diferente que pueden llegar a pensar los expertos en seguridad. Es totalmente viable transferir datos de manera secreta; consiste, simplemente, en que no sean encontrados en "estado salvaje". ¿Hay alguien utilizando estas cosas?

Esteganografía: Es real, es fácil y funciona

Cuando estás haciendo investigaciones como forense digital, no es suficiente con recuperar fotos, documentos, vídeos, audio y datos VoIP contenidos en un medio de almacenamiento sospechoso sin probar también a buscar alguna prueba sobre cualquiera rastro potencialmente oculto como por ejemplo la estegonagrafía. Mientras que una imagen puede parecer una imagen inocua, puede contener una gran cantidad de información oculta.

La esteganografía, a veces llamada **stego**, es la capacidad de esconder información en comunicaciones sin que nadie sea capaz de detectar algún cambio o modificación del objeto original sin el uso de herramientas software especiales. Por ejemplo, una imagen conteniendo un mensaje oculto por esteganografía puede parecer idéntico para un espectador ocasional y no proporciona indicios obvios de que se haya hecho alguna modificación en la original. Aunque es parecido a cifrar, ya que la esteganografía se usa para esconder objetos y datos, la esteganografía no debe confundirse con la criptografía. La esteganografía inserta información en cosas como documentos o imágenes mientras que la criptografía cifra la información usando un cifrado o una clave de cifrado que es usada para codificar y decodificar el mensaje.

En un caso reciente, el FBI detectó y empleó la esteganografía en una de sus investigaciones. Diez criminales especializados en stego fueron deportados a Rusia como parte de un intercambio rutinario de espías. Puedes leer más sobre ello aquí:

http://www.reuters.com/article/2010/07/08/us-russia-usa-spy-idUSTRE66618Y20100708

La esteganografía usa muchas técnicas distintas, desde la inserción de datos hasta técnicas algorítmicas, pero para hacer el concepto más fácil de entender diremos que la esteganografía inserta datos dentro de un fichero anfitrión, de tal forma que se cambie de una manera poco obvia, y que será distribuido a otras personas las cuales podrán reconstruir el mensaje oculto contenido en ese archivo. Aunque las ímágenes (los mapas de bits) en particular son la forma más comúnmente usada como ficheros anfitriones, también se pueden utilizar archivos de audio, vídeos o documentos.

Hay más de 600 herramientas conocidas para la creación y la detección de esteganografía disponibles en Internet. Pero incluso con todas esas herramientas, una persona que esté entrenada en el uso de editores hexadecimales puede detectar rápidamente ficheros anfitriones de esteganografía si cuenta con una biblioteca de imágenes originales, documentos, vídeos y ficheros de audio con los cuales pueda comparar los ficheros sospechosos. La esteganografía también está enfocada al uso de firmas de esteganografía de un modo parecido a las detecciones de los antivirus como puede ser la comparación de los valores de resúmenes hash. Algunos valores de resúmenes hash están disponibles en sitios como por ejemplo http://www.hashkeeper.org o http://www.stegoarchive.com

Algunos pocos ejemplos de herramientas de creación de esteganografía incluirían **S-Toolsv4**, **JP Hide-and-Seek**, **JStegShell**, **ImageHide**, **ES Stego** y **Dound's Stegonagraphy**. Por otra parte **StegDetect** y **Stegbreak** son herramientas usadas para detectar anfitriones infectados. Para más información acerca de la esteganografía puedes visitar http://stegano.net

Ejercicios

Técnicas de Recuperación de Esteganografía

8.8 Obtén una copia del programa Dound's Steganography.

http://download.cnet.com/Dound-s-Steganography/3640-2092_4-8880146.html

8.9 Crea y codifica un mensaje.

1. Busca una imagen .bmp y guárdala en el escritorio.

2. Lanza el programa Dound's Steganography. Para tener una configuración de color de 32 bits, lee el fichero "how to use" que viene con el programa. La configuración tiene que estar en el lugar del programa para funcionar correctamente.

3. Haz clic en la pestaña "File", selecciona "Open", busca la imagen .bmp y haz clic en "Open". La imagen aparecerá en el campo de la imagen bajo el campo "Message".

4. Escribe un mensaje de texto que quieras esconder en el campo "Message".

5. Haz clic en la pestaña "Function" y selecciona "Encode Message", lo que codificará (esconderá) la información en la foto. Después de que la codificación se haya completado, aparecerá el mensaje "Encoding complete". Ahora haz clic en "Ok".

6. Haz clic en la pestaña "File" y selecciona "Save As". Dale al fichero un nombre único y selecciona el lugar donde quieres guardarlo.

7. Cierra el programa y vuélvelo a abrir.

8. Haz clic en "File" y selecciona "Open". Busca el fichero con los datos ocultos y selecciona "Open". La imagen .bmp aparecerá en el campo de imagen.

9. Haz clic en la pestaña "Function" y selecciona "Decode Message". Se desencriptará el texto oculto y aparecerá en el campo "Message".

8.10 Demuestra cómo esconder datos en una imagen.

1. Busca una imagen .bmp

2. Usa Dound's Steganography para abrir la imagen

3. Introduce datos en el campo de mensaje de Dound's Steganography.

4. Codifica la imagen .bmp que has encontrado en el paso 1 con los datos que quieres ocultar.

5. Guarda el fichero.

6. Envía el fichero por email a otro estudiante.

8.11 Abre la imagen que te haya enviado otro estudiante y decodifica el mensaje de texto oculto.

1. ¿Fuiste capaz de esconder tu mensaje de texto usando Dound's Steganography? ¿Lograste codificar la imagen?

2. ¿Fue el otro estudiante capaz de abrir, decodificar y leer el mensaje

oculto?

3. ¿Fuiste capaz de descubrir o decodificar sus mensajes de texto?

O, para verlo desde otro punto de vista, sigue leyendo

La esteganografía es un timo

Uno de nuestros revisores, que ahora nos paga para que no revelemos su nombre, tiene algo que decir (por eso seguimos insistiendo en que pienses dos veces lo que vas a escribir antes de enviarlo por correo, ponerlo en un foro, o enviarlo en un mensaje):

Quiero hacer constar mi queja por incluir la estenografía como una parte de la Lección 8. Tras leer innumerables documentos, artículos y toda clase de mierdas sobre el tema, creo que hay formas mucho más sencillas de esconder datos. En el 2009, el Departamento de Justicia de los Estados Unidos de América financió una investigación durante ocho meses para localizar mensajes terroristas en fotos pornográficas. La investigación se llevó a cabo por la Universidad de Texas. Al cabo de esos ocho meses se informó, con gran satisfacción, que tras analizar 130.000 imágenes pornográficas no se habían encontrado mensajes de terroristas en ninguna de ellas. Toda esa investigación se basó en que 18 estudiantes de postgrado estudiasen minuciosamente todas y cada una de las páginas porno que pudieran encontrar en Internet. Y todos los investigadores eran hombres.

La conclusión que obtengo es que lo único que conseguimos con todo ese dinero fue un grupo de estudiantes calentorros y ningún dato útil. Por si os lo estuvieseis preguntando, el Departamento de Seguridad Nacional y las Fuerzas Aéreas realizaron el mismo estudio (cada uno por su lado y sin conocer que ya se había hecho) buscando mensajes ocultos en fotos porno. Ninguno de estos estudios encontró nada, salvo un mensaje dentro de un pequeño lote de imágenes. Y esas imágenes eran una broma de alguien que intentaba comprobar si merecía la pena esconder mensajes en fotos guarras. ¡Lo juro por Dios!

La estenografía no es más que un montón de mierda, a menos que me digáis algo que yo no sepa. Este tema se usa para rellenar espacio en libros de seguridad que de otra forma estarían vacíos de contenido. No quiero caer en el mismo error. Incluso una vez entrevisté a uno de los científicos más reputados sobre este tema, y no logró convencerme.

Personalmente, nos encantan este tipo de discusiones. Para empezar, porque simplemente obliga a la gente a pensar. Y es entonces cuando aparecen las preguntas: ¿Estuvieron esos grupos de estudiantes masculinos aprovechándose de la oportunidad de ver porno gratis todo el día? ¿Les pagaban? (A algunos de nosotros nos gustaría ese trabajo). El hecho de que fueran tres las organizaciones las que hicieran esos estudios parece ser una prueba de ello. Pero hay algo más ¿Eran las fotos porno el tipo de imágenes adecuado donde buscar?

Ejercicio

8.12 ¿Cuál sería el mejor tipo de imágenes o contenidos para enviar mensajes por estenografía? ¿Y el mejor sitio para compartirlas?
Piensa en ello.

Análisis forense en Windows

Windows puede ser su propio peor enemigo cuando llega el momento de mantener datos. Este sistema operativo es un devorador de recursos, llena el disco duro y nunca parece estar de brazos cruzados. ¿Cómo podrías examinar una de las bujías del motor de un coche en marcha a gran velocidad sin ninguna posibilidad de detenerlo? ¡Oh! y además Windows está moviendo constantemente ficheros de un lado a otro y modificándolos, incluso aquellos que estás buscando.

Empezaremos ese desastre analizando los diferentes tipos de información volátil y no volátil que un investigador podría recolectar de un sistema Windows. Esta sección tratará con más detalle cómo conseguir y analizar datos en la memoria, registro, eventos y ficheros.

Los portátiles son como cofres del tesoro

Algunos casos forenses tienen que ver con fugas de información. Los datos más recientes muestran que los incidentes relacionados con ordenadores portátiles son los que provocan mayores pérdidas de información que otros casos. El hacking se encontraba muy por detrás en la lista frente al robo de portátiles, y sólo representaba el 16% del total de intrusiones. ¿Qué te hace pensar esto?

Los portátiles se entregan normalmente a empleados sin restricciones y sin mantener un registro. Sería cómo dar las llaves de los coches de empresa sin que a esta le importe quién usa el vehículo y a donde va. Los resultados de estas negligencias son un montón de portátiles en el lugar incorrecto, perdidos o robados, sin ningún tipo de supervisión. Esos mismos portátiles suelen tener configurado un acceso remoto a los servidores de la empresa. Tu trabajo podría consistir en averiguar cómo un criminal pudo acceder a la red de la empresa. Y un portátil perdido puede ser la respuesta.

Mantén esta idea en la cabeza: si pierdes TU portátil... ¿Qué podrían encontrar en el otras personas? ¿Te gustaría que pudieran ver esa información?

Información volátil

La **información volátil** es aquella que se pierde cuando se apaga un sistema o este se queda sin electricidad. Esta información se encuentra en la memoria física o RAM, y consiste en información acerca de procesos, conexiones de red, archivos abiertos, contenido del portapapeles... En definitiva, esta información describe el estado del sistema en un instante concreto.

Cuando se realiza un análisis "en vivo" de un ordenador, una de las primeras cosas que debe recoger un investigador es el contenido de la RAM. Si hace esto en primer lugar, conseguirá minimizar el impacto de la actividad de recopilación de datos sobre el contenido de la memoria.

Estos son algunos ejemplos de información volátil que debería recopilar un investigador:

- Hora del sistema.
- Usuario(s) conectado(s)
- Ficheros abiertos
- Conexiones de red
- Información de procesos
- Mapa de puertos asociados a procesos
- Procesos en memoria
- Estado de la red
- Contenido del portapapeles
- Información sobre servicios y drivers
- Histórico de comandos
- Unidades de red conectadas o compartidas

Herramientas para recopilar información volátil en Windows

Para recolectar información volátil en un sistema Windows, puede utilizar las siguientes herramientas libres, que se encuentran en la suite **Sysinternals** de Microsoft. Puedes descargarla gratuitamente en el sitio web de Microsoft a través del siguiente enlace: http://technet.microsoft.com/en-us/sysinternals/bb842062. Tras descargarla, hay que instalarla en directorio raíz (C:\) del disco de tu estación de trabajo. Tendrás que usarlas (¡sorpresa!) desde una línea de comandos, de esta forma:

```
psloggedon
```

Este programa de Sysinternals te permite ver quién está conectado al sistema de forma local, así como los usuarios que lo están remotamente.

```
time /t command
```

Utiliza este comando para ver la fecha actual del sistema. Windows utiliza el formato UTC, que es el mismo que el GMT (Hora universal), para mostrar la fecha de los archivos. La fecha del archivo se muestra con una precisión de 100 nanosegundos en formato hexadecimal de 8 bits. La fecha del sistema Windows se presenta en 32 bits, mostrando el mes, día, año, día de la semana, hora, minuto, segundo y milisegundo.

```
net session
```

Este comando te muestra no sólo los nombres de los usuarios que están accediendo al sistema remotamente, sino que también te indica su dirección IP y el tipo de cliente que están utilizando para acceder al sistema.

```
openfiles
```

Este comando da una lista de los usuarios que están conectado al sistema remotamente; los investigadores también podrán ver qué archivos tienen abiertos, si es que hay alguno. Se utiliza para conectar o desconectar ficheros y carpetas que estén abiertos en un sistema.

```
psfile
```

Este programa también forma parte de la suite Sysinternals que te estamos mostrando. Es un programa para línea de comandos que devuelve la lista de archivos de un sistema que se han abierto de forma remota. Permite a un usuario cerrar esos archivos por su nombre o mediante su identificador.

```
net file
```

Este comando muestra los nombres de todos los archivos abiertos en un sistema, el número de archivos bloqueados, y cierra los archivos compartidos y elimina los bloqueos.

En la página de Microsoft Tech que te hemos indicado un poco más arriba, encontrarás la explicación de cada herramienta incluida en Sysinternals y las opciones de las que dispone cada una de ellas. En definitiva, este paquete es un conjunto de herramientas muy potentes para especialistas en análisis forense y técnicos de red.

Otra cosa que podrías querer hacer es buscar archivos borrados en la base de datos de previsualización de miniaturas de Windows. Busca un archivo que se llama thumbs.db_. Este te mostrará todas las miniaturas de las imágenes mostradas en el explorador.

Información no volátil

La **información no volátil** se guarda en dispositivos de almacenamiento secundario y se mantiene una vez que se haya apagado el sistema. No desaparece y puede recopilarse tras haberlo hecho con la volátil. Los siguientes puntos detallan algunos de los tipos específicos de información no volátil que un investigador debería recuperar:

- Archivos ocultos.
- Espacio slack.
- Archivos de intercambio
- Archivos index.dat
- Metadatos
- ADS (Alternate Data Streams) ocultos
- Windows Search index
- unallocated clusters
- unused partitions
- Registro del sistema
- Dipositivos conectados
- Registro de eventos

¿Preparados? Luces, cámaras... ¡Acción!

Cada vez que un objeto (un archivo) es accedido por alguien (un intruso), habrá efectos residuales. Estos efectos pueden no ser fáciles de localizar o detectar, pero estas acciones (borrarlos o modificarlo) pueden tener consecuencias en otros lugares. Para reducir las acciones detectables, un hacker profesional usará herramientas que ya se encuentren disponibles en el sistema. No instalará nuevo software, si no que se utilizarán las herramientas del sistema de forma que parezca un comportamiento normal.

Localización y edición del registro de eventos de Windows Server 2008

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application]

```
%WinDir%\System32\Winevt\Logs
```

También puedes usar Windows Powershell para ver los registros de seguridad con un único comando:

```
get-eventlog security
```

Si lo que quieres es examinar un evento de seguridad en concreto, prueba esto

```
$events = get-eventlog security -newest 20
```

Ejercicios

8.13 Aunque no estés utilizando Windows Server, encuentra los siguientes registros en Windows: Instalación (Set up), Aplicación (Application), Eventos reenviados (Forwarded Events) y Seguridad (Security). ¿Qué cantidad de eventos hay en cada registro de tu equipo? ¿De qué tipo son?

8.14 Mientras examinas el registro de eventos, crea una "Vista personalizada" (custom view) de forma que puedas ver eventos críticos de los registros seleccionados. ¡Caray, mira eso! ¿Puedes importar una vista personalizada? ¿Qué filtros elegirías para registros muy extensos, como el de Aplicaciones?

8.15 Obtén una copia de Sysinternals de la dirección que te hemos facilitado. Encontrarás que ese programa es, en realidad, un conjunto de programas más pequeños, pero muy potentes. Examina las opciones de las que disponen algunos de ellos. ¿Podrías combinar algunos de esos programas y crear de esa forma una herramienta nueva?

Análisis forense en Linux

Linux se utiliza habitualmente en análisis forense porque:

- Trata todos los dispositivos como ficheros.
- No necesita usar write blocker (los análisis forenses necesitan una controladora capaz de acceder a los discos en modo de sólo lectura para mantener la integridad de los datos)
- En muy flexible y permite trabajar sobre muchos sistemas operativos y tipos de ficheros.
- Puedes arrancarlo desde un soporte extraíble.
- Suele incorporar un kit de herramientas forenses, con muchas utilidades.

Linux, al igual que Unix, no dispone de **flujos alternativos de datos** (ADS, o Alternative Data Streams) asociados a los ficheros. Los datastreams de Linux no se destruyen si usas las herramientas para eliminar archivos más comunes. Borrar un archivo de forma segura implica que este no debe ser recuperable dado que se ha eliminado del soporte. Una limpieza correcta significa que ese archivo no puede recuperarse, o que sólo lo será dedicando mucho tiempo y dinero.

Un archivo que se elimine con el comando

```
/bin/rm
```

todavía estará en el soporte y puede recuperarse sin mucho esfuerzo.

El Slack en Linux

Los sistemas de archivos en Linux también tienen espacio de slack, al igual que Windows. Pero este espacio es mucho más pequeño, aproximadamente unos 4K por bloque. Esto significa que un sospechoso puede esconder unos 4K de datos en ese pequeño bloque de archivos. Las técnicas que te mostramos para el espacio de slack en Windows pueden aplicarse a Linux. Este espacio no se detecta por el sistema de archivos o las herramientas de uso de disco. Cuando un dato se elimina, el espacio slack todavía mantendrá el contenido que se haya ocultado.

Cadenas simples

Es muy fácil buscar y localizar cadenas de texto en Linux usando el comando

```
/dev/hdaX | grep 'texto que quiero buscar'
```

Según el tamaño del dispositivo, esta búsqueda puede tardar más o menos tiempo, porque buscará ese texto en todos los rincones de esa partición. No querrás hacerlo usando un editor hexadecimal porque te llevaría aún más tiempo, aunque son útiles para determinar el tipo de contenidos del soporte.

Grep

Grep es una herramienta potentísima que encontrarás en Linux. Se utiliza para encontrar ciertas líneas en un archivo. Esto te permitirá encontrar rápidamente archivos que contengan cierto contenido dentro de un directorio o sistema de archivos. ¡Y puedes usar expresiones regulares! Hay patrones de búsqueda que te permitirán especificar un criterio que debe cumplir la búsqueda. Por ejemplo: encontrar todas las cadenas en un diccionario que empiecen por una "s" y terminen con una "t".

Muy útil cuando estás haciendo un crucigrama.

```
grep ^s.*t$ /usr/share/dict/words
```

Más herramientas en línea de comandos

Las utilidades forenses "Live" que te hemos enseñado antes son un maletín de herramientas muy completo para Linux. Linux, por sí mismo, también dispone de utilidades sencillas para obtener imágenes y efectuar análisis básicos de los discos, como las siguientes:

Herramienta	Descripción
`dd`	El comando dd puede copiar datos de cualquier disco que Linux pueda montar y acceder. Este comando puede hacer copias directas de disco a disco, de disco a un archivo de imagen, copiar por bloques, o volcar bloque a un archivo.

`sfdisk` y `fdisk`	Muestra la estructura del disco.
`grep`	Busca patrones o cadenas dentro de un archivo.
`md5sum` y `sha1sum`	Calcula y almacena los hash en MD5 o SHA-1 hash de un archivo o una lista de ellos (incluyendo los dispositivos).
`file`	Lee la cabecera de un archivo para determinar de qué tipo se tratará, sin importarle el nombre o su extensión.
`xxd`	Una herramienta en línea de comandos para hacer volcados en hexadecimal.
`ghex` y `khexedit`	Editores hexadecimales para Gnome y KDE (X Windows Interface)

Cómo encontrar un pajar en una aguja

El software forense Open Source dispone de herramientas de búsqueda que te permitirán encontrar muchas combinaciones y permutaciones de elementos para buscar datos escondidos. No hay necesidad de comprar carísimas herramientas comerciales, lo que hace que esta sea la parte más maravillosa del usar programas de fuentes abiertas. Linux te ofrece un gran abanico de posibilidades para construir herramientas parecidas usando las utilidades estándar. El siguiente párrafo explica cómo usar find, grep y strings, y te enseña el uso del *pipe* para combinarlos.

Cifrado, descifrado y formatos de archivo

Muchos de los archivos que encontrarás no pueden ser leídos inmediatamente. Algunos programas tienen un formato de archivo propietario, mientras que otros usan formatos estándar como, por ejemplo, los archivos de imágenes como gif, jpg, png, etc... Linux dispone de una excelente herramientas que te ayudará a determinar el tipo de un archivo dado. ¿Te acuerdas del comando **file** que vimos antes?

Modificadores en línea de comandos	Efecto
`-k`	No se detiene en la primera coincidencia, y sigue buscando.
`-L`	Sigue los enlaces simbólicos
`-z`	Intenta buscar dentro de los archivos comprimidos.

Estos switches te permitirán intentar leer un archivo. Existen varias herramientas de conversión de tipos de ficheros disponibles en Linux, y existen muchas más disponibles en Internet, así como visores de archivos para varios formatos. A veces se requiere dar más

de un paso para llegar a un sitio donde puedas trabajar con los datos. Reflexiona sobre esta analogía.

En ocasiones te encontrarás con archivos que han sido encriptados o protegidos con una contraseña. La dificultad es variable, desde encriptaciones que son fáciles de romper hasta aquellas que les darán un buen dolor de cabeza a los profesionales. Merece la pena examinar el espacio alrededor del ordenador que estés analizando. La gente no es muy buena recordando contraseñas: puede que la hayan anotado en algún sitio. Las elecciones más comunes para contraseñas son: mascotas, parientes, fechas (de la boda o nacimiento), números de teléfono, matrículas de coche y combinaciones sencillas (123456, abcdef, qwerty etc.). Las personas también son reticentes a emplear más de una o dos contraseñas, y las usan para todo; así que si eres capaz de obtener el password de un archivo o aplicación, pruébalo con el resto de ficheros. Muy posiblemente sea el mismo. Repasa la "Lección 11: Contraseñas" para saber más sobre cómo crackear passwords.

Ejercicios

8.16 Arranca tu equipo con Linux y crea un archivo que se llame "planes malignos" en una unidad USB o cualquier otro soporte de datos extraíble.

8.17 Borra el archivo usando la técnica que prefieras.

8.18 Dale ese soporte a tu compañero de laboratorio y dile que has perdido un archivo. Pídele que te lo recupere, pero no le digas el nombre del fichero que has "perdido"

8.19 Repite este proceso con otros soportes y sistemas operativos, intercambiándolos con tu compañero de laboratorio.

8.20 ¿Cuantas veces tienes que formatear un disco u otro soporte extraíble para garantizar que todos los datos han sido borrados?

8.21 Si una partición se elimina y luego se reasigna ¿los datos se han perdido para siempre, o pueden recuperarse? ¿Qué herramientas utilizarías para intentar llevar a cabo esta tarea?

8.22 Esconde un archivo secreto en el espacio de slack space de otro archivo. Borra el archivo principal. ¿Pueden recuperarse los datos ocultos? ¿Cómo lo harías si fuera posible?

8.23 Si el método de cifrado es demasiado fuerte como para romperlo, puede que necesites ejecutar un "ataque de diccionario" (también denominado "ataque de fuerza bruta"). Busca en qué consiste esto.

8.24 Investiga qué es y cómo funciona Truecrypt. Aprende todo lo que puedas sobre contenedores ocultos. ¿Crees que serías capaz de acceder a un archivo de ese tipo? ¿Cómo? (Una posible respuesta: http://xkcd.com/538/)

Alimenta tu mente: algunos casos reales

Veamos unos ejemplos de cómo se emplean los análisis forenses.

Quién	Qué
Morgan Stanley	En un tribunal de Florida, Morgan Stanley (MS) no entregó en varias ocasiones la información que se le había requerido para un juicio en su contra por fraude. MS ocultó 1423 cintas de backup que contenían correos detallando el fraude. Un técnico de MS que había sido despedido informó al tribunal que esas cintas existían y que muchas otras habían sido etiquetadas erróneamente adrede. El examen forense confirmó que el fraude fue intencionado. El juez sancionó a MS con una multa de 1600 millones de dólares por actuar con "dolo y maldad"
David Kernell	En septiembre de 2008, el demandado hackeó la cuenta de correo en Yahoo! de Sarah Palin (candidata a la vicepresidencia de Estados Unidos). Antes de que el FBI acudiera a investigar, Kernell desinstaló su navegador web y desfragmentó su disco duro. El gobierno fue capaz de conseguir pruebas y análisis forenses suficientes para condenarlo por varios delitos.
TJX A.K.A. Albert González	Una de las mayores condenas que ha recibido alguien por delitos informáticos recayó en TJX. Albert González fue acusado de robar 90 millones de números de tarjetas de crédito y débito. El acusado dirigió durante varios años una red de ciberdelincuentes y se compró un yate con el dinero robado. Se pidió a varios equipos de analistas forenses que estudiaran el caso y proporcionaran las pruebas necesarias. TJX fue condenado a 20 años de prisión y al pago de una multa de 25.000 dólares.

Análisis forense de móviles

Usar comunicaciones móviles como herramienta en la planificación o ejecución de un hack te proporcionará un nuevo conjunto de opciones. Los teléfonos móviles utilizan distintas señales: una es el enlace por radio que conecta tu terminal a la antena más cercana, otra es el Bluetooth que se usa en conexiones de corto alcance; la señal de localización del GPS puede emplearse para otras cosas y, finalmente, tenemos las prestaciones de conexión digital. Vamos a centrarnos en la parte digital de un teléfono móvil.

Dentro del terminal tenemos una tarjeta SIM (**Subscriber Identification Module**) que hace que tu teléfono sea único para tí y tu proveedor de telefonía. Esta tarjeta SIM es la misma que guarda tu agenda de teléfonos y otros datos en formato de texto, y tiene un microprocesador incorporado.

La tarjeta SIM también contiene un conjunto especial de números conocido como *International Mobile Subscriber Identity* (**IMSI**). El IMSI es el número de teléfono de ese

dispositivo, y se puede considerar como la MAC (**Machine Access Code**) del teléfono móvil. El primer conjunto de números de un MDN se asigna por el fabricante. Hay editores para tarjetas SIM como los disponibles en Dekart http://www.dekart.com/products/card_management/sim_manager/ que te permitirán ver ese conjunto de números.

Si vas a hacer algo especial con un teléfono móvil y quieres evitar ser rastreado, puedes usar varias tarjetas SIM. Si cambias la tarjeta tras cada llamada, será casi imposible rastrear el terminal. Hay tarjetas SIM internacionales de prepago disponibles en Europa, Corea, Japón y otros muchos países que no tienen un monopolio de telefonía móvil cómo ocurre en Estados Unidos.

Algo que tienes que tener en cuenta es que los teléfonos móviles se rastrean continuamente por las antenas de telefonía, aunque no lo uses y sólo lo tengas encendido. Esto es algo completamente normal, y es parte del proceso de comunicaciones para garantizar que al llamar la conexión se establezca rápidamente, en cualquier momento. En un futuro no muy lejano, las antenas de telefonía mantendrán un registro de cada terminal que pase por su zona comunicándose. Puede parecer contradictorio si lo comparamos con el párrafo anterior, pero hemos de tener en cuenta que la tarjeta SIM almacena el identificador del terminal. Por tanto, cambiar la SIM es casi como cambiar el terminal.

Los mensajes SMS (**Short Message Service**) se guardan en el proveedor de telefonía durante un plazo de varios días... o ninguno. Esto muestra lo rápido pueden desaparecer las pruebas, y que el tiempo de respuesta es crítico. Estos mensajes se guardan en el teléfono del usuario, normalmente en la tarjeta SIM o en una tarjeta de memoria externa.

¿Cómo te sientes ahora que sabes de la capacidad de "traza-habilidad" de TU teléfono?

Conecta el cable azul al conector rojo.

Otro aspecto de las comunicaciones digitales móviles es la posibilidad de usar VOIP (**Voice Over Internet Protocol**). Esta herramienta de comunicación usa un software de VOIP para comunicarte con otro usuario de VOIP mediante el uso de comunicaciones de datos de voz. ¡Fantástico! ¿A que si? ¿De qué podría servirte?

Bien, dado que la VOIP es digital y es software, podemos encriptar los paquetes si estás utilizando. AED (Advanced Encryption Standard) es un cifrado de bloques y puede proporcionar muchos niveles de seguridad. Tendrás que usar el menor nivel de encriptación, ya que la VOIP iría bastante lenta usando la conexión de datos de un teléfono móvil.

Requiere desmontaje

Antes de intentar recuperar cualquier dato de un teléfono móvil, desconecta la señal, tal y como ocurre cuando lo pones en "Modo avión". Los proveedores de telefonía móvil pueden restringir o borrar los datos de un dispositivo si este ha sido declarado como robado o perdido. ¡No seas la persona que olvida desconectar la señal a la nave nodriza!

Los dispositivos más viejos necesitaban de un cable propietario para cargar y transferir datos. Esos cables eran distintos para cada dispositivo y no servían para otra cosa. Actualmente, la mayoría de los terminales utilizan un cable con un conector mini USB en un extremo, y un USB estándar en el otro. Los productos de Apple son la excepción a esta regla por "motivos de seguridad"

Serán muy seguros, pero el cable de Apple para conectar el dispositivo al ordenador tiene un conector USB en una punta. Y si eso no fuera suficiente para trabajar bien, puedes comprar el kit de adaptador de cámara para iPad. Este kit incluye una conexión USB directa a la tableta y otro adaptador que permite conectarle una tarjeta SD. Así que te da la opción de conectar una tarjeta SD o una unidad USB directamente al dispositivo. Mola, ¿verdad?

Los dispositivos móviles pueden almacenar datos en cualquiera de las tres zonas locales. Estas áreas son: la memoria interna del teléfono, la tarjeta SIM y la tarjeta de memoria externa. Las cosas interesantes (las pruebas "de verdad") se pueden encontrar frecuentemente en la memoria interna del teléfono y en la tarjeta SIM. Los dispositivos que puedan enviar SMS incluyen un software de "texto predictivo". Y los archivos de texto predictivo pueden contener partes o incluso mensajes completos que no se pueden encontrar en otro lugar.

Tantos dispositivos, tan poco tiempo

Viajemos al pasado, cuando los teléfonos sólo servían para enviar y recibir transmisiones de voz. Esas cosas estaban colocadas en la pared, sobre una superficie o atornilladas a una cabina telefónica. Hoy día ya no son sólo un teléfono: son ordenadores portátiles conectados a una red. Las comunicaciones móviles están disponibles en distintos tamaños y modelos. Un iPad no es un teléfono, pero puede comunicarse de muchas de las formas que estos lo hacen. Una tablet, Android OS, Pocket PC... todos tiene muchas de las características de un teléfono, pero no podemos considerarlos como tales. "Colega, déjame tu tablet para poder llamar a mi amigo" es algo que no escuchas ahora, pero lo harás pronto. Entonces tendrás que preocuparte de que puedan encontrar tus cartas de amor, tu porno... o de que pongan cartas de amor o porno en tu teléfono.

Los productos que ejecutan Android OS son bastante sencillos de examinar, dado que se trata del sistema operativo abierto de Google. Android está basado en el kernel de Linux que vimos anteriormente. Google ofrece el código fuente de Android y un kit de herramientas de desarrollo de forma gratuita. Otros sistemas operativos son BlackBerry OS, Windows, Windows CE, Nokia, Symbian y Linux.

Todos los sistemas operativos necesitan almacenar archivos de forma ordenada, y no hay muchas formas distintas de llamar a los archivos "SMS" o "Video". Si fisgoneas un poco en cada uno de los dispositivos, utilizando el software de la lista que te proporcionamos más abajo, podrás encontrar las pruebas que andabas buscando; por esos nunca deberías pensar que tu dispositivo es invulnerable o que al menos está protegido.

Aparte del hecho de que los dispositivos móviles tienen capacidad de comunicarse por Bluetooth, transmitir datos y WiFi, muchos tienen el GPS activado. Todas estas señales almacenan información en el teléfono, la tarjeta SIM o la tarjeta de memoria externa. El software forense permite examinar el historial de cada uno de ellos, incluido el GPS. Si el sospechoso tenía activado el GPS, todos los "puntos de interés" y su historial de localización pueden recuperarse para obtener incluso aún más pruebas.
http://www.gpsvisualizer.com/ te permite cargar los datos del GPS y creará un mapa que te mostrará donde has estado.

No te olvides del GPS ni del ordenador de a bordo del vehículo del sospechoso. Cualquier vehículo construido en la década pasada (y desde 1985 en EE.UU.) tiene un ordenador de diagnosis que registra la velocidad, consumo de combustible, secuencia de encendido y mucha más información que te ayudarán con el caso que investigas.

Puedes estar seguro de que oirás pasos que se acercan a tu posición mientras te siguen. Incluso puede que seas capaz de llamar por teléfono con un zapato.

iDevices: Algunas personas han dedicado tiempo y esfuerzo en proyectos de fuentes abiertas como IPBackup Analyzer. El objetivo de este programa es analizar los datos de la copia de seguridad de un iPhone y hacerlos legibles. Puedes descargar esta herramienta de fuentes abiertas en http://ipbackupanalyzer.com/. Un problema exclusivo con los dispositivos móviles de Apple es que necesitan una contraseña para el backup. Pero el código de acceso puede omitirse mediante herramientas de software, que te permitirán examinar los mensajes de texto, agenda de contactos, fotos, vídeos, correos y todas las pruebas que puedas necesitar examinar.

Ejemplo de análisis forense de un iPhone

Mira este artículo que detalla una investigación forense sobre un iPhone: http://www.nxtbook.com/nxtbooks/evidencetechnology/20120910/#/30

AVISO:
Este artículo trata sobre un tema bastante delicado que puede resultarte ofensivo.

Herramientas software para teléfonos

La mayoría de los principales fabricantes de software forense para teléfonos han encontrado un nicho de mercado que les permite cobrar un extra por sus herramientas. Hay unas pocas herramientas open source y libres que deberías mirar. Como en otros casos, cada herramienta tiene sus pros y sus contras, pero necesitas tener un conocimiento práctico de varias de ellas para tener éxito en tus investigaciones.

Oxygen: Este fabricante de hardware y software dispone de varios productos para efectuar análisis forenses en móviles. El software puede usarse gratis durante un periodo de tiempo, unos seis meses de media. Si no puedes obtener los datos que necesitas en ese tiempo, quizás te resulte más útil un martillo. Puedes descargar la versión gratuita de Oxygen Forensic Suite (Standard) en http://www.oxygen-forensic.com/en/freeware/. Este programa es capaz de leer los backups de un iPhone, incluso si los datos estás protegidos con el password de iTunes. ¡Genial!

Bit Pim: Un proyecto open source. Bit Pim se ha estado empleando durante años. Este software tiene un pequeño inconveniente, y es la falta de soporte para los smartphone más recientes. Siendo honesto, Bit Pim no funciona en unos cuantos de los teléfonos inteligentes más recientes. Pero por suerte para ti, los autores tratarán de crear un paquete si se lo pides educadamente. Para hacerlo, tienes que seguir las reglas que puedes encontrar en su web, dentro de "FYI", si es que quieres obtener una respuesta suya. Si no lo haces, no obtendrás nada. Nada de nada. Lee la documentación en http://www.bitpim.org/.

Sleuth Kit: Ya hemos hablado anteriormente de Sleuth Kit en esta lección. Es otro programa de fuentes abiertas con muchísimas prestaciones, incluyendo el análisis forense de terminales móviles: Sleuth Kit te da las mismas posibilidades que muchos productos comerciales. Puedes encontrar información más que suficiente, e incluso una wiki completa en www.sleuthkit.org.

https://viaforensics.com/products/tools/ dispone de enlaces gratis para herramientas forenses para Android OS. También tiene un libro sobre análisis forense en Android además de varios scripts para obtener tus propios datos. Estos chicos también disponen

de una sección dedicada al iPhone en https://viaforensics.com/iphone-forensics/howto-iphone-forensics-free-andor-open-source-tools-91411.html. Recuerda: si tienes un Apple, mantén el backup de iTunes a buen recaudo.

¿Y ahora qué?

Si un dispositivo digital es una prueba en un caso, no lo apagues si esto fuera posible. Busca un cargador de baterías, cómpralo o fabrícate uno si tienes que mantener el dispositivo encendido y necesitas conservarlo así. Esto es crítico si el teléfono es desechable, ya que no existe un contrato firmado con un operador de telefonía móvil: son muy difíciles de rastrear.

Por supuesto, no podrás examinar o copiar los datos de la tarjeta SIM sin quitar la batería. Esta es otra razón para mantener el dispositivo alimentado de otra forma, sin depender de la batería. Vista nuestra suerte, seguramente la batería estará siempre a punto de agotarse: los malos nunca se acuerdan de cargar sus dispositivos.

El examen forense debe hacerse empleando un cable conectado directamente entre el teléfono y el ordenador del laboratorio. Esto significa que todas las opciones de comunicación necesitan estar desconectadas: Bluetooth, WiFi, GPS y demás deben estar apagados antes de comenzar el examen. El no hacerlo podría hacer que la prueba no fuera válida para los tribunales de justicia.

Ejercicios

8.25 Usa un cable Mini USB para conectar un terminal móvil a tu ordenador. El dispositivo debería mostrar una pregunta con tres respuestas posibles. ¿Cuáles son esas respuestas? ¿Cuál deberías escoger si quieres evaluar los datos de tu dispositivo?

Una vez que tengas establecida una conexión entre tu ordenador y el dispositivo, comprueba qué información puedes obtener sobre ti. ¿Hasta dónde puedes llegar sin utilizar un software especial? ¿Puedes leer cualquier información en el propio dispositivo, o sólo los que están en la tarjeta de memoria externa?

Desconecta el cable y descarga el software de análisis forense para móviles que más te guste en tu equipo. Instala el software. Ahora apaga y enciende el teléfono. Seguidamente, vuelve a conectar el cable de la misma forma en que lo hiciste antes. Bien, ahora ya puedes ejecutar el software forense que has descargado. ¿Puedes acceder a todos los datos de la SIM, o sólo a parte de ella?

¡¡No trastees con el número PUK o Pin!! Muchos teléfonos se bloquean si estos números se introducen mal varias veces. ¿Qué son los números PUK y Pin? ¿Por qué son importantes para ti como analista?

8.26 Pídele a un familiar o amigo que te preste su teléfono y conéctalo a tu supercomputador. ¿Puedes acceder a sus SMS, fotos, contactos o al registro de llamadas? ¿Cuál es el número de serie del teléfono? ¿Es el que está en la SIM, o el que puedes encontrar dentro de la carcasa?

Análisis forense de la red

Este análisis se utiliza para averiguar donde se encuentra un ordenador y probar si un archivo en concreto fue enviado por la red. Aunque los análisis forenses de la red pueden resultar bastante complejos, te enseñaremos algunos conceptos básicos que puedes usar en tu día a día para encontrar cosas... o ser encontrado.

Registros del firewall

¿Quién intenta conectarse a tu equipo? El firewall es una utilidad que permite controlar las conexiones entre dos puntos de una red. Hay muchas clases de firewalls. Sin importar qué tipo o uso le des al firewall, siempre tendrás los registros para consultar los detalles. Con la ayuda de los registros podrán encontrar patrones de ataques e intentos de explotación del tu firewall.

Y como sucede con cualquier archivo de registro, la integridad de estos es fundamental. Debes pensar en ellos como una **prueba irrefutable**. Cada archivo está marcado con una fecha y hora y ciertos privilegios. Los registros de los firewalls se consideran como "registros inteligentes" ya que están generados por un dispositivo que tiene un perímetro y no es un simple hub o concentrador. No es que se registre cada paquete: es que se hace con cada petición y conexión. Y lo que estás buscando son las conexiones entre dos direcciones IP en concreto, o el envío de ficheros entre dos conexiones.

Packet Sniffers

Los **paquetes de datos** fluyen por las venas de todos los dispositivos de red. Y dado que hay, literalmente, millones de paquetes moviéndose entre servidores y otros dispositivos, controlar los paquetes uno a uno era algo que parecía imposible. Pero con la mayor potencia de los ordenadores y un software mejor, ahora disponemos de la capacidad de buscar entre millones de paquetes transmitidos para encontrar aquellos que cumplen con nuestros requisitos. A esta técnica la llamamos "packet sniffing."

Imagínate que viajas en un autobús repleto de pasajeros. Todos están hablando, pero a ti sólo te interesa la conversación que tiene lugar dos filas más allá. Tu cerebro tiene la capacidad de eliminar el ruido y centrarse es esa conversación. El packet sniffing hace exactamente lo mismo: elimina el ruido y se enfoca en los paquetes en los que estás interesado.

Hay packet sniffers de todos los sabores y colores, pero todos ellos deben instalarse entre las transmisiones de datos. No puedes escuchar una conversación si no estás con las personas que hablan. Los packet sniffers pueden ser activos (que buscan) o pasivos (que escuchan), pero ambos te devolverán los paquetes que cumplan con tu criterio de búsqueda. Lo que le interesa a un intruso es capturar, almacenar y transmitir esos paquetes de tu red sin ser descubierto.

Sistemas de detección de intrusos, o Intrusion Detection Systems (IDS)

Este nombre tan sugerente es el término que usamos para definir cualquier cosa que pueda detectar, avisar o terminar cualquier actividad anormal en la red. Snort es el ejemplo perfecto de un programa que busca tráfico anormal en la red. Un ejemplo de comportamiento extraño sería que estuvieras de vacaciones y tu email se activara. Tu cuenta comenzaría a enviar y recibir toda clase de archivos adjuntos y a reenviar mensajes, tal y como sucedería si alguien estuviera usándolo. Un IDS detectaría ese comportamiento anómalo y actuaría por su cuenta para bloquear la cuenta o notificar a alguien que algo raro sucede mientras estás ausente.

Los IDS se diseñaron para ser los perros guardianes del tráfico de red. Cada tipo de IDS busca en protocolos, firmas, puertos y otros sitios donde exista un comportamiento extraño. Algunos sistemas deniegan todo y sólo permiten pasar a los usuarios autenticados, mientras que otros IDS ponen un cebo y permanecen a la espera. En los registros de los IDS puedes encontrar cosas increíbles relacionadas con comportamientos extraños.

Registros en los Routers y Administración de red

Como comentamos en los registros de los firewalls, los registros de los routers y en la administración de red se recopilan detalladamente las actividades típicas. En ocasiones aparecerá en ellos algún dato que atraerá el interés del investigador forense en un caso. Aparte del hecho de ser una prueba de que sucedieron ciertos eventos, los registros resultan difíciles de manipular. Las herramientas de software que mencionamos antes tienen programas que automatizan el filtrado de registros. Usar herramientas con automatización te permitirá ahorrar tiempo, y te ayudarán a no volverte loco.

Herramientas para el tráfico de las redes

Existe una gran variedad de herramientas Open Source que deberían formar parte del kit de cualquier recopilador de pruebas, empezando por el famosísimo **Wireshark**. Dado que el tráfico de red consiste en paquetes de datos o fragmentos de información, Wireshark los capturará y analizará. En lugar de hacerte buscar línea por línea en cada paquete para identificar las cabeceras, la información de enrutamiento, el remitente y el contenido de cada paquete, Wireshark se encargará de hacer el trabajo pesado por ti. Además, Wireshark es una herramienta multiplataforma.

Netcat (http://netcat.sourceforge.net/) es otra poderosísima herramienta Open Source que analiza todo el tráfico de red, tanto TCP como UDP, entrante y saliente, Ethernet o IP, incluyendo cualquier servicio o puerto que quieras comprobar. Al igual que Wireshark, Netcat es una aplicación multiplataforma, y ambos se actualizan regularmente por un equipo de voluntarios.

Netcat tiene una herramienta de **volcado hexadecimal** incorporada y puede capturar y/o analizar paquetes.

Cabeceras del E-Mail

Los e-mails contienen información sobre cada equipo por el que pasan hasta que llegan a to. Esta se añade a la **cabecera** que contiene la información del correo. A veces la información más importante se encuentra en las cabeceras. Ver las cabeceras no resulta siempre sencillo. Distintos tipos de clientes de correo tienen distintas formas de verlas. Pero el truco de leer las cabeceras está en que se leen al revés. ¿Por qué? En lo más alto de la lista está el receptor, y por cada ruta que atraviesa el correo se añade una línea hasta llegar a la última que es donde se refleja desde que red o equipo se envió el correo.

Esto sólo será cierto si el remitente del correo utilizó su dirección de correo real para enviarlo. Los correos pueden falsificarse, las IP puedes alterarse y hay toda clase de trucos que se pueden emplear para ocultar el remitente real. Las cabeceras pueden proporcionarte pistas, pero no esperes resolver ningún caso basándote únicamente en la información de las cabeceras del correo.

En las cabeceras del correo hay un segmento llamado “Message-ID." Este conjunto de caracteres se añade por el servidor de correo desde el que se envió el mensaje. Dado que cada ID es único, conectarte podría ayudarte a identificar la ubicación del remitente original del mensaje: busca el link que aparece justo después de la serie de números y letras en el ID.

El campo “From” que contiene la información sobre el remitente se configura en el cliente de correo, y no puede considerarse fiable. Las marcas de tiempo también resultan engañosas porque los clientes de correo pueden configurarse para enviar los

mensajes horas o días después de que se hayan escrito. Es una técnica conocida como "Envío retrasado."

Ejercicios

8.27 Elige un correo basura que tengas en tu bandeja de entrada. Usando la información que te hemos dado, disecciona la cabecera del correo para intentar localizar el origen del mensaje. ¿Cómo consiguió el spammer tu dirección de correo?

8.28 Investiga cómo buscar los encabezados de los correos en los e-mails que recibes. ¿Hay algún campo que te resulte desconocido? Posiblemente tengas varias cuentas de correo; envíate un mensaje a ti mismo, pero hazlo con tu mejor esfuerzo para ocultar tu ubicación real.

8.29 Envíale un correo falso a tu compañero de laboratorio diciéndole que tiene que ir a recoger algo para la siguiente clase. Por ejemplo, un donut. Asegúrate de falsificar el remitente para que sea el profesor, o de otro modo no conseguirás tu donut.

8.30 Si tienes una cuenta de correo en una red social, envíate un correo desde esa cuenta a la cuenta que uses habitualmente. Dale un vistazo a los encabezados para ver si puedes averiguar cómo se enrutó ese mensaje.

8.31 Ahora, repite el ejercicio pero envía el mensaje desde el correo de la red social como anónimo a tu cuenta habitual. Comprueba el encabezado del correo anónimo para ver si puedes averiguar cómo de bien ha ocultado tu identidad esa red social.

Comienza el juego: Boca abajo y sucia

"Por favor, dime que estás haciendo en el basurero de la escuela" preguntó Mokoa mientras intentaba peinar su melena al viento. Había dos piernas colgando en el borde del contenedor verde, que indicaban que la otra mitad de Jace estaba lidiando con las bolsas de basura del contenedor.

"¡Sujétame la tapa del contenedor!", gritó el intruso en la basura. Un fuerte "¡clunk!" sonó en el lateral del contenedor metálico cuando algo de gran tamaño lo golpeó en el interior. "¡Lo tengo! Ahora ayúdame a salir de aquí" grito Jace. El eco de su voz en el cubo de basura sonó como si hablara a través de una lata de sopa con un globo en su interior. La mera imagen de la sopa le produjo nausea mientras aferraba al premio que intentaba sacar del contenedor.

Mokoa sujetó las dos piernas intentando evitar que le golpeasen en la cara, e hizo girar a la hacker maloliente sobre la apertura del contenedor. Para sorpresa de ambos, Jace apareció aferrando un tablet usado en sus brazos para no dejarlo caer. Ya con los pies en el asfalto del aparcamiento, sujetó el fruto del sucio trabajo como un trofeo.

"¡Mira! ¡Esto es el dispositivo de acceso a la sala de descanso de los profesores!", exclamó Jace mientras sonreía. Como cualquier señorita, peinó su pelo andrajoso hacia atrás para tener mejor aspecto en este momento triunfal. En ese instante, el dispositivo resbaló de sus manos y cayó de punta sobre su piee.

Mokoa nunca había oído maldecir tanto a Jace, y jamás había escuchado un

aullido de dolor tan fuerte como ese. Hizo todo lo posible para evitar reírse del dolor de su amiga, sobre todo porque él era el que se hacía daño cuando estaban juntos.

Mokoa puso sus manos en las caderas y le dijo a la niña "¡Nunca había oído maldecir tanto desde la última vez que fui a la iglesia!"

Jace se olvidó de sus doloridos dedos del pie y miró sorprendida a los ojos de su amigo "¿De qué estás hablando? Mira que eres raro".

Mokoa dejó caer los brazos y le explicó: "En la iglesia siempre están hablando sobre el infierno, sobre cómo nos condenamos y cosas por el estilo". Estaba tratando de animar a Jace, aunque su sentido del humor era horrible.

"Mokoa, esa broma me hace más daño de lo que me duele el pie ahora", dijo Jace. "Pero mira otra cosa interesante que encontré en la basura", dijo mientras sacaba un teléfono móvil roto del bolsillo.

Con un tono de puro aburrimiento Mokoa respondió "¡Oh! ¡Un móvil roto y una tablet destrozada! ¿Qué piensas hacer con semejantes tesoros?"

Jace inclinó la cabeza ligeramente mientras su boca mostraba la mueca reservada a los genios malignos. "Ya verás", dijo.

De vuelta en el laboratorio... bueno, en realidad de regreso al pequeño dormitorio que tenía en el apartamento en el que vivía con su abuela, Jace retiró las tapas traseras de los dispositivos. Incluso tras haber limpiado los dispositivos, todavía despedían un olor fétido en la pobremente ventilada habitación.

"Bien, ¿Qué estamos viendo?" preguntó Mokoa mientras miraba por encima del hombro de Jace a los gadgets rotos. Dio un paso atrás tan pronto como se dio cuenta de que ella olía tan mal como la basura del contenedor.

"Para empezar, tenemos que encontrar qué sistema operativo utilizan estas cosas", contestó Jace sin mirar a Mokoa.

"¡Pero puedes saberlo si miras en las tapas! Este funciona con IMO porque lo fabricó Anvil y tiene el logotipo de Anvil, y el otro funciona con Robot. Lo pone justo en la parte de atrás de esa cosa."

"Amigo, sólo porque haya sido fabricado y embalado por una marca no significa que ejecute ese sistema operativo. Puedes rootear el dispositivo, ponerle el sistema operativo que quieras, y añadir modificaciones a los circuitos internos usando EEPROM para permitir un arranque dual. Y no vayas a decirme que eso sólo pasa con los teléfonos piratas que falsifican en Hinad. Nunca puedes saber lo que hay en estas cosas".

Mokoa dio otro paso atrás y dijo "De acuerdo, daré un paso atrás y cerraré la boca"

"No, no lo harás", dijo Jace. "No puedes estar más callado de lo que yo lo estoy. Te enseñaré los pasos que hay que seguir para conseguir los datos. Busca una silla" dijo Jace sabiendo que la única silla disponible estaba en la cocina.

"¡Ah! Y ya que vas a buscar la silla, tráeme unas galletas y un vaso grande de agua fría".

Mokoa ya conocía el truco, porque sabía que Jace era una experta consiguiendo que hiciera cosas por ella.

Tuvo que ir y volver tres veces a la cocina para traer las galletas, el agua, la silla y un aperitivo para él. Finalmente pudo sentarse detrás de Jace para que comenzara la

lección.

"El 80% de estos dispositivos móviles ejecutan distintas versiones de dos sistemas operativos: Robot o Anvil. Robot tiene millones de versiones, y cada una de ellas es ligeramente distinta dependiendo de quien fuera el fabricante del dispositivo. IMO lo fabrica sólo una compañía, así que no hay muchas diferencias en estos dispositivos móviles. Es mucho más sencillo sacar una imagen de Robot que de IMO, porque IMO es un sistema operativo cerrado y tiene una seguridad muy buena. Pero si alguien le hizo un Jailbreak a este dispositivo, me llevará menos tiempo conseguir el pin encriptado"

Mokoa no entendía todo lo que le contaba Jace, pero sabía que no podía interrumpirla mientras trabajaba; ya le preguntaría cuando hiciera una pausa para beber o comer una galleta. Mientras tanto, se quedó en silencio y observó cómo trabajaba.

Jace continuó: "Cada sistema operativo almacena los datos de una forma distinta. Por suerte Robot se desarrolló basándose en el kernel de Linux, y es fácil descargar el Software Developer Kit (SDK) de la web de los creadores de Robot. Es prácticamente software Open Source. IMO no. Si el teléfono o el tablet funcionan con IMO y el usuario utilizó un PIN para bloquear el equipo, nos costará más trabajo. No es imposible recuperar los datos, pero implica que hay que dedicarle más tiempo".

Jace sacó un ordenador portátil de su mochila; A Mokoa le tocó de nuevo preparar las cosas que necesitaban. Jace levantó la tapa del portátil y arrancó los programas mientras buscaba cables USB en el cajón de su escritorio. Mientras tanto, Mokoa se acercó y pulsó los botones de cada uno de los dispositivos destrozados. Ninguno parecía funcionar.

"Escucha genio," le dijo Jace, "ya intenté hacer eso. No estaría buscando cables de conexión si esos trastos se hubieran encendido"

Mokoa se sintió un poco estúpido, como siempre. A Jace nunca se le olvidaban esos pequeños detalles, como intentar en primer lugar encender los equipos.

"¡Si! Encontré los dos que necesitaba. Espero que funcionen", dijo Jace mientras desenredaba los cables.

"Mmmh... Jace, ¿has pensado en ducharte antes de seguir con esto? Hueles mal, como el Sr. Tri" Mokoa no podía soportar ese hedor mucho más tiempo.

"¡MAL! ¿Piensas que huelo tan mal como el Sr. Tri? ¡Te vas a enterar de lo que es bueno!". Se dio la vuelta y agarró a Mokoa más rápido de lo que él esperaba al estar sentado justo detrás de ella.

"¿Qué significa esto? ¡Apestas y no puedo aguantar seguir sentado a tu lado! Me marcho y no volveré hasta que te duches y me pidas perdón por lo que me has hecho" dijo Mokoa mientras salía de la habitación de Jace. La puerta del apartamento se cerró de un portazo.

Molesta por la situación, olió su pelo y se sintió realmente mal por lo que le había hecho a su amigo. Jace se maldijo a sí misma.

Fin del juego

Comencemos con la diversión

Una parte fundamental del hacking es pensar en el proceso completo antes de tocar el teclado

- ¿Cómo vas a entrar en tu objetivo?
- ¿Qué controles necesitas desactivar o monitorizar mientras visitas esa red?
- ¿Qué quieres y cuál es la localización de ese objetivo?
- ¿Cómo vas a transferir los datos y dónde vas a guardarlos?
- ¿Qué registros y auditorías necesitas reiniciar al salir para cubrir tus huellas?
- ¿Quieres mantener los datos por tu seguridad y para usarlos tú exclusivamente?

La ingeniería social es una herramienta excelente para conseguir acceso a redes y localizaciones físicas. El reconocimiento es una forma estupenda de ser inmune (a todas o en parte) de ellas.

Reconocimiento

Reconocimiento es aprender las vulnerabilidades de las redes y el tipo de servidores a los que te enfrentarás. ¿Qué medidas de seguridad se usan y cuáles son sus vulnerabilidades? ¿Puedes hacer que esos dispositivos de seguridad se conviertan en una ventaja? ¿Dónde se almacenan los registros de red y auditoría? ¿Vas a instalar un backdoor para volver más adelante? ¿Cuáles son los vectores de ataque con los que te sientes cómodo y cuales funcionarán en cada red?

Vulnerabilidades software y hardware

Puedes conocer todos los exploits y vulnerabilidades de cada producto visitando http://www.cvedetails.com/ o www.cve.mitre.org/. Ambos sitios deben formar parte de tu metodología de ataque para aprender todo, tan pronto como sea posible, sobre el entorno al que te enfrentas.

OpenVAS

OpenVAS (http://www.openvas.org/) es un scanner y un gestor de vulnerabilidades open source. Las organizaciones disponen de bases de datos con tests de vulnerabilidades de red (**Network Vulnerability Test – NVT**) que se emplean para actualizar el escáner diariamente. Esta "compra rápida" de vulnerabilidades se puede comparar con CVE, pero sin toda esa jerga técnica. El software es una colección de herramientas que puedes ajustar para cubrir tus necesidades, incluso si sólo quieres saber qué vulnerabilidades se encuentran en una versión del servidor web Apache.

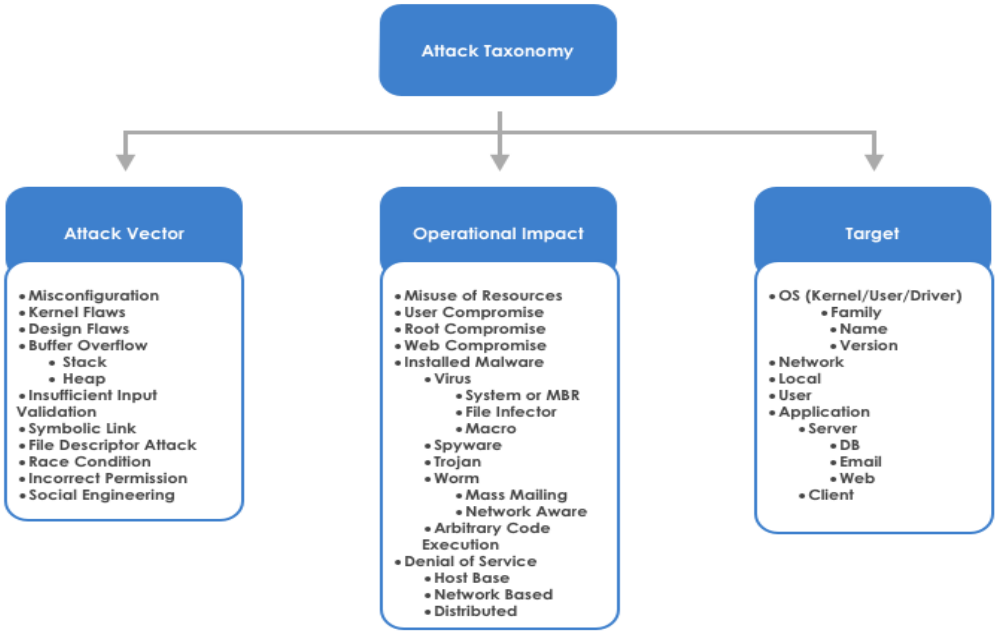

Figure 8.3: Attack Taxonomy

Attack Vectors (Vectores de ataque): Son los métodos para entrar en las redes, usando varias herramientas o vulnerabilidades conocidas. Con frecuencia encontrarás este término junto a la palabra "malware", dado que los que los vectores de ataque se ven principalmente como puntos de entrada maliciosos por los profesionales de la seguridad. En el uso que daremos a este término, sólo te mostraremos los distintos caminos para entrar en una red, dentro de una categoría en concreto. Repite conmigo, "No usaré los vectores de ataques para instalar malware." Levanta tu mano derecha como un juramento oficial cuando lo digas, igual que si estuvieras jurando o prometiendo un cargo. Este es el tipo de cosas que pueden llevarte a la cárcel, y no nos gustaría tener que ser nosotros los que tuviéramos que hacerlo.

Armas para hackear redes

Blackhole es un paquete de exploits que se instalan con un simple "clic" de ratón, destinado a proporcionar a un hacker con cualquier nivel de conocimientos distintas formas de obtener acceso de administrador a una red. Al contrario que otros programas de exploits, Blackhole 1.0 se ganó cierta reputación en la industria de la seguridad porque el programa disponía de varias vulnerabilidades zero-day. Los creadores de la versión 2.0 prometieron incorporar "URL dinámicas" proporcionadas por otra empresa de AV, que permitirían desarrollar exploits a tu medida

http://malware.dontneedcoffee.com/2012/09/blackhole2.0.html Cuesta $50 por un día de uso ¡Toda una ganga!

THC-Hydra 7.3 se actualizó en Mayo de 2012; Hydra se utiliza para crackear las contraseñas de login en red. El programa dispone de varios switches excelentes que podrás emplear en la línea de comandos de Linux. Este programa puede ejecutarse a través de un proxy (para ocultar tu localización), mediante FTP, IRC, HTTP y otros muchos protocolos.

http://www.thc.org/thc-hydra/

Metasploit es un software para tests de penetración de la comunidad Open Source. Aunque hay distintas variantes comerciales de Metasploit, el que querrás utilizar es el libre. Como muchas otras herramientas de comunidad, Metasploit dispone de una gran librería de add-ons, plugins y configuraciones. Muchos profesionales de la seguridad consideran esta herramienta como imprescindible en su arsenal. Querrás tenerla, porque se añaden continuamente nuevos exploits al motor.

http://www.metasploit.com/

Fedora Security Lab es otro proyecto de comunidad enfocado a la educación y la ejecución de pruebas seguras. Fedora es personalizable hasta el punto de permitirte elegir las herramientas que quieres usar y las quieres utilizar para experimentar en un sandbox. Como muchas otras herramientas de seguridad, el paquete viene en formato ISO y puedes grabarlo en un CD o instalarlo en una memoria USB. El conjunto de herramientas llamado **spins** está repleto de software profesional de seguridad Open Source.

http://spins.fedoraproject.org/security/#home

Cain and Abel es la herramienta definitiva para el Script Kiddie. Cain estaba diseñado originalmente como un programa independiente para recuperar contraseñas de volcados SAM (Archivos de contraseñas de Windows). Es programa sigue siendo excelente para ejecutar esta tarea, solo que encontrar a alguien que siga utilizando una versión obsoleta de Windows es difícil. Abel se creó para incrementar la utilidad de la herramienta y generar un paquete para pruebas de penetración. Esto dos programas trabajando en conjunto te permite acceder fácilmente a redes inseguras

http://www.oxid.it/cain.html

Fyodor incluye las 125 mejores herramientas para seguridad de red. La lista ha estado disponible desde hace años, y se ha ido actualizando (bueno... más o menos). La página web no sólo te proporciona una breve descripción de cada herramienta, sino que también te da un enlace al software. Algunas de las herramientas son bastante antiguas, pero te resultarán muy útiles si trabajas todavía trabajas con FORTRAN o usas un ábaco. Comprueba el sitio regularmente, por lo menos una vez cada dos años, para ver las nuevas herramientas de las que ya has oído hablar.

http://sectools.org/

El proyecto **Open Web Application Security Project (OWASP)** es de la misma gente que te proporciona Hacker Highschool e ISECOM. Todo lo que quisiste saber acerca de la seguridad en la web está explicado detalladamente y con ejemplos. Este tipo de información requiere algún esfuerzo por tu parte. Tendrás que estudiar, no es como en las clases de "Economía doméstica", pero si mucho más interesante.

Si miras el apartado "a Vision for OWASP" en su página principal, te encontrarás con que hay "Builders", "Breakers", y "Defenders". ¿Cuál quieres ser tú? ¡Recuerda de darle las gracias a "Pete Herzog" cuando aprendas algo nuevo!

https://www.owasp.org/

Ejercicios

8.32 Ve a la web de Metasploit y descarga la versión más reciente. Graba la ISO en un CD o instálala en un USB.

Los chicos de Metasploit han puesto a disposición del público un servidor vulnerable que te permitirá trabajar con Metasploit sin meterte en problemas. Este servidor se llama "Metaploitable." Usa Metasploit para crear una cuenta en

Metasploitable y prueba tu nuevo software para pruebas de penetración. http://updates.metasploit.com/data/Metasploitable.zip.torrent

El juego continúa: Arreglándose para el "Gran Pestazo"

Jace necesitó tres días para quitarse el olor a basura de encima, y tres más para disculparse con Mokoa. Se sentía sola sin tenerle a su alrededor, incluso cuando le hizo prometer que nunca más le tocaría la cara. Le dolía el alma, y empeoraba cada vez que pensaba que podía perder a su mejor amigo; tendría que tener cuidado cuando estuviera con él. Siempre consideró que su amistad era algo permanente dado que siempre habían estado juntos. Durante seis días estuvo sola y no le gustó la sensación de estar sin Mokoa. Esa cruel ausencia cambió la forma en la que pensaba sobre él.

Mokoa accedió por fin a encontrarse con Jace en su apartamento para continuar las investigaciones sobre los dispositivos móviles. No le resultó sencillo estar junto a Jace: actuaba de forma distinta a la habitual, como si hubiera algo nuevo en ella. Estaba más simpática y le hablaba con un tono más tranquilo. Incluso le miraba a los ojos cuando le hablaba. Jace nunca había hecho eso antes. No estaba seguro de cómo tomarse esta nueva personalidad, pero le gustaba su amabilidad.

De vuelta en el laboratorio, Jace puso su silla de forma que Mokoa pudiera ver lo que estaba haciendo en la mesa de su cuarto. Incluso tenía leche y galletas preparadas en la mesa para compartirlas con él. Mokoa puso una cara rara mientras pensaba qué narices le estaba pasando.

Jace miró a Mokoa, lo que le sorprendió, ya que normalmente sólo le veía la nuca cuando estaba trabajando con ordenadores. Jace comenzó a hablar "¿Recuerdas los dos dispositivos móviles que sacamos del contenedor de basura de la escuela la semana pasada?"

Mokoa asintió, suspicaz. Entrecerró sus ojos marrones mientras comprobaba la habitación por su hubiera trampas explosivas o cámaras ocultas. "Esto tiene que ser una broma", pensó. "¿Qué estará tramando?". Jace siguió la conversación cuando retomaron el contacto visual.

"Primero, tenemos un teléfono móvil dañado y al que le quitaron la tarjeta SIM antes de tirarlo a la basura. Lo he limpiado, así que ya no huele mal".

Mokoa no se había dado cuenta del olor a fresco en la habitación hasta que ella mencionó que había limpiado el teléfono. La habitación parecía distinta, más femenina. Olía y tenía un aspecto como si alguien más viviera allí, porque Jace nunca tuvo su habitación tan limpia como ahora. Un aroma a pino y jazmín flotaba en el aire a su alrededor. Era un buen cambio, sabiendo que antes olía como el armario de los zapatos. "¿Dónde estará la cámara oculta?" pensó.

Jace se puso derecha, corrigiendo su mala postura habitual. Con la espalda bien derecha en la silla del despacho y los dos dispositivos frente a ella, comenzó con la lección.

"Hay dos formas de enfrentarse a este reto. Podemos intentar recuperar pruebas sobre el crimen, o podemos intentar ver lo que podemos sacar de estas cosas. Si intentamos hackearlos para obtener datos del teléfono, no nos importará dañarlo aún más. Pero si vamos a ejecutar un análisis forense para obtener pruebas válidas del crimen, tenemos que ir comprobando un buen montón de pasos para conseguirlas"

Mokoa frunció el ceño ante la idea de tener que pasar por una larga y tediosa lista de comprobación de cada paso. Jace se dio cuenta de lo que le preocupaba y

dijo "No te preocupes; voy a explicarte algunos de los métodos forenses. Por el momento sólo estamos interesados en ver qué tipo de datos se dejaron en cada dispositivo".

"No dejes el teléfono o la tablet conectada a una red antes de empezar. Usa cualquier cosa que puedas imaginar para impedir que el dispositivo se conecte a una de las antenas de telefonía o una red WiFi. Eso implica usar papel de aluminio, contenedores de plomo, jaulas de Faraday y cajas metálicas que puedan bloquear las señales de radio. Los teléfono móviles subirán la potencia de la señal para intentar conectarse al operador."

Mokoa intentó añadir algo inteligente a la conversación, para demostrar que estaba prestando atención: "¿Y qué tal si los ponemos en modo Avión?"

"¡Espera! ¡Para"" Jace salto de repente de su silla. Metió la mano en el bolsillo de su pantalón y sacó su teléfono móvil con la pegatina de las tibias y la calavera en la parte de atrás.

Mokoa sabía que esto era parte de la broma y dijo "¿Qué pasa? ¿A qué viene todo eso de parar y esperar?"

Jace no se molestó en mirar a Mokoa mientras apretaba los botones del teléfono para apagarlo. "Amigo, antes de empezar, tenemos que apagar nuestros teléfonos y cualquier cosa que tenga una señal de conexión, como Bluetooth, WiFi o similar. No podemos dejar que los dispositivos intenten conectarse a algo que esté a nuestro alrededor". Mokoa apagó su teléfono.

"Si usamos el modo Avión para impedir que se conecte al operador, necesitamos trabajar rápido, porque muchos dispositivos se pueden borrar remotamente si se conectan a la antena de telefonía"

"Y además la memoria interna del teléfono es limitada, lo que significa que sin una tarjeta SIM instalada, el teléfono sólo recordará las últimas llamadas que se realizaron. Un criminal inteligente intentará esconder los datos de llamada del teléfono llamando a su número docenas de veces para intentar sobrescribir el registro del teléfono".

"Si necesitamos una imagen forense de la tarjeta SIM, la copiaremos antes de encender el dispositivo. Cuando un dispositivo se enciende se inician decenas de aplicaciones y los datos del teléfono se actualizan constantemente. Esto puede invalidar cualquier prueba que intentemos recuperar si queremos que tenga fines legales. Por supuesto, eso es lo último que se me pasa por la cabeza. No quiero a nadie relacionado con la ley cerca de mí mientras hago estas cosas. Sólo quiero los datos porque soy curiosa."

"Podemos obtener una imagen del iPad usando el kit de conexión para la cámara, lo que me permitirá utilizar dispositivos de almacenamiento USB. En cuanto el iPad detecte que la unidad USB que estoy conectando tiene un directorio llamado /DCIM, lo montará y leerá la unidad. Los iPads pueden montar y leer particiones en FAT y HFS mediante el protocolo Picture Transfer Protocol (PTP) como enlace de comunicaciones. Se puede acceder a los iPods e iPhones usando el cable USB. Los datos de usuario están almacenados en una zona de la partición del dispositivo de estado sólido: el directorio /private/var."

"La parte divertida sobre el software forense comercial, es que utilizan exploits o vulnerabilidades poco conocidos es ese sistema operativo. Tan pronto como el fabricante del dispositivo parchee ese agujero, ese software tan caro resultará inútil

hasta que lo actualices".

"Y por cierto, amigo mío, no pienses ni por un instante que la policía no tiene acceso a herramientas y software para examinar estas cosas. Los fabricantes de móviles, las empresas de telefonía y los ISP mantienen registros de tus datos para proporcionarle información a la policía. Si no tienen los datos, la empresas ofrecen las herramientas para obtener esa información personal de los dispositivos que venden"

Mokoa quería que Jace tomara aliento un instante; su cara se estaba poniendo azul de tanto hablar. "Entonces, ¿estás tratando de decirme que toda esa privacidad que pensamos que tenemos es mentira, o que puede romperse si alguien tiene una orden judicial?"

Jace contuvo la respiración y abrió sus ojos como platos: "Amigo, ni siquiera necesitas una orden judicial"

Mokoa se dio cuenta de que esta conversación iba camino de convertirse en una lección sobre los derechos de privacidad. Estas lecciones suelen ser muy profundas y necesitaría el 100% de su atención mientras Jace hablaba, de otra forma repetiría la clase para asegurarse de que había entendido cada palabra. Esto iba a ser un día muy, muy largo.

Fin del juego

Contramedidas forenses

El software de contramedidas forenses intenta eliminar los archivos de registro y/o borrar todos los datos que pudieran haber sido alterados durante la visita a la red. Ambos métodos pueden hacer saltar las alarmas si no se usan correctamente y, como consecuencia, recibirás la visita de un grupo especial de la policía muy cabreado porque no han tenido tiempo de tomar su café mañanero. Estas herramientas de contramedidas se utilizan principalmente sobre un único equipo para eliminar, esconder, camuflar y, por lo general, hacer el trabajo de los analistas forenses más difícil... o imposible.

Hay unos cuantos detalles que la persona que quiera usar software de contramedidas forenses debe tener en cuenta. El primero de ellos es que los analistas forenses nos daremos cuenta de que se ha empleado este tipo de software en el equipo. Sólo con esto, ya tendremos sospechas sobre porqué se ha empleado este software si no hay nada que ocultar.

Segundo, tienen que localizar y borrar cada bit de información que pueda quedar en los archivos de intercambio, directorios temporales, archivos de paginación y cualquier otro dato residual que puedan conectarles con el hack.

Tercero, los analistas forenses pueden cobrar tanto una nómina como hacerlo facturando las horas trabajadas. Se nos paga, principalmente, para recopilar pruebas suficientes como para condenar a alguien. Si alguien crea un reto para recuperar las pruebas forenses que implique dedicar demasiado tiempo como para conseguir las suficientes en su contra, seguramente el análisis se detendrá en algún momento. El tiempo es dinero. Pero esa persona necesitará dedicar mucho tiempo para añadir trabajo extra a las tareas de los analistas forenses, ahora y la próxima vez que lo intente, a menos que quiera pasar una buena temporada trabajando muy duro en un lugar poco soleado. Y ya sabes a que nos referimos.

Por cierto, los analistas forenses tenemos nuestro orgullo y nos encantan los retos: nunca descansamos hasta que hemos resuelto el caso, aunque tengamos que dedicar nuestro tiempo libre a ello.

Quién tiene ventaja

Los criminales tienen muchas oportunidades de usar contramedidas forenses en un dispositivo. Estas incluyen:

- Muchos forenses no saben cómo lidiar con usuarios avanzados que conocen cómo manipular el sistema operativo o saben esconder información. La demanda de nuevos profesionales forenses está dando como resultado unos procesos "listos para cocinar" donde los estudiantes van a un par de clases y se les entrega un software que es el que deben utilizar. Esto deja la experiencia necesaria en manos de los fabricantes de software.
- El software forense no tiene establecido un estaádar científico para los procesos de recopilación, análisis y resultados que sea repetible. Diferentes software devolverán distintos resultados. Además, esos resultados no pueden reproducirse. Y esto está mal, muy mal.
- No existe algo así como unas áreas comunes de conocimientos entre los expertos forenses digitales. Esto es como decir que hay varias formas de cortar una manzana: ninguna es correcta o incorrecta. No existe un método establecido para realizar un examen forense o incluso publicar los resultados.

- Tanto los analistas forenses digitales como el software y el hardware no han sido diseñados para trabajos de campo. Fueron creados para trabajar en un bonito y limpio laboratorio, con las condiciones perfectas y con todas las herramientas que puedan necesitar a su disposición. En el mundo real, esto no ocurre nunca.
- Cualquier pequeña alteración en la prueba, como una actualización del sistema o cambiar la hora del sistema puede hacer que los datos recopilados sean inútiles. Esos datos no se aceptarán en un tribunal debido a que se han visto afectados por un cambio.

Tienes que ser social

Facebook, Twitter, Google, Tumblr y todos esos sitios con redes sociales son parte del almacenamiento en la nube. Cada uno de ellos ofrece un acceso sencillo a los usuarios para comunicarse con amigos, conocer nuevas personas, compartir ideas, publicar fotografías, imprimir calendarios y socializar en un entorno digital. Muchos de estos proveedores en la nube parecen estar regalando sus productos sin prestar atención a sus beneficios. Parece que "todo es gratis".

La idea es muy sencilla: proporcionar un entorno en línea donde la gente pueda interactuar proporcionándoles los medios para expresarse en un entorno que los usuarios piensan que es privado. Cuantos más usuarios se unan a la fiesta, se reúne más información sobre cada uno de ellos para crear material de marketing a su medida. El servicio en la nube puede entonces vender ese material de marketing personalizado a los anunciantes o fabricantes de productos directamente. Podrías argumentar que se trata de un modelo de beneficios mutuos, ya que los usuarios obtienen un espacio para socializar y los servicios en la nube ganan lo suficiente como para continuar con el negocio.

Por supuesto, esta no es la única forma en que estas redes sociales ganan dinero. Facebook anunció hace poco que cuenta con mil millones de usuarios. Con tanta gente accediendo a su red alrededor de todo el mundo, Facebook se ha convertido en la mayor base de datos de fotos e identificación de personas del planeta. Todo lo que se publique en cualquiera de esas redes sociales pasa a ser propiedad de ese servicio. Y toda esa información personal está valorada en una cantidad tremenda de dinero.

Piensa en las redes sociales de esta forma: si no te están vendiendo nada, entonces te están vendiendo a otra persona. Tú eres el producto.

Con la cabeza en las nubes

Las leyes, herramientas y técnicas forenses no funcionan en un entorno de nube. Principalmente debido al diseño del entorno, cualquier análisis forense implicará recursos compartidos. Esto significa que cuando un analista forense intente conseguir pruebas del sospechoso, también se incluirá información datos de otras personas. Esto no significa que un ataque contra un servicio en la nube no se vaya notificar o investigar. El proveedor de la nube llevará a cabo su propia investigación y comprobará los aspectos legales. Los delitos que impliquen una cuenta, un sospechoso, una víctima o un evento serán difíciles de investigar porque el proveedor podría no estar dispuesto a ayudarte. Pero como siempre, depende del bando en que te encuentres.

Problemas con los análisis forenses en la nube

1. No hay jurisdicción sobre los datos. Muchos proveedores tienen Centros de Datos en distintos lugares alrededor de todo el planeta.

2. El número de dispositivos móviles accediendo, cargando, creando, alterando y moviendo datos en la nube va en aumento. Esto significa que los datos pueden estar en varios sitios a la vez al mismo tiempo.
3. No existe un puesto de gestión que te ayude a filtrar sospechosos. No eres el propietario del almacenamiento de datos, sólo lo estás alquilando.
4. No existe un control de acceso que te permita mantener los datos aislados para realizar un análisis forense. Los clientes pueden acceder a los datos, en cualquier momento, a cualquier hora y desde cualquier sitio.
5. Falta de una infraestructura física para crear una línea de tiempo o determinar las marcas de tiempo o registrar eventos.
6. Las condiciones y términos de uso entre la organización y el proveedor de la nube puede que no te permitan realizar una investigación forense que se ajuste a tus necesidades.
7. Obtener una prueba sin modificarla es extremadamente dífcil.
8. Cada servicio de nube tiene normas para el almacenamiento de datos y condiciones de servicios diferentes a los de los demás.

Si el crimen se ha cometido contra el proveedor de la nube, este tiene jurisdicción sobre esas actividades criminales. El cliente puede tener un acceso limitado o nulo a los datos en la nube; lo que es más, la red social es la propietaria de esos datos. Este es el caso de servicios como Facebook, donde el usuario puede manejar el contenido, pero este es propiedad del servicio de la nube.
¿Te ha sorprendido saber que tu contenido de usuario es propiedad de la red social? ¿O quizás no?

Ejercicios

8.33 Hay un par de técnicas que te servirán si quieres identificar al remitente de los datos, salvo que este remitente esté utilizando un proxy. Hay ciertos add-ons para Firefox y Chrome que te permiten ver el contenido de una fuente HTTP. ¿Cómo podrías usar esta información para bloquear al emisor? Hazlo en tu navegador.

Conclusiones

El análisis forense digital no es una tarea sencilla, ni una profesión fácil. Debes estar muy centrado en los detalles, ser capaz de documentar cualquier cosa que hagas a las pruebas que encuentres, pensar como un criminal y tener grandes dosis de paciencia para encontrar todas las pruebas. Aparte de esto, tienes que estar dispuesto y ser capaz de presentarte como un testigo experto si te llaman a testificar en un caso.

Por otra parte, tener conocimientos y experiencia en técnicas y herramientas forenses te pueden ayudar a mantener la privacidad y confidencialidad que has estado perdiendo rápidamente en este mundo digital.

Si eres lo suficientemente valiente como para terminar esta lección, ya sabes donde entran en juego los medios como fuente para esconder datos, arrancar un ordenador y esconder información en los datos o en el sistema operativo. Te hemos enseñado algunos lugares muy curiosos en los que puedes esconder información y sabes cómo frustrar a los expertos forenses.

El análisis forense está repleto de zonas en las que se requiere un conocimiento experto, o al menos una buena comprensión de esa área. Esta lección se diseñó para ofrecerte una muestra de lo que puedes encontrarte si quieres trabajar en este campo tan apasionante... o si sólo quieres ser un usuario con conocimientos.

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM