

Reto Forense Episodio III - Resumen Ejecutivo

José Salvador González Rivera

Puebla, México / Marzo 2006

Introducción

La idea de este resumen ejecutivo es mostrar los resultados de la investigación sobre un sistema comprometido para el concurso "Reto Forense Episodio III". El escenario básico a entender es el siguiente:

El administrador de sistemas de una pequeña empresa ha notado que existe una cuenta que él no creó en su sistema de ERP, por lo que sospecha de algún ingreso no autorizado, del que desconoce el alcance. El sistema en que se ejecuta la aplicación es un servidor Windows 2003, cuya principal función era proporcionar acceso al sistema ERP a través de la Web. Hace poco tiempo que habían migrado al uso de este servidor.

Según el administrador, trataba de mantener el sistema actualizado por lo que no sabe cómo pudieron ingresar a su sistema. Sin embargo, también mencionó que más de una persona tiene acceso a cuentas privilegiadas en el sistema y aceptó que ocupaban a veces estas cuentas para labores no sólo administrativas, sino también personales o para aplicaciones que no requerían ningún tipo de privilegio para ejecutarse.

Objetivos

El objetivo principal es determinar si existió un ingreso no autorizado, cómo ocurrió y el alcance del daño al sistema e información.

Evidencias

Se cuenta únicamente con la imagen del servidor Windows, sin más información adicional.

Herramientas utilizadas

El sistema operativo que utilicé fue *WindowsXP* por la única razón que es mi sistema operativo de escritorio y se pueden aprovechar sus utilerías; ya instalados tenía *TheCleaner* (AntiTrojans) y *Norton Antivirus*. Utilicé *MountImage Pro* (versión de prueba) para montar la imagen y *Cygwin* para trabajar bajo un entorno similar a Linux y aprovechar el uso de sus comandos de manera gratuita. También usé el programa gratuito *PC Inspector File Recovery* para la recuperación de archivos borrados y *QuickViewPlus* (versión de prueba) para la visualización de archivos sin abrirlos. Adicionalmente busqué y encontré *Windows Registry File Viewer* el cual es un programa gratuito para ver archivos del registro de *Windows* y *hfind/sfind/galleta* de Foundstone los cuales son *software* gratuito. No utilicé *suites* específicas para análisis forense, sino más bien, comandos y programas ordinarios.

Metodología

Esta es la primera vez que realizo un análisis forense por lo que busqué un método que me llevara de la mano, por lo que revisé el documento *Forensic Examination of Digital Evidence* del **NIJ** (U.S. National Institute of Justice) que consiste en:

- Preparar un directorio independiente para almacenar datos recuperados o extraídos.
- Extracción de información física (búsqueda de palabras clave) y lógica (recuperación y extracción).
- Análisis de datos de interés, aplicaciones, programas ocultos, código malicioso, etc.
- Conclusión del análisis.

El documento puede encontrarse en la dirección: <http://www.ojp.usdoj.gov/nij>

Es necesario destacar que toda la extracción de información puede ser verificada al repetirla tanto con las mismas herramientas como con otras que cumplan con la misma función, en cualquier momento, en cualquier equipo y con el mismo objetivo descrito en cada sección del reporte técnico para que el resultado sea el mismo.

Resultados

Este resumen muestra los resultados del análisis realizado sobre la imagen del servidor comprometido, para conocer lo que se hizo, se muestra la siguiente tabla con las actividades realizadas:

Actividad	Descripción	
Archivos de imagen	Se obtuvieron las imágenes del sistema de una fuente confiable, se verificó su integridad y se cargó el sistema de archivos en una estación de trabajo.	✓
Versión del sistema	Se verificó que el sistema operativo era un Windows 2003	✓
Listado de archivos	Se realizó un listado de archivos que había en el servidor.	✓
Detección de archivos ocultos	Se realizó un listado de archivos ocultos.	✓
Registro de Windows	Se verificó la existencia de bitácoras y registro interno.	✓
Programas instalados	Se verificó en el registro del sistema operativo que aplicaciones estaban o habían estado instaladas.	✓
Programas de los usuarios	Se verificaron los programas instalados o desinstalados de los usuarios.	✓
Programas usados	Se verificaron las modificaciones al registro del sistema operativo para conocer algún otro programa que hubiera sido instalado en el sistema.	✓
Tareas programadas	Se buscaron tareas programadas a futuro.	✓
Arranque de programas al inicio	Se buscaron programas que arrancaran al iniciar el sistema.	✓
Detección de código malicioso	Se buscaron programas que fueran dañinos al sistema.	✓
Detección de archivos escondidos	Se realizó una búsqueda de archivos escondidos en el sistema de archivos de Windows.	✓
Recuperación de archivos borrados	Se rastreó cualquier tipo de archivo borrado y se analizó su contenido.	✓
Revisión de memoria	Se revisó la memoria de intercambio del sistema. Esta memoria es un archivo que contiene datos binarios, pero que se tiene la posibilidad de reconstruir información a partir de identificar el texto encontrado.	✓
Rastreo de archivos temporales	Se rastrearon archivos temporales del sistema y de los usuarios.	✓
Investigación de usuarios	Se determinaron fechas de creación y logueo de cuentas, así como sus privilegios establecidos.	✓
Documentos y archivos	Se revisó la existencia de archivos temporales de internet, historial de navegación y sus vínculos en Favoritos.	✓
Recuperación de bitácoras	Se estudió el contenido de las bitácoras del sistema, así como de los programas MySQL y Apache.	✓
Análisis de información	Una vez extraída la información, se analizó y se escribió el informe.	✓
Conclusión del análisis	Se responde a las preguntas realizadas por el reto.	✓

El administrador de sistemas de quien se desconoce su nombre real, se encontraba en la oficina el día **domingo 5 de febrero** del presente año trabajando en el servidor con la cuenta **Johnatan** que pertenece a un usuario de nombre Johnatan Tezca. Al mismo tiempo se encontraba logueado al sistema *web-erp* con la cuenta **aconteras** que pertenece a un usuario de nombre Alberto Contreras Zacarías. A continuación se muestra el desarrollo de actividades importantes del día que se creó la cuenta de usuario en el sistema *web-erp* que el administrador no creó:

1:57 pm

Se registra una entrada lícita por el usuario **acontreras** al sistema *web-erp* desde una dirección de internet, el ingreso es registrado por *Apache* y por *MySQL* en sus respectivas bitácoras.

2:00pm

El usuario *acontreras* crea la cuenta **admin** en el sistema *web-erp*, este movimiento se registra por *Apache* y por *MySQL* en sus respectivas bitácoras.

2:19pm

El administrador de sistemas, quien también se encuentra logueado al sistema *web-erp* con la misma cuenta de usuario **acontreras**, lista los usuarios del sistema y se alerta por una cuenta de usuario que él no había creado. Este movimiento es registrado por *Apache* en su respectiva bitácora.

2:45pm

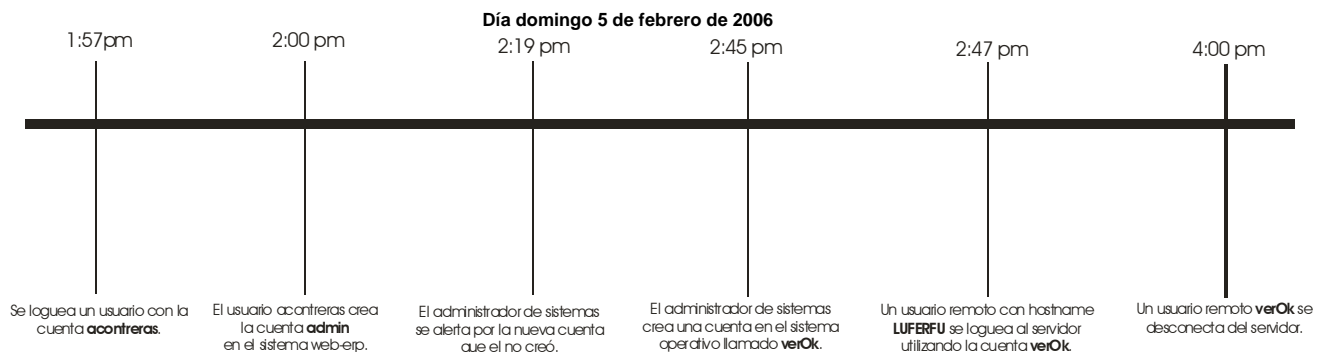
En el sistema *Windows 2003* el administrador del sistema crea una cuenta de usuario nueva con iguales privilegios que los demás, de nombre **verOk**. Posteriormente comprueba conectividad con un host remoto y ejecuta algunos comandos del sistema operativo.

2:47pm

Un usuario se logea a *Windows 2003* mediante la función de *escritorio remoto* con la cuenta **verOk** desde internet. Visualiza archivos de configuración del sistema *web-erp*, ejecuta *MySQL* y *MySQLAdministrator*. Posiblemente un usuario avanzado, amigo del administrador a quien le pidió ayuda. Quien no perdió la oportunidad de ver las fotos de las modelos desnudas de la cuenta *Administrator*. Estos movimientos se registran en las bitácoras del sistema operativo.

4:00pm

El usuario **verOk** se desconecta sin cerrar la sesión en el sistema operativo, este movimiento se registra en las bitácoras del sistema operativo.



Cabe destacar que la dirección de internet de **verOk** está en la misma red que el usuario que creó la cuenta **admin**, ambos del proveedor Verizon Internet ubicado en la ciudad de New York. También se debe mencionar que el nombre del host que se conectó con la cuenta **verOk** es *LUFERFU*, el cual rastreando a éste como un sobrenombre, la única persona asociada pertenece a Luis Fernando Fuentes Serrano con posibles correos: **1) luferru @ hotmail.com 2) lfuentes @ correo.seguridad.unam.mx 3) luis @ cancun.fi-a.unam.mx**

4:21pm

El administrador de sistemas, aún logueado con la cuenta **Johnatan** ejecuta herramientas para revisión de *spyware* y de respuesta a incidentes mediante un *secondary logon* (mediante la opción *Ejecutar como...*), sin embargo decide cerrar sesión y loguearse como *Administrator*. Nervioso se equivoca y logra entrar hasta el segundo intento. Vuelve a correr las mismas herramientas y procedió con el apagado del sistema a las **5:44pm**.

Conclusión del análisis

Partiendo de que solo se contaba con la imagen del sistema afectado, por razones ajenas a mi no se entregó la información volátil que obtuvo el administrador de sistemas antes de apagar el equipo a pesar de ser solicitada. Se pueden obtener más datos de la imagen del disco, sin embargo es suficiente la información obtenida pues se alcanzó el objetivo principal y ya se pueden responder las preguntas realizadas por el Reto-Forense:

¿El sistema ha sido comprometido?

Si ha sido comprometido, sin embargo no ha sido hackeado. Un usuario logró el ingreso mediante una cuenta de usuario válida con autorización y privilegios.

¿Quién (desde dónde) se realizó el ataque?

Un usuario ubicado en New York (Estados Unidos), con Verizon Internet Services Inc como Proveedor de Internet. Mismo proveedor que el usuario *verOk*, por lo que es posible, forman parte de una red que mantiene conectividad con el sistema *web-erp* por motivos de negocio. Sin embargo, no se descarta la posibilidad que ante las condiciones de oportunidad encontradas, se trate de la broma de un usuario (LUFERFU).



¿Cómo se realizó el ataque?

Comprometiendo la cuenta de usuario, debido a que un atacante busca el camino más fácil los puntos a atacar no siempre son los sistemas o computadoras, también los usuarios. Hay que mencionar que la autenticación con passwords fijos, como en este caso utilizaron *c0ntr3t0* para la cuenta *acontreras*, no siempre es lo más adecuado.

¿Qué hizo el atacante en el sistema comprometido?

Añadió la cuenta *admin* en el sistema *web-erp* dentro del grupo administradores, para mantener su posterior ingreso de manera sencilla (o solo para demostrar que pudo crearla). No tengo registro de más actividad relacionada con esta dirección de internet.

Recomendaciones Urgentes

La situación de esta red de cómputo es totalmente precaria, se resiente la falta de normatividad sobre los recursos informáticos así como de la falta de conciencia en usuarios y responsables de infraestructura en el tema de seguridad, ya que este servidor se utilizaba no solo para el servicio de *web-erp* sino también como estación de trabajo.

Otro punto urgente a mencionar es que los usuarios dados de alta pertenecían a un grupo con privilegios especiales en el sistema, por lo que se puede percibir que el **administrador** no cumple con el perfil ni la responsabilidad que su puesto de trabajo le exige. Por esta razón no fue capaz de prevenir los riesgos en los que se encontraba el servidor. Considero es el responsable (o al menos corresponsable) de este ataque en grado de su negligencia profesional e incompetencia técnica.

Por último, cabe decir que se encontraron escaneos análisis de vulnerabilidades automatizados desde las siguientes direcciones de la red interna:

192.168.100.144
192.168.5.32

Y desde la dirección de internet:

84.18.17.15

Por lo que es posible que más de un usuario de la red interna, quiera obtener información del sistema *web-erp*. Por esta razón hago las siguientes recomendaciones:

1) Realizar una entrevista dirigida con el administrador de sistemas para determinar:

- Su relación con Luis Fernando Fuentes Serrano.
- Su interacción con la red desde donde se conectó éste último.
- Si existe un precedente de análisis de vulnerabilidades (autorizado) sobre el servidor.

2) Considerar el uso de políticas de seguridad, las cuales deberán estar por escrito y contar con apoyo institucional. Entre otras, considerar:

- *Políticas de Uso*, Consiste en determinar qué se puede hacer con los recursos de cómputo y asignar responsabilidades a los usuarios. Así como también definir la utilización de los recursos en días laborables o no laborables e impedir los hábitos pornográficos.
- *Políticas de Cuentas de Usuario*, Consiste en determinar los privilegios y vigencia de las cuentas de usuarios así como el procedimiento de identificación y autenticación.
- *Políticas de Acceso Remoto*, Consiste en determinar si es permitido acceder a un sistema de manera remota, los métodos a utilizar y el personal que podrá hacerlo.
- *Políticas de Cuentas Administrativas*, Consiste en determinar quienes tendrán cuentas con privilegios para la administración de los diferentes servidores de la organización, por ejemplo, para monitorear la seguridad o la instalación de software.

3) Se tiene en las bitácoras del sistema operativo, una entrada donde se puede visualizar el reinicio del sistema de forma inesperada, por esta razón es urgente también contar con medidas físicas de prevención para el servidor y los equipos de cómputo que posteriormente pueden ser usadas como base para desarrollar más políticas de seguridad.

4 y 5) Crear un procedimiento para la administración de respaldos y tener lineamientos para la actualización de software, ya que en este caso, *Apache* se encontraba en una versión obsoleta y vulnerable.

6 y 7) Crear un procedimiento para la administración de parches y fixes de seguridad en el sistema operativo y aplicaciones, para mantener actualizado el sistema y considerar también mantener actualizado al administrador de sistemas en conocimientos (capacitación).

8) Crear un procedimiento para el manejo de incidentes de seguridad y designar un responsable que coordine a las personas involucradas en un incidente.

9) Verificar la autenticación de usuarios en el sistema *web-erp* así como iniciar una campaña de conciencia para que cada usuario proteja sus passwords.