

Análisis forense: un caso ilustrativo en la universidad

La ciencia forense aplicada a la informática es una especialidad fascinante que cada día tiene más difusión en el mercado de la seguridad. Tiene como objetivo la recolección, comparación, análisis y evaluación de datos procedentes de cualquier medio informático con fines judiciales, o la de informar adecuadamente al cliente acerca de las posibilidades reales de la evidencia supuesta o existente. En las siguientes líneas se resume una reciente actuación encaminada a constatar evidencias digitales en un contexto usualmente propicio en el germen de este tipo de incidentes: una universidad.



Las siguientes líneas se resume una reciente actuación encaminada a constatar evidencias digitales en un contexto usualmente propicio en el germen de este tipo de incidentes: una universidad.

Román Ramirez / José Manuel Medina

El contenido de este artículo muestra una experiencia de un proyecto de análisis forense realizado en una Universidad. El personal técnico de esta Universidad solicitó los servicios de personal especializado, tras detectar un posible incidente de seguridad por parte de uno sus profesores. Dicho profesor informó que llevaba días teniendo extraños problemas con su correo electrónico, con desapariciones de mensajes de su buzón de correo, y otras anomalías.

Una de las primeras fases en la analítica forense es la de confirmación del incidente, es decir, el primer paso es *demonstrar* que se ha producido un incidente de seguridad. No debemos olvidar que en muchas ocasiones el afectado sospecha de un presunto atacante y las evidencias pueden llevar a demostrar, simplemente, un error de gestión.

Generalmente la demostración de que un incidente ha ocurrido suele ser trivial (pensemos en ataques a sitios web donde ha quedado un *graffiti* como evidencia clara de que el incidente ha ocurrido). En el caso de "La Universidad", la demostración no fue un asunto trivial, ya que aparentemente el problema de seguridad estaba restringido al correo-e de este profesor.

Detección del incidente

En un caso forense tradicional, uno de los primeros pasos habría sido acotar la escena del crimen, e impedir el acceso a los servicios que se prestaran a través de ella. En este caso fue imposible, debido a que las máquinas implicadas, por requerimiento de "La Universidad", debían mantener el servicio permanentemente en funcionamiento.

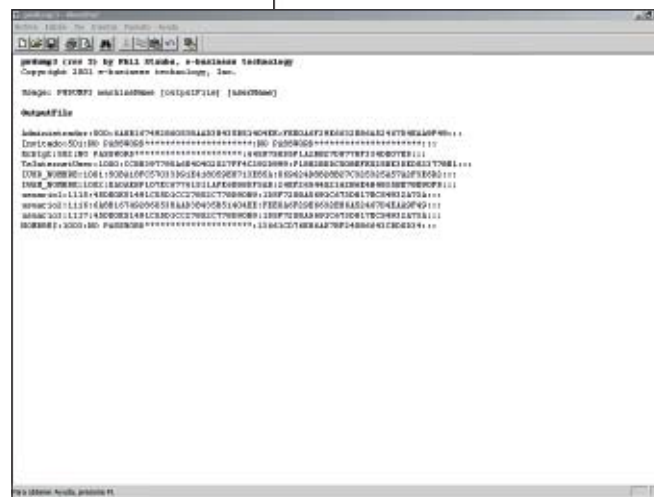
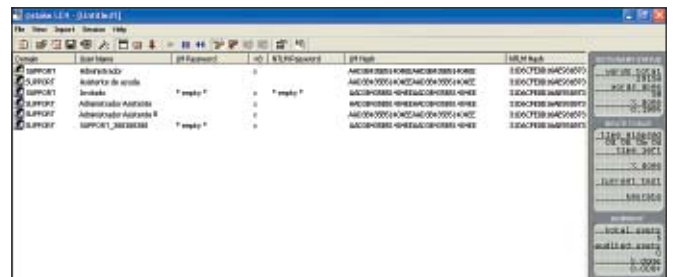
También, se partía de un supuesto en el que el posible incidente se había producido días antes, lo que invalidaba automáticamente todas las evidencias volátiles (memoria de los sistemas, ficheros temporales, etc.).

Se decidió recopilar los archivos históricos (*log*) de todas las máquinas involucradas (servidores de correo entrante y saliente, y servidores de correo Web), así como de todas las máquinas "en tránsito" (que ac-

tuaran como enrutador, *proxy* o cortafuegos, frente a las involucradas).

Desafortunadamente los enrutadores y los cortafuegos no almacenaban ninguna información de los archivos históricos de las conexiones, lo que centró el foco de investigación en los históricos de las máquinas servidoras de correo y de correo Web.

El servidor de correo, tanto para pop como para smtp, se ejecutaba sobre plataforma Linux, con la aplicación Courier (de amplia distribución). Para la gestión del correo Web, se había instalado la aplicación sqwebmail.



Dando por sentado que en los históricos de smtp no se encontrarían detalles sobre el incidente, se dedicó la mayor parte de los esfuerzos a examinar exhaustivamente los de pop.

Previamente, se habían revisado las máquinas del despacho del profesor en cuestión, así como la de los demás profesores, y se habían obtenido las configuraciones de correo de todos, así como sus direcciones ip.

Inicialmente se realizó un filtrado ex-

haustivo de todas las conexiones realizadas por el profesor en cuestión, y se observó que todas las conexiones se habían originado en su máquina (y ninguna a través de correo Web), excepto un grupo de conexiones en días alternos, de las que citamos algunas:

Oct 5 10:12:10 correo pop3d: LOGIN, user=profesor@universidad.es, ip=[::ffff:192.168.204.22]

Oct 5 10:12:10 correo pop3d: LOGOUT, user=profesor@universidad.es, ip=[::ffff:192.168.204.22], top=0, retr=0

Oct 6 17:33:28 correo pop3d: LOGOUT, user=profesor@universidad.es, ip=[::ffff:192.168.204.22], top=0, retr=0

Oct 6 17:33:28 correo pop3d: LOGOUT, user=profesor@universidad.es, ip=[::ffff:192.168.204.22], top=0, retr=0

La dirección de la máquina del profesor pertenecía a un segmento de red completamente diferente (172.16.10.18), y tras una breve consulta se averiguó que esa dirección de red interna, pertenecía a una de las aulas públicas, donde los alumnos podían trabajar con los ordenadores de "La Universidad".

Además, el profesor había confirmado que siempre leía el correo desde la máquina de su despacho.

En este punto se conocían dos aspectos importantes: una posible máquina atacante, y la confirmación de que se

había producido un incidente.

La máquina sospechosa

Una vez obtenido permiso para trabajar sobre la máquina sospechosa y las máquinas relacionadas, y a última hora del día (para evitar coincidir en el aula con alumnos) se procedió a investigar la máquina en cuestión.

El sistema operativo de los equipos en las aulas, Microsoft Windows 2000 Profesio-

nal, estaba limitado para evitar potenciales problemas de seguridad, de manera que en teoría los alumnos sólo podían dar uso a herramientas aprobadas e instaladas por "La Universidad".

Como primer paso, se decidió proteger las evidencias realizando un volcado físico del contenido del disco duro de la máquina sospechosa (partiendo del supuesto de una escena corrupta, ya que los equipos del aula eran compartidos por decenas de alumnos). De esta manera, conectando un disco externo a la máquina y utilizando herramientas forenses se protegió el contenido del disco.

Una vez terminada la copia, se procedió a examinar la máquina objeto de estudio, en busca de evidencias, y tras unos minutos de trabajo, fue evidente que realizar la copia del disco había sido innecesario (pero un paso obligatorio para proteger las evidencias; en otras circunstancias las evidencias obtenidas del disco habría sido imprescindibles).

Dentro del disco, se encontró un directorio oculto, donde aparecieron una serie de herramientas conocidas para el equipo de seguridad:

`pwdump3.exe` `enum.exe` `nmap.exe`
`ngrep.exe` `lc4.exe`

Además, se descubrió una herramienta programada en C (el código fuente se encontraba en el directorio), que podía realizar conexiones al puerto de correo pop (110/tcp) con el nombre de usuario y la contraseña como parámetros.

Observando las herramientas, una de las preguntas que había estado en la mente del equipo de seguridad desde el principio, quedaba probablemente resuelta, ¿cómo había obtenido el presunto atacante la contraseña?

La respuesta podía encontrarse en la herramienta "ngrep". Ngrep es una herramienta que busca patrones de cadenas de texto en paquetes de red, actuando como un analizador de protocolo (sniffer).

Pero, ¿cómo era posible que mediante ngrep hubieran obtenido la contraseña, si el profesor no había leído el correo desde ese mismo segmento de red? Tras realizar una llamada al profesor en cuestión, se confirmaban las sospechas del equipo de investigación. Las contraseñas utilizadas para acceder a la red Microsoft y para acceder a leer su correo eran las mismas.

La herramienta `pwdump3` permite obtener contraseñas de máquinas Microsoft Windows NT en remoto, y la herramienta `lc4` (`L0pht Crack`) permite, a través de sofisticados ataques de diccionario y fuerza bruta, romper esas contraseñas.

La hipótesis

El presunto atacante había obtenido una forma de desbloquear el acceso al sistema operativo de la máquina local, obteniendo

de alguna forma privilegio de administrador en esa máquina local (probablemente reiniciando la máquina con algún tipo de disco de arranque especial).

Una vez obtuvo el privilegio necesario, copió al disco local las herramientas que necesitaba y realizó una prueba de la máquina que le autenticaba en el dominio (el Controlador Primario de Dominio).

Obtuvo una lista de usuarios y contraseñas cifradas del dominio e intentó "romperlas" con la herramienta `L0pht Crack`, y de hecho, obtuvo por lo menos la contraseña del profesor afectado por el incidente.

Una vez obtenida la contraseña, el presunto atacante se decidió a verificar que las contraseñas de correo y de acceso a la red Microsoft eran las mismas, y una vez confirmado, desarrolló su propia herramienta, que le permitía obtener el correo del profesor y volcarlo a un fichero de texto.



La trampa

Tras desarrollar esta hipótesis, se procedió a verificarla instalando herramientas de captura de tráfico y control de red, así como herramientas de alerta que notificaran cuando se dieran las circunstancias que se estaban esperando. En ese momento, se contactó con el profesor y se le solicitó que cambiara las contraseñas de acceso a la red Microsoft y al correo por la contraseña, "xPxRzXzR11", de manera que nuestro potencial atacante, detectando el cambio en la contraseña, procediera a repetir la secuencia de acciones que le llevaron a capturar la anterior.

Las herramientas de captura utilizadas, estaban preparadas para que en cuanto se detectara la cadena de texto, "xPxRzXzR11", avisaran vía mensaje de correo electrónico a una persona del equipo.

En el mismo día en que se puso en marcha la trampa, se recibe confirmación, y se observa que desde la máquina en cuestión nuestro presunto atacante había enviado un paquete de red con la cadena de texto trampa. De inmediato, y acompañados por el profesor y el jefe del departamento de informática, se accede al aula de prácticas, en la que se descubre a un alumno sentado en la máquina "sospechosa".

La investigación no habría servido para mucho, si el equipo de seguridad no hubiese observado que el alumno había conectado una unidad ZIP externa a la máquina de la sala.

La captura

Hay un principio muy importante en la ciencia forense, el principio de **Locard**, que dice, "Cada contacto deja un rastro". La interpretación de este principio es que muchas veces se encuentran evidencias de que el presunto criminal ha estado en la escena del crimen, por los restos de "escena del crimen" que lleva consigo.

Tras informar al alumno de que se le había detectado realizando acciones no permitidas y consideradas ilegales por el código de "La Universidad", se le pidió que se levantara y cediera el sitio en el equipo. Tras acceder directamente a la unidad ZIP, se encontraron dentro de dicha unidad copias del correo del profesor (y de otros profesores y alumnos), así como copias comprimidas de directorios completos del servidor de dominio, y diversas herramientas de seguridad (herramientas de "hacking").

Tras una charla con el alumno, y una explicación por su parte, se confirmó que antes de desarrollar la herramienta que capturaba el correo, realizó una serie de pruebas con lectores de correo (lo que pudo llevar a que el profesor detectara la pérdida de los correos).

"La Universidad" zanjó el tema con una amonestación al alumno y la prohibición de acceder a las aulas públicas de informática. En caso de haber querido tomar acciones legales, "La Universidad" podría haber planteado un caso por una violación clara del artículo 197 del código penal español: Descubrimiento y revelación de secretos (entre los que se incluyen las contraseñas y el correo electrónico). ■

ROMÁN RAMÍREZ
Director General
Chase The Sun
rramirez@chasesun.com

JOSÉ MANUEL MEDINA
Director Técnico
Identra Ingeniería Tecnológica, S.A.
jmp@identra.com

ENLACES DE INTERÉS

@stake LC4
<http://www.atstake.com/research/lc/index.html>
Polivec pwdump3
<http://www.polivec.com/pwdump3.html>
Delitos Informáticos Guardia Civil
<http://www.guardiacivil.org/dtelematico/delitos/>