INFORME DE MATERIA DE GRADUACION
"INTRUSIÓN EN EL BANCO JBR"

Sharon Johanna Baquero Balladares ([1]); Leonardo Andrés Muñoz Pantoja ([2])
Facultad De Ingeniería En Electricidad y Computación
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
lamunoz@espol.edu.ec ([1]); sbaquero@espol.edu.ec ([2])
Febrero 2012 – Febrero 2013
Guayaquil-Ecuador

Resumen

El principal objetivo de este proyecto es implementar las técnicas aprendidas en nuestra vida académica y en el seminario asistido con respecto a las técnicas de computación forense para resolver un cyber crimen corporativo que se suscita en la empresa "JBR BANK" la cual ha solicitado investigar los datos que el equipo de respuestas a incidentes de la misma ha recogido durante un acto sospechoso, en donde se ha encontrado un archivo de nombre Update.exe con una longitud de 0 bytes y que se comenta fue instalado durante horas fuera de horario de trabajo de la empresa.

Se solicita explicar al Banco JBR los métodos utilizados por cualquier intruso, y el alcance de la intrusión, si es que el sistema ha sido comprometido.

Palabras Claves: infiltración, forense, banco, Windows 2000, virus

Abstract

The main objective of this project is to implement the techniques learned in our academic life and during the attended seminar about computer forensics techniques to solve a cyber corporate crime that arises in the company "JBR BANK" which has sought to investigate the data that the incident response team has collected over a suspicious act, where they found a file called Update.exe with a length of 0 bytes that they believed was installed after work hours.

The Bank has requested that we explain the methods used by an intruder, and the scope of the intrusion, if the system has been indeed compromised.

Keywords: infiltration, forensic, bank, Windows 2000, virus

1. Introducción

El objetivo del proyecto es resolver un caso de cyber crimen de manera eficiente aplicando nuestros conocimientos y demás temas aprendidos durante el trascurso de la materia de graduación.

En primera instancia haremos una descripción detallada de conceptos sobre computación forense para de esta manera entender de una mejor manera el caso.

Posteriormente realizaremos una descripción general del caso, el problema en sí y lo que la empresa requiere de nuestros servicios además de la solución del mismo.

A continuación se dará un detalle sobre las herramientas de hardware: como la laptop que hemos usado para la evaluación de este caso. Además de las herramientas de software: fport, pslist, psloggedon, auditpol, psinfo, psfile, psservice, pwdump3, las cuales se han usado durante el proceso.

Luego, trataremos sobre el diseño e implementación de la solución del caso, una breve bitácora, que describirá paso a paso la resolución del caso e incluye una breve descripción de cada punto.

Finalmente se mostrarán las pruebas que hemos considerado pertinente recalcar, ya que

las mismas fueron las únicas responsables de llevarnos hacia la solución del caso.

2. Computación Forense

Al igual que Sherlock Holmes, los investigadores forenses de la informática descubren, analizan y recopilan evidencias digitales que incriminan a los atacantes virtuales, quienes hace más de dos décadas vienen afectando desde el universo computacional al mundo real.

Muchos pensarán que la informática forense tiene que ver con los programas o aplicaciones que se utilizan en la medicina forense, aquella especialidad que se encarga de la investigación penal en sus aspectos médicos con el fin de resolver problemas civiles, penales o administrativos y para cooperar en la formulación de leyes; pero la realidad es que la informática forense realiza las mismas funciones que esta medicina pero en otros "cadáveres" y en otros delitos computacionales.

3. Descripción general del caso

JBR Bank es una muy respetada institución financiera, y muchos de sus colegas usan sus servicios. JBR tiene un sitio Web para que los clientes puedan comprobar la actividad de la cuenta, pagar las facturas por vía electrónica, y ejecutar otras tareas financieras.

El Director de IT de JBR indica que en octubre 1 del 2003, uno de los empleados de help desk encontró un archivo extraño en uno de los sistemas de simulación de los clientes de escritorio. Se accedió a la estación de trabajo Windows 2000 (en la dirección IP 103.98.91.41) y se dio cuenta que el archivo update.exe se encuentra en la unidad C: \ con cero bytes de capacidad. Este archivo no fue colocado en la máquina durante la práctica comercial normal, por lo que el Help Desk llama a la seguridad corporativa. La política de respuesta a incidentes del Banco indica que la máquina debe ser investigada utilizando un proceso de respuesta en vivo, que recoge los datos volátiles que pueden ser perdidos si el ordenador está apagado. La dirección IP del consultor durante la respuesta en vivo fue 103.98.91.200.

Después de que la respuesta en vivo fue completada, el equipo del Banco JBR de respuesta a incidentes realizó una duplicación forense con la utilidad dd. El servicio de ayuda estaba llevando a cabo un monitoreo de red durante el tiempo que se sospecha ocurrió la intrusión y puede haber recogido tráfico de red de interés.

Al Director de IT de JBR le gustaría investigar los datos que su equipo de respuesta a incidentes ha recogido. El Banco JBR quiere saber si violaciones de confidencialidad o integridad pudieron haber ocurrido. El Banco está preocupado por las nuevas directrices de la SEC, que alientan a los bancos a informar de posibles compromisos de la información de los clientes. Nuestro objetivo es ayudar a entender al Banco JBR los métodos utilizados por cualquier intruso, y el alcance de la intrusión, si es que el sistema fue comprometido.

4. Herramientas De Software

- **Virtual Machine:** Con Sistema Operativo Linux
- **Caine:** (Computer Aided INvestigative Environment), es una distribución Live CD para realizar análisis forense informático.
- **Autopsy:** es un aplicativo Web que permite realizar operaciones de análisis forense sirviendo como interfaz gráfica del popular juego de herramientas forenses Sleuth Kit.
- **Fport:** Esta aplicación que se ejecuta a través del símbolo de sistema nos mostrará los puertos abiertos, sean conocidos o no. Y a qué aplicación y puerto están apuntando.
- **Pslist:** permite ver los procesos remotos con gran detalle.
- **Psloggedon:** muestra quién ha iniciado sesión en el sistema. Puede tratarse de inicios de sesión locales (interactivos) o de recursos compartidos de red.
- **Auditpol:** llama directamente a las API de autorización para aplicar los cambios en la directiva de auditoría granular.
- **Psinfo:** es una herramienta de línea de comandos que reúne información clave acerca del sistema Windows NT/2000 local o remoto, por ejemplo, el tipo de instalación, la versión de kernel, el propietario y la organización en registro, el número de procesadores y los tipos, la cantidad de memoria física, la fecha de

instalación del sistema y, si se trata de una versión de prueba, la fecha de caducidad.

- **Psfile:** es una utilidad de línea de comandos que muestra una lista de archivos de un sistema que se abren de forma remota; así mismo, permite cerrar los archivos abiertos tanto por nombre como por un identificador del archivo.
- **Psservice:** es un visor de servicios y un controlador para Windows. Muestra el estado, la configuración y las dependencias de servicios, y permite iniciarlos, detenerlos, pausarlos, reanudarlos y reiniciarlos.
- **pwdump3:** Permite recuperar las hashes de passwords de Windows localmente o a través de la red aunque syskey no esté habilitado.

5. Solución del caso

No debemos llamar la atención del atacante al conectarnos al mismo segmento de red.

Transferir la información mediante el comando NETCAT

Nc –v –l –p 2222 > command.txt command | nc forensic_workstation_ip 2222
Md5sum –b command.txt > command.md5.

El archivo resultante command.txt contendrá todos los datos volátiles de los comandos que se han ejecutado.

- ✓ Datos volátiles:
  - Conexiones de red concurrentes.
  - Puertos TCP/UDP abiertos.
  - Sesiones de usuarios logoneados.
  - Procesos/servicios en ejecución.
  - Proceso de volcado de memoria.
  - Volcado de memoria del sistema completo.

- ✓ Datos no volátiles
  - Versión del sistema y nivel de parche.
  - Registro del evento del sistema.
  - Registro del IIS.
  - Archivos sospechosos.

Conexiones de red concurrentes

Es posible que mientras nosotros estemos ejecutando nuestra respuesta de incidentes en vivo el atacante se encuentre conectado al servidor durante este momento, al mismo tiempo el atacante puede estar corriendo un mecanismo de fuerza bruta hacia las máquinas en el Internet desde el servidor. Esto se logra identificar mediante el comando netstat:

```
TCP    103.98.91.41:445       95.208.123.64:3762     ESTABLISHED
TCP    103.98.91.41:1033      95.208.123.64:21       CLOSE_WAIT
TCP    103.98.91.41:1174      95.145.128.17:6667     ESTABLISHED
TCP    103.98.91.41:1465      95.208.123.64:3753     ESTABLISHED
TCP    103.98.91.41:3992      95.208.123.64:445      TIME_WAIT
TCP    103.98.91.41:60906     95.16.3.23:1048        ESTABLISHED
```

Figura 1. Datos de Netstat -an

Puertos TCP/UDP abiertos.

Si recordamos la lista que descubrimos con el comando netstat recordamos cuales eran las conexiones con puertos abiertos y estamos interesados en estas líneas por una razón: un puerto abierto negado, ejecuta una puerta trasera en la máquina víctima.

Las primeras líneas a través del puerto TCP 515 son normales, por lo general, inician cuando un servicio IIS y TCP / IP son instalados en la máquina. Los siguientes puertos TCP, hasta haber establecido conexión, son los puertos efímeros:

```
Pid   Process        Port   Proto  Path
1224  iroffer   ->   1174   TCP    C:\WINNT\system32\os2\dll\iroffer.exe
1224  iroffer   ->   1465   TCP    C:\WINNT\system32\os2\dll\iroffer.exe
1224  iroffer   ->   4153   TCP    C:\WINNT\system32\os2\dll\iroffer.exe
1224  nc        ->   60906  TCP    C:\WINNT\system32\os2\dll\nc.exe
```

Figura 2. Datos de fport

Sesiones de usuarios logoneados.

Hay que ser cautelosos durante una respuesta en vivo, por lo tanto usaremos una herramienta llamada PsLoggedOn la cual muestra a los usuarios que se encuentran loggoneados en el momento o han accedido a recursos compartidos. Al ejecutar esta herramienta en JBRWWW sin parámetros de línea de comandos, recibimos la siguiente información:

Figura 3. Datos de PsLoggedOn

Dirección IP del Atacante: 95.208.123.64

Procesos/servicios en ejecución.

Nos gustaría saber qué procesos el atacante ejecuta en JBRWWW porque pueden contener puertas traseras. Podemos listar de la tabla de procesos con pslist, lo cual nos da como resultado:

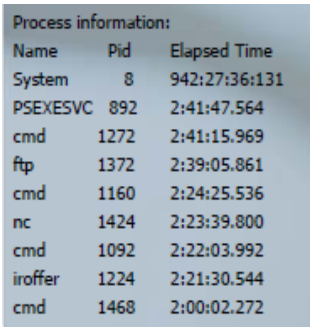

Figura 4. Datos de PsList

A continuación, se muestran los procesos ejecutados por el atacante. Los procesos fueron ejecutados aproximadamente 2 horas y 40 minutos antes de que ejecutemos nuestra respuesta en vivo. Esta información nos da un marco de tiempo sobre cuando el atacante estuvo en JBRWWW. Debido a que la máquina fue arrancada hace mucho tiempo, su ataque inicial puede haber sido casi tres horas antes de nuestra respuesta. Si calculamos 2 horas y 40 minutos antes de nuestra respuesta, recordando la primera información esto nos indica que fue en Octubre 1 del 2003 a las 19:18.

Proceso de volcado de memoria.

Tenga en cuenta que userdump tiene varias opciones útiles, en la captura de múltiples procesos en una sola línea de comandos y ver los procesos que se están ejecutando. Para ejecutar el userdump en un único proceso sospechoso, simplemente ofertamos con un ID de proceso (PID) que hemos obtenido a partir del comando pslist y un destino. Para guardar la sesión netcat del atacante (PID 1424) mapeada a nuestro disco duro en Z se ejecuta el siguiente comando:

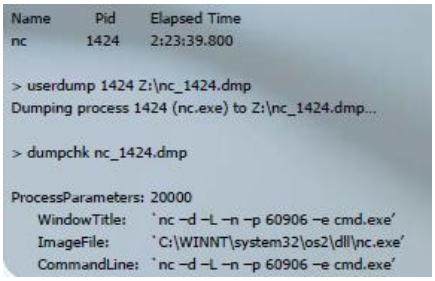

Figura 5. Datos de Userdump

Ahora que tenemos los archivos sospechosos de la aplicación de volcado de memoria, podemos realizar un examen inicial con Dumpchk.exe. Esta utilidad está diseñada para validar un volcado de memoria, sin embargo, proporciona información valiosa.

El resultado confirma el nombre del archivo y la ubicación y proporciona una lista de vínculos dinámicos asociados con los archivos a lo largo de la hora y la línea de comandos utilizados para iniciar el proceso de netcat. Y nos indica que netcat fue configurado para abrirse desde la consola, escuchar desde el puerto 60906, y ejecutar un shell de comandos cuando se produzca cualquier conexión.

Estos datos volátiles se hubieran perdido si el proceso de la memoria no hubiese sido capturado, y simplemente no estaría disponible si examinábamos solo la captura binaria de nc.exe. El examen con Dumpchk reveló que el PID 1224 se inició con una línea de comandos de iroffer myconfig, y el PID 1372 con ftp 95.208.123.64.

Datos no Volátiles

Archivos sospechosos.

- Archivos copiados usando nc
- Archivos creados durante la intrusión.

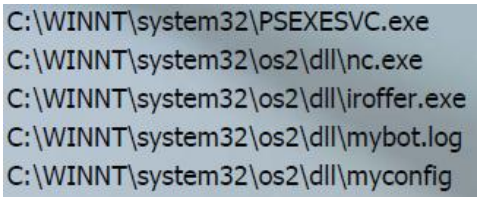

Figura 6. Archivos Sospechosos

6. Conclusiones

El objetivo inicial era determinar si se produjo un incidente. Los datos volátiles y no volátiles recogidos durante la respuesta de incidentes indica que una intrusión no autorizada de hecho ocurrió. La figura 7 muestra el estado en curso de las conexiones de red no autorizadas detectadas durante la respuesta.

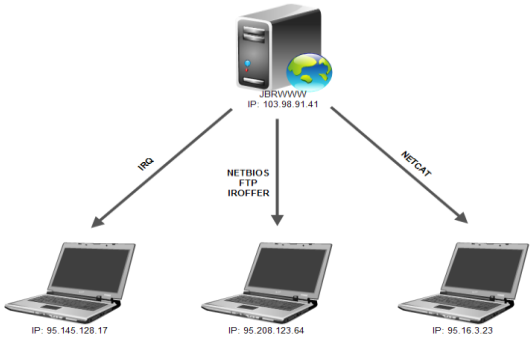

Figura 7. Escenario del Ataque

Aunque no hubo registros de eventos de seguridad de Windows, los registros de IIS indicaron que JBRWWW fue escaneada con una utilidad de escaneo Web conocida como Nikto a las 6:51:17 PM del 23 de septiembre de 2003, de la dirección IP 95.16.3.79. Aproximadamente 18 segundos antes de la exploración, una página web predeterminada de IIS se accede desde la dirección IP 95.16.3.23. Esto es común antes y después de un ataque por un intruso para comprobar el estado de la página web mediante el acceso a una página. Esto puede indicar que el atacante tiene acceso o control del sistema en 95.16.3.73 o tal vez estaba trabajando con alguien que lo hizo.

Luego, el 1 de octubre de 2003, un atacante desde la dirección IP 95.208.123.64, posiblemente trabajando en conjunto con 95.16.3.79, inició un ataque Unicode éxitoso después del fracaso de intentos de desbordamiento de búfer de "Impresora".

Aunque los detalles no se han determinado, parece que los atacantes fueron capaces de ejecutar comandos en JBRWWW a través del ataque Unicode de IIS y establecer una sesión FTP de nuevo a uno de sus sistemas. También fueron capaces de instalar netcat e iroffer en el directorio C: \ WINNT \ system32 \ OS2 \ directorio dll. La Figura 8 muestra una secuencia general de la actividad basada en la información recogida durante la respuesta.

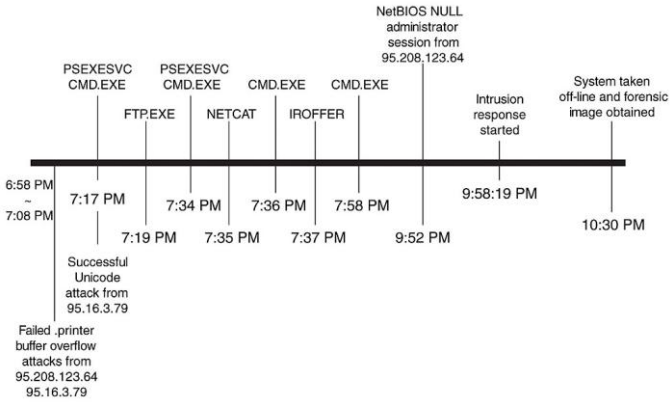

Figura 8. Línea de tiempo para Octubre del 2003

7. Agradecimientos

A Dios, sobre todas las cosas, por permitirnos culminar de manera satisfactoria nuestros estudios, y llevarnos a cumplir una de nuestras metas.

A la familia, por ser nuestra guía de formación humana, por darnos la educación y principios, que nos llevan a ser las personas que somos hoy.

A nuestros profesores y a todas las personas que nos apoyaron en el desarrollo de este trabajo.

Y a todos quienes fomentan el desarrollo tecnológico en Ecuador.

8. Referencias

[1] http://www.portsdb.org
[2] http://www.iroffer.org
[3] http://www.google.com
[4] http://www.sysinternals.com
[5] http://www.secutiryfocus.com
[6] http://www.foundstone.com
[7] http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/ref_we_logging.asp
[8] http://www.cirt.net/code/nikto.shtml.
[9] http://www.qosient.com/argus/gettingstarted.shtm
[10] http://staff.washington.edu/dittrich/talks/core02/tools/tools.html

[11] Fuentes, F., & Dulal, K. (2005). Ethereal vs. Tcpdump: a comparative study on packet sniffing tools for educational purpose. Journal of Computing Sciences in Colleges, 20 (4), 169-175

[12] Laurie, B. (2004). Network Forensics. Queue, 2 (4), 50-56

[13] Ostermann, S. (2003, November 4). tcptrace - Official Homepage. Retrieved August 5, 2010, from tcptrace: http://tcptrace.org/

[14] Roesch, M. (n.d.). About Snort. Retrieved August 5, 2010, from Snort :: About Snort: http://www.snort.org/snort