Máquinas trampa y análisis forense

Honeypots and Forensic Analysis

F. J. Monserrat y J. M. Navarro

Resumen

La seguridad en equipos de redes de ordenadores sigue siendo un tema de gran relevancia en la actualidad; y dentro de los diversos enfoques que se le puede dar, el análisis forense es uno de los campos que más importancia tendrá en el futuro. En este articulo se comenta la creación de un sistema de máquinas trampa y su uso para la experimentación de herramientas de análisis forense y obtención de información sobre los ataques.

Palabras Clave: análisis forense, máquinas trampa, honeypots, ataques, seguridad

Summary

Nowadays security in computer networks equipments still constitutes a very relevant topic, specially the scope concerning forensic analysis which is becoming one of the most interesting fields. In this article is described the creation of a honeypot system and its use for the development of forensic análisis tools in order to obtain information on attacks suffered.

Keywords: forensic analysis, honeypots, attacks, security

1.- Introducción

Los ataques a servidores conectados a Internet siguen aumentando cada año. La complejidad de los métodos empleados por los atacantes ha ido creciendo paralelamente, al igual que las herramientas que emplean para disimular sus acciones en los equipos una vez que han conseguido acceso al sistema.

Hasta hace algún tiempo los sistemas atacados no solían contener información confidencial, por lo que los administradores procedían a la reinstalación y actualización de estos equipos atacados, para así borrar los binarios y puertas traseras instaladas por los atacantes, continuando posteriormente con la actividad normal del sistema.

En la mayoría de las situaciones, las únicas medidas que se solían adoptar con respecto a los atacantes consistían en la notificación del ataque a los administradores de los equipos "origen" del ataque, si se llegaba a averiguar, y el envío de un aviso interno a los usuarios del equipo, para que procedieran a cambiar sus claves de acceso.

Sin embargo, con este incremento del número de equipos atacados, es cada vez más frecuente el tener que analizar las acciones realizadas por los atacantes en los equipos, por un lado para averiguar el alcance del mismo y, llegado el momento, poder tomar las medidas oportunas para denunciar el ataque a las autoridades competentes y por otro, para llevar a cabo la actualización parcial del equipo, ya que muchas veces no es posible dejar sin servicio a los usuarios para proceder a una instalación completa.

El número de incidentes reportados cada año sigue en aumento, como se puede ver en las estadísticas del CERT/CC[Cen02]. Aunque el código de los programas de ataque, o *exploit*, últimamente no suele aparecer de forma directa en listas de correo y servidores www, es evidente que hay muchos foros de discusión y servidores en Internet donde se pueden obtener estas herramientas ya compiladas, lo que hace que el número de ataques siga creciendo.

Con el incremento del número de equipos atacados es cada vez más frecuente el tener que analizar las acciones realizadas por los atacantes en los equipos, por un lado para averiguar el alcance del ataque y por otro para intentar proceder a la restauración parcial del equipo

Los sistemas de detección de intrusos son una de las herramientas que más ha evolucionado en los últimos años

Muchas veces se observa que los atacantes no suelen tener conocimientos extensos sobre el funcionamiento general del sistema al que han conseguido acceder: no saben cómo compilar los programas, ni dónde se encuentra la configuración del sistema de logs del equipo, e intentan ejecutar programas pertenecientes a otros sistemas operativos. La mayoría de ellos se limitan a utilizar una serie de programas "precocinados" para borrar los rastros dejados e instalar una serie de binarios precompilados para atacar después otros servidores.

Las dificultades de acceso a los programas que emplean los atacantes impiden muchas veces que los administradores puedan evaluar si un determinado problema de seguridad afecta directamente a los equipos de la institución, teniendo que esperar bien a que los fabricantes del sistema operativo o aplicación distribuyan la versión actualizada del programa o a filtrar determinados servicios al exterior.

Los sistemas de detección de intrusos son una de las herramientas que más ha evolucionado en los últimos años, habiéndose convertido en uno de los principales mecanismos empleados por los administradores de redes para detectar cuándo se produce un ataque, aunque muchas veces no son suficientes para evitar que estos se produzcan.

La dificultad para analizar los binarios instalados en los equipos por los atacantes complica muchas veces la solución de estos ataques. Los administradores deben intentar eliminar todas las puertas traseras que se hayan podido dejar para entrar con facilidad en el equipo, al igual que los programas de recolección de claves que circulan en claro por la red (sniffer) y las herramientas de ataque a otros equipos.

En los últimos años se ha empezado a utilizar equipos trampa o *honeypots* como un mecanismo de seguridad en la red; estos sistemas suelen ser equipos vulnerables monitorizados en la organización, que sirven para detectar cuándo se ha producido una intrusión y analizar en profundidad las acciones realizadas por los atacantes.

En esta articulo se va a comentar los pasos necesarios a seguir para la puesta en marcha de un sistema de máquinas trampa en una organización. Estos sistemas simulan hacia el exterior equipos vulnerables que al ser atacados permiten a los administradores observar las acciones realizadas por los atacantes, pudiendo de esta forma analizarlas.

Este análisis permitirá, por un lado verificar el uso de los procedimientos de análisis de ataques –o análisis forense–, y por otro, capturar los nuevos patrones de ataque empleados por los atacantes. De este modo se podrán configurar los sistemas de detección de intrusos con estas nuevas reglas para detectar, a su vez, otros nuevos ataques.

Estas máquinas trampa proporcionan muchas veces a los administradores los programas de ataque empleados por los atacantes, que pueden servir para evaluar la seguridad interna de la organización, siempre y cuando se tomen las medidas oportunas.

2.- Máquinas trampa y análisis forense

Antes de pasar a la puesta en marcha del sistema de máquinas trampa se realizará una breve introducción de los distintos conceptos y herramientas que se van a emplear.

2.1.- Detectores de intrusos

Tradicionalmente la detección de intrusos se solía realizar en los servidores conectados a Internet, empleando sistemas como cops[FS90] o tripwire[KS93], que comprobaban cada cierto tiempo que determinados ficheros de los sistemas no hubieran sido modificados.

Estos sistemas de detección requieren una gestión centralizada de los equipos (instalación y configuración de los programas en cada uno de los sistemas administrados), lo que dificulta su puesta en marcha en redes descentralizadas donde la administración de los equipos la realizan, de forma independiente, diversos grupos de usuarios; además en la última década el aumento de capacidad en los equipos de sobremesa y la aparición de diversos sistemas operativos gratuitos para estos equipos ha hecho que aumente el número de sistemas conectados permanentemente a Internet, convirtiéndose en víctimas potenciales de ataques.

El aumento de capacidad en los equipos ha permitido, por otro lado, que puedan procesar mayor cantidad de información, siendo en muchos casos capaces de capturar y procesar todo el tráfico destinado a la red de la organización, y así han ido surgiendo los modernos Sistemas de Detección de Intrusos en Red (NIDS) que permiten la monitorización del tráfico que tiene como origen o destino la red de la institución, detectando patrones de tráfico que pueden indicar que se está produciendo un ataque[Abe01][Alm01].

Estos NIDS se basan principalmente en las cadenas de caracteres que constituyen los ataques, comprobando que no aparecen estos mismos caracteres en el tráfico que circula por la red, de forma similar al funcionamiento de los programas antivirus en los equipos personales. Al igual que estos, los NIDS solamente detectan los ataques que tiene registrados en su base de datos de conocimiento, por lo que se debe actualizar periódicamente esta base de datos para incorporar los nuevos ataques que van apareciendo.

Los modernos Sistemas de Detección de Intrusos en Red (NIDS) permiten la monitorización del tráfico que tiene como origen o destino la red de la institución, detectando patrones de tráfico que pueden indicar que se está produciendo un ataque

2.2.- Análisis forense

Una vez que se ha detectado el acceso no autorizado al equipo se suele proceder a un proceso de solución o "recuperación" ante el incidente hasta que el problema ha sido solventado.

En la mayoría de los casos la solución consiste en la reinstalación del Sistema Operativo del equipo atacado y la modificación de las claves de accesos de los usuarios, sin embargo cada vez es más costoso el parar un servicio para efectuar estas operaciones y por otro lado, muchas veces es conveniente evaluar en profundidad las implicaciones que ha tenido este problema de seguridad mediante las herramientas de análisis forense.

Estas técnicas de análisis forense se aplicaban en principio a análisis judiciales y de ahí proviene gran parte de los términos y metodología, ya que fue en ese entorno donde empezó a surgir la necesidad de realizar estas actuaciones.

Las actuaciones que se solían realizar consistían en un análisis a nivel de aplicación –para determinar cuándo se empleó determinado programa, en base a los registros y datos (mensajes de correo,...)– y en búsquedas de cadenas de texto en los ficheros y dispositivos de almacenamiento. Estas técnicas estaban indicadas sobre todo para el análisis "in situ" de los equipos –principalmente en equipos personales– para determinar si desde ese equipo se habían realizado determinadas acciones ilegales.

The Coroner Toolkit (TCT) es un conjunto de herramientas para equipos Unix que permite automatizar la extracción de información en los equipos atacados

En los últimos años ha empezado a surgir la necesidad de analizar servidores atacados, donde el principal problema es el desconocimiento del origen del ataque o la forma en la que se ha producido. En este sentido, dos iniciativas han destacado fundamentalmente en el análisis de equipos atacados: el conjunto de herramientas "The Coroner Toolkit"[aDF99] y los análisis forenses realizados dentro del Proyecto HoneyNet[pro00].

The Coroner Toolkit (TCT) es un conjunto de herramientas para equipos Unix que permite automatizar la extracción de información en los equipos atacados, de forma que se puede analizar con mayor facilidad las modificaciones realizadas sobre estos. No se trata pues, de un programa que realice el análisis del equipo atacado, sino de un conjunto de herramientas que permiten automatizarlo.

Entre las diversas herramientas que lleva este programa se encuentra una utilidad para la recuperación de ficheros borrados y otro programa que permite extraer los distintos tiempos de Modificación, Acceso y Creación (tiempos MAC) de cada uno los ficheros que hay en el equipo. Esta información sirve para, en concordancia con los datos que se puedan obtener de los logs del sistema, indagar en las acciones que realizó el atacante una vez que se conectó al equipo.

Por otro lado, dentro del proyecto HoneyNet, que se comentará más adelante se ha procedido a documentar las diversas actuaciones a seguir a la hora de analizar un incidente, poniendo a disposición de los usuarios interesados imágenes sobre incidentes de seguridad y ejemplos de estos análisis.

2.3.- Máquinas trampa

Los sistemas trampa, generalmente llamados "honeypots" (tarros de miel en inglés), son equipos conectados a Internet que ofrecen desde el exterior una configuración que los hace "apetecibles" a los atacantes, ya sea porque parece que disponen de servicios vulnerables a determinados ataques por estar situados en determinadas redes o por tener un nombre que pueda sugerir que tienen información útil para los atacantes.

Aunque exteriormente parezca que estos equipos disponen de las mismas medidas de seguridad que en el resto, en realidad se encuentran monitorizados continuamente, de forma que se puede detectar cuándo se produce el ataque y así obtener información sobre el atacante.

Existen diversas maneras de construir este tipo de sistemas. En su forma más básica, un sistema trampa puede ser un proceso que esté escuchando en un puerto y capture la información que se le envía; este sistema se empleó, por ejemplo, para obtener copias del gusano "CodeRed" en equipos de usuarios, teniendo un programa escuchando en el puerto de servidores HTTP y capturando la información enviada.

Otros sistemas más complicados, como Mantrap[Tec02], consisten en la alteración del sistema operativo de un equipo para que simule el comportamiento de varios equipos simultáneamente y así poder detectar los ataques.

Sin embargo, los sistemas de máquinas trampa más famosos en la actualidad se basan en la propuesta del Proyecto HoneyNet surgido en el año 2000 y que pretendía servir de plataforma para el estudio de las acciones realizadas por los atacantes en los equipos vulnerados.

En este artículo se va a presentar la configuración de un sistema de máquinas trampa empleando equipos de bajas prestaciones previamente retirados, aunque gran parte de la configuración puede ser empleada en otras configuraciones de equipos virtuales simulados, utilizando emulación completa de hardware con productos como VMWARE[Inc01] o Bochs[Var00].

3.- Diseño del sistema trampa

El sistema de máquinas trampa está formado por un conjunto de equipos vulnerables –las máquinas trampa propiamente dichas– y un equipo de control que monitoriza al resto de los equipos. Este sistema permitirá el tráfico entre la red de equipos trampa y el exterior, bloqueando los equipos cuando se detecta un ataque, de forma que no se puedan emplear estos, a su vez, para realizar nuevos ataques.

El sistema de máquinas trampa está formado por un conjunto de equipos vulnerables –las máquinas trampa propiamente dichas– y un equipo de control que monitoriza al resto de los equipos

En los equipos trampa se pueden instalar los diversos sistemas operativos usados en la institución con la configuración de servicios que se deseé monitorizar (servidor WWW, FTP, etc.). Dado que estos equipos trampa no necesitan tener un rendimiento alto, se pueden emplear sistemas antiguos que hayan sido retirados del servicio, aunque es conveniente que pueden ejecutar versiones actuales de los sistemas operativos.

Además, y para proceder más adelante al análisis de los datos dejados por el atacante en el equipo, no conviene que los sistemas tengan una capacidad de almacenamiento muy elevada. Así un equipo "Pentium 133 con un disco duro de 1,6 ó 2Gb y 32 Megas de memoria RAM se puede emplear para la instalación de diversos sistemas operativos Unix/Linux sobre plataforma Intel; mientras que un antiguo Sparc puede servir para la instalación de un Solaris 2.7, por ejemplo.

Estos equipos trampa tendrán direccionamiento propio de la red de la organización y estarán conectados entre sí a un hub que permita al atacante, en un momento dado, capturar el tráfico "falso" entre equipos externos y las máquinas trampa de manera que el atacante pueda ser dirigido a otros equipos trampa.

El equipo de control funciona en modo puente Ethernet, actuando de forma transparente a nivel IP, pudiendo, de esta manera, conectar las máquinas trampa a la red, manteniéndolas aisladas del resto de los equipos de la organización y sin tener que implementar una subred donde incluirlas. Este equipo de control deberá tener, a su vez, una dirección IP para poder gestionarlo.

Para poder monitorizar los ataques, el equipo de control capturará todo el tráfico con origen y/o destino a la red de máquinas trampa, de forma que se pueda tener un registro de las conexiones que realiza el atacante a ellas.

Este registro de tráfico sirve, entre otras cosas, para poder detectar nuevos ataques y vulnerabilidades ya que se puede comparar el tráfico generado por el uso del ataque o *exploit* con los realizados por otros ataques similares; y detectar así cuando aparecen nuevos ataques o variaciones de otros ya existentes.

En la figura se observa la configuración del sistema trampa propuesto. Como se puede observar, el equipo trampa divide en dos la red de la institución, separando los equipos trampa del resto

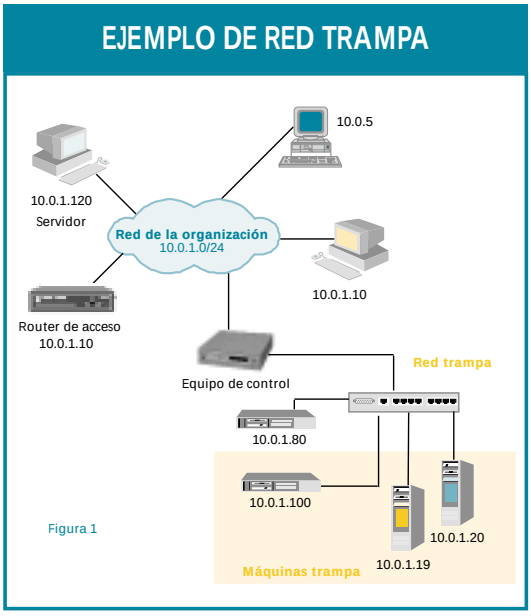

Figura 1

La captura del tráfico generado con origen/destino en/a los equipos trampa se puede realizar directamente con el programa tcpdump

de equipos de la organización. Esta separación a nivel físico impide que los equipos trampa puedan capturar el tráfico a nivel IP que circule por el resto de la red, con independencia del tipo de entorno (conmutado o compartido) en el que se encuentre la red de máquinas trampa.

El tráfico entre los equipos de usuarios del servidor no se detectaría en ninguna de las máquinas trampa, solamente aquél destinado a toda la red de broadcast Ethernet llegaría a estos equipos.

Así pues, cuando desde el exterior se realizase un escaneo contra la red 10.0.1.0/24 todos los equipos, normales y trampa, responderían a las conexiones y, llegado el momento, el atacante podría entrar en una de las máquinas trampa, por ejemplo la 10.0.1.80, e instalar un sniffer en ella para intentar capturar las claves de acceso; sin embargo, solamente obtendría la información generada por las máquinas trampa –proporcionada mediante scripts para simular tráfico– y no la generada por los equipos de usuario (10.0.1.5 y 10.0.1.10).

Para evitar que una vez que el atacante haya accedido a los equipos pueda atacar a otros sistemas, es conveniente limitar en el router de acceso la cantidad de conexiones salientes que se pueden realizar desde estos equipos. No se debe filtrar completamente ya que, de lo contrario, es muy posible que algunos programas, como los clientes y servidores de FTP, no funcionen correctamente.

Para el equipo de control se puede emplear un sistema Linux con la característica de puente Ethernet activada. Esta característica está presente en las últimas versiones de los núcleos 2.4.x, donde también hay una opción que permite el filtrado a nivel de dirección Ethernet de los equipos del tiempo, que se puede emplear para bloquear el tráfico de los equipos atacados sin tener que aplicar filtros en los router de acceso de la organización.

CONFIG_BRIDGE=m	Activa el empleo de las funciones de puente Ethernet en el núcleo del equipo
CONFIG_BRIDGE_NF	Indica que se van a poder emplear las facilidades de filtro de paquetes (netfilter) para las tramas Ethernet que circulen por el puente
CONFIG_NETFILTER	Activa las funcionalidades de filtro de paquetes IP y tramas en el núcleo del equipo
CONFIG_IP_NF_IPTABLES	Activa el sistema de IPtables para el filtrado de las tramas
CONFIG_IP_NF_MATCH_MAC	Permite filtrar en función de la dirección Ethernet (MAC) de las tramas, para impedir por ejemplo que desde los equipos trampa se pueda acceder a determinados equipos de la red
CONFIG_IP_NF_FILTER	Activación de los filtros

Tabla 1: Opciones de configuración del núcleo de Linux

En la tabla 1 se muestran las opciones más importantes que hay que activar para que el equipo pueda funcionar como puente Ethernet y filtrar las conexiones. En general se pueden activar todas las funcionalidades que aparecen dentro del menú de configuración de los filtros (IP Netfilter configuration) de los núcleos 2.4.

Además de la compilación del núcleo, hay que instalar en el equipo la utilidades de gestión de puentes (bridge-utils) que permiten la configuración y gestión de los puentes Ethernet.

La captura del tráfico generado con origen/destino en/a los equipos trampa se puede realizar directamente con el programa tcpdump, separando el tráfico en ficheros distintos y clasificándolo según la dirección IP del equipo origen/destino. Periódicamente se deben realizar rotaciones de estos logs, para evitar tener ficheros de captura demasiado grandes.

Las opciones que se han empleado con el programa tcpdump para capturar el tráfico aparecen comentadas en la tabla número 2.

tcpdump -n -nn -s 1500 -w trampa-10.0.1.80 -i br0 host 10.0.1.80

-n	No consultar en el servidor de DNS el nombre asociado a las direcciones IP
-nn	No consultar en el fichero /etc/services el nombre de los puertos involucrados en cada conexión
-s 1500	Número máximo de bytes a almacenar de cada paquete, este valor debe ser igual o mayor que la MTU de los interfaces Ethernet (1.500 normalmente)
-w fichero	Almacenar la información directamente en un fichero
-i br0	Emplear el interface del puente, en este el br0.
host equipo	Capturar sólo el tráfico con destino a este equipo a nivel IP

Tabla 2: Opciones de captura para TCPDUMP

Además, en el equipo de control se lanzará el software de detección de intrusiones snort, que avisará cuando se haya producido un ataque contra las máquinas trampa.

Estos programas de detección de intrusos funcionan leyendo todo el tráfico que llega al equipo y comparando cada paquete IP con una base de datos de reglas que especifican un determinado ataque.

Estas reglas detectan patrones de ataques conocidos, por lo que deben actualizarse periódicamente con los patrones de nuevos ataques que van surgiendo.

Una vez que se ha detectado que la integridad del sistema ha podido ser vulnerada por algún tipo de intrusión, es conveniente hacer una copia de la información que hay en el sistema y, dependiendo de la situación, puede ser conveniente incluso hacer una "copia" de los procesos que se están ejecutando en ese momento

4.- Análisis de un caso real

Desde un punto de vista práctico, una vez que se ha detectado (o se sospecha) que la integridad del sistema ha podido ser vulnerada por algún tipo de intrusión, es conveniente hacer una copia de la información que hay en el sistema. Dependiendo de la situación, puede ser conveniente incluso hacer una "copia" de los procesos que se están ejecutando en ese momento en el equipo, del espacio de intercambio (swap), de las conexiones activas, etc.

Para realizar una copia de las particiones del sistema de ficheros, en los equipos Unix, se puede usar el comando dd. Las copias obtenidas pueden volcarse en una partición libre del propio equipo o a un fichero (cosa poco recomendable, ya que el contenido del sistema atacado debería modificarse lo menos posible), sin embargo es preferible enviar los contenidos a otro equipo empleando, por ejemplo, el programa Netcat (nc).

El siguiente ejemplo muestra cómo se podría realizar esta copia, transfiriendo el contenido de la partición sda4 del equipo víctima al equipo de control.

En el equipo víctima se ejecutaría:

```
dd if=/dev/hda2 - | nc equipo_remoto -p 100
```

y en el equipo remoto se recibiría el fichero:

```
nc -l -p 100 > disco-hda2
```

Una vez que se ha realizado la copia y la migración de los datos al equipo remoto donde se va a efectuar al análisis, se debe proceder a la recopilación de datos relacionados con el tipo de sistema y su entorno

También se pueden enganchar los discos a un equipo y realizar la copia a bajo nivel, empleando discos duros de iguales características (mismo modelo) y haciendo la copia mediante dd.

```
dd if=/dev/sda of=/dev/sdv
```

En sistemas operativos como Windows NT, que no disponen de un procedimiento de backup a bajo nivel, se puede utilizar el procedimiento empleado para sistemas Unix: arrancar el equipo desde un disco de rescate o instalación de Linux/Unix (menos recomendable por aquello de modificar datos del sistema) y proceder a realizar la copia de los dispositivos a bajo nivel.

En cualquier caso, es conveniente realizar estas copias a bajo nivel para poder restaurar los datos en caso de que ocurra algún problema al analizar los ficheros, además esto permitirá el análisis de los archivos buscando las fechas de modificación de los mismos.

Todo este proceso (es decir, los pasos dados para la copia de los datos del sistema) debería quedar registrado y documentado en algún sitio de forma automática. En estos casos, comandos como script pueden resultar muy útiles.

Una vez que se ha realizado la copia y la migración de los datos al equipo remoto donde se va a efectuar al análisis, se debe proceder a la recopilación de datos relacionados con el tipo de sistema y su entorno: versión del sistema operativo, particiones utilizadas, fecha en la que se detectó el ataque, fecha en la que se desconectó de la red el equipo y cualquier otra modificación que pudiese tener relevancia para el análisis.

Posteriormente, se procederá a montar las imágenes de las particiones para comenzar el análisis de las mismas en el equipo remoto. Para esto se puede usar el mecanismo de loop-back disponile en Linux, que permite el montaje de los ficheros imagen de la partición en el equipo Unix, pudiendo así acceder a archivos de estos sistemas de ficheros.

```
mount -o loop, ro, noexec /home/forensic/disco-hda2 /analisis
mount -o loop, ro, noexec /home/forensic/disco-hda3 /analisis/var
```

Una vez montadas las particiones, se utilizará fundamentalmente el paquete TCT para realizar el análisis. El primer paso será la obtención de los tiempos de Modificación/Acceso/Cambio (tiempos MAC) de todos los ficheros del sistema. Es fundamental capturar estos tiempos antes de emprender cualquier acción sobre los ficheros del equipo atacado que pueda modificar su valor. La secuencia de accesos a los ficheros permitirá crear una línea temporal que muestre los acontecimientos ocurridos en el sistema.

Mediante las herramientas ils e ils2mac[1] se podrán obtener los tiempos MAC de los nodos-i borrados de las particiones. El fichero resultante será combinado, a su vez, con el fichero obtenido tras la ejecución de grave- robber[2] sobre el sistema de ficheros anterior, para, de esta forma, tener los tiempos MAC tanto de los nodos-i borrados como de los nodos-i activos. La secuencia de comandos usada para hacer esto podría ser la que se detalla a continuación:

1 Herramientas incluidas en el paquete "The Coroner Toolkit", que permiten acceder directamente a la información almacenada en los nodos-i de las particiones (ils) y convertir esta información al formato manejado por el TCT (ils2mac)

2 Script de obtención automática de información, disponible en TCT

```
# /root/tct-1.07/bin/grave-robber -o LINUX2 \
-c home/analisis/disco -m -d ./resultados
# /root/tct-1.07/bin/ils /home/analisis/raiz-hda4 \
|/root/tct-1.07/extras/ils2mac > raiz-hda4.ilsbody
# /root/tct-1.07/bin/ils /home/analisis/var-hda3 \
|/root/tct-1.07/extras/ils2mac > var-hda3.ilsbody
# cat raiz-hda4.ilsbody var-hda3.ilsbody > body-deleted
# cat body body-deleted > body-full
# /root/tct-1.07/bin/mactime -p home/analisis/disco/etc/passwd \
-g home/analisis/disco /etc/group -b body-full 08/04/2001 \
 mactime.txt
```

En muchas intrusiones, lo primero que hace el atacante es modificar los programas y herramientas del sistema para ocultar su acceso

Al final de este proceso se obtiene un listado completo (contenido en el fichero 'fichero.txt') de los tiempos MAC de todos los ficheros del sistema (incluidos los borrados) que hayan modificado alguno de sus tiempos MAC desde 'fecha'.

La siguiente acción a realizar, una vez obtenidos los tiempos MAC, es comprobar todos los programas y ficheros de configuración instalados en el equipo.

En muchas intrusiones, lo primero que hace el atacante es modificar los programas y herramientas del sistema para ocultar su acceso; además, suelen modificar los ficheros de configuración para crear nuevos usuarios, permitir accesos desde determinadas máquinas, etc., de forma que puedan acceder al equipo más cómodamente con posterioridad.

Por todo lo comentado anteriormente, es conveniente que no se empleen los programas instalados en el propio equipo, sino versiones que se tengan compiladas estáticamente –siempre que se tenga que realizar el análisis sobre el mismo equipo atacado y no se pueda usar otro sistema para realizarlo–. El motivo de utilizar ficheros compilados estáticamente se debe a que no emplean llamadas a librerías del sistema susceptibles de ser modificadas por los atacantes. Por esa misma razón no es conveniente que se emplee el sistema operativo de la máquina atacada, ya que puede ser modificado mediante módulos para ocultar los procesos y ficheros del atacante. Sin embargo, aunque se usen programas compilados estáticamente, esto no evita que la información mostrada pueda ser errónea, ya que existen rootkits que pueden modificar, mediante módulos, el propio núcleo del sistema operativo. Un ejemplo sería Adore.

Si no se dispone de una base de datos de integridad en un dispositivo externo para poder comprobar la integridad de los ficheros (ayudándose de herramientas como, por ejemplo, *Tripwire*), se pueden usar técnicas como comparar los ficheros binarios existentes en el sistema con los de la instalación original (cuando no estén empaquetados) o con los que hay en otro equipo con la misma versión y parches del sistema operativo, empleando comandos como cmp.

La mayoría de los sistemas operativos disponen de un sistema de verificación de paquetes instalados. La base de datos se mantiene en el propio equipo (por lo que el atacante puede modificarla) pero de todas maneras puede emplearse muchas veces para comprobar qué ficheros se han modificado.

Aunque es habitual que algunos ficheros cambien de permisos o de contenido, por ejemplo al añadir usuarios al fichero de password, después de realizar algunas instalaciones que producen cambios en los formatos, etc.; no suele ser habitual que comandos como /bin/ls sean modificados, lo que puede indicar que se trata de una versión troyanizada.

En los ataques más recientes se están empezando a utilizar ficheros que se ejecutan comprimidos

Para comprobar la consistencia de los paquetes instalados en el sistema atacado, buscando especialmente errores de chequeo de md5, se puede usar la utilidad rpm (o su equivalente –si existe– en el sistema operativo atacado) con las opciones adecuadas, como por ejemplo:

```
rpm -V -a –root=home/analisis/disco/ > consistencia_rpm
cat consistencia_rpm | grep ^..5
S.5....T c /etc/services
S.5....T c /etc/localtime
S.5....T c /etc/info-dir
..5....T c /etc/mime.types
S.5....T c /etc/httpd/conf/httpd.conf
S.5....T /usr/lib/umb-scheme/slibcat
S.5....T c /etc/inetd.conf
S.5....T c /etc/rc.d/rc.sysinit
S.5....T c /etc/sysconfig/pcmcia
S.5....T /bin/netstat
S.5....T /sbin/ifconfig
SM5....T /bin/ps
SM5....T /usr/bin/top
S.5....T c /etc/pam.d/rlogin
S.5....T /var/log/sendmail.st
S.5....T c /etc/syslog.conf
S.5....T /usr/sbin/tcpd
S.5....T c /etc/pam.d/login
SM5....T c /etc/ftpaccess
S.5....T c /etc/ftpusers
```

La aparición de modificaciones en ficheros como: netstat, ifconfig, ps, top, ls, top, tcpd..., sugeriría la posibilidad de que se haya instalado un rootkit en el sistema.

Un método para saber si los ficheros modificados son versiones troyanizadas de los originales es examinar los ficheros sospechosos buscando cadenas que delaten esta posibilidad. Normalmente, la información que se obtiene de este estudio suelen ser rutas de directorios y ficheros que no deberían aparecer en el sistema, por ejemplo:

```
# strings -a home/analisis/disco/bin/ps > strings_ps
# cat strings_ps
...
/dev/xdta
NR   PID   STACK   ESP   EIP TMOUT ALARM STAT TTY   TIME COMMAND
PID TTY MAJFLT MINFLT   TRS   DRS   SIZE  SWAP  RSS  SHRD   LIB   DT  COMMAND
PID TTY STAT   TIME   PAGEIN TSIZ DSIZ   RSS   LIM  %MEM COMMAND
...
```

El fichero ‘‘‘/dev/xdta” resulta ser un fichero de configuración que contiene un listado con todos los procesos que no mostraría el comando ps (aunque se estuvieran ejecutando), para no delatar la presencia de intrusos en el equipo.

Sin embargo, este sistema no siempre da buenos resultados ya que en los ataques más recientes se están empezando a utilizar ficheros que se ejecutan comprimidos –por lo que no es posible visualizar las cadenas de texto que contienen– y otras técnicas de ofuscación que impiden obtener información útil empleando el método anterior.

Una vez analizadas las cadenas de los programas supuestamente modificados, se debe intentar recuperar el contenido de los ficheros borrados (el número de nodo-i que tenía asociado cada archivo antes de ser borrado se puede obtener del fichero de tiempos MAC generado anteriormente).

Para recuperar el contenido de estos ficheros se puede usar el comando icat, incluido en el TCT. Este programa devuelve toda la información que encuentra sobre el nodo-i que se le pasa como parámetro realizando la búsqueda en la imagen de la partición indicada.

Anteriormente se han obtenido, mediante el comando ils, los nodos-i actualmente vacíos que hubiesen contenido información en el periodo en el que se produjo el incidente. Para obtener una copia de estos ficheros se puede emplear el comando icat, en lugar de realizar una búsqueda mediante un editor.

Una vez analizadas las cadenas de los programas supuestamente modificados, se debe intentar recuperar el contenido de los ficheros borrados

```
/root/tct-1.07/bin/icat var-hda3 12216 > fich-12216
/root/tct-1.07/bin/icat raiz-hda4 92962 > fich-92962
/root/tct-1.07/bin/icat raiz-hda4 92961 > fich-92961
/root/tct-1.07/bin/icat var-hda3 26422 > fich-26422
/root/tct-1.07/bin/icat var-hda3 40645 > fich-40645
/root/tct-1.07/bin/icat raiz-hda4 2404 > fich-2404
/root/tct-1.07/bin/icat raiz-hda4 90629 > fich-90626
/root/tct-1.07/bin/icat raiz-hda4 92570 > fich-92570
/root/tct-1.07/bin/icat raiz-hda4 92571 > fich-92571
/root/tct-1.07/bin/icat var-hda3 26421 > fich-26421
/root/tct-1.07/bin/icat raiz-hda4 166537 > fich-166537
/root/tct-1.07/bin/icat var-hda3 38613 > fich-38613
/root/tct-1.07/bin/icat var-hda3 38614 > fich-38614
/root/tct-1.07/bin/icat var-hda3 38615 > fich-38615
/root/tct-1.07/bin/icat var-hda3 38617 > fich-38617
```

Realizado este proceso, la siguiente tarea será averiguar el tipo de cada fichero para abrirlo con el programa adecuado (el comando file, o sus análogos en cada sistema operativo, pueden facilitar esta tarea).

Posteriormente, se deberá analizar el contenido de cada uno de estos ficheros. Así, por ejemplo, los ficheros de texto pueden contener trozos de logs borrados deliberadamente por el intruso, los ficheros ejecutables pueden corresponder a programas utilizados por el atacante, los ficheros comprimidos pueden ser paquetes instalados...

```
file fich*> tipos
$cat tipos
fich-12216: International language text
fich-92962: ASCII text
fich-92961: ASCII text
fich-26422: empty
fich-40645: data
fich-2404: gzip compressed data, deflated, last modified:
Wed Jul 11 19:25:03 2001, os: Unix
fich-90626: English text
fich-92570: ASCII text
fich-92571: ASCII text
fich-26421: empty
fich-166537: English text
fich-38613: ASCII text
fich-38614: empty
fich-38615: ASCII text
fich-38617: ASCII text
```

Por último se puede observar la creación y modificación de diversos ficheros en los directorios del sistema, que reemplazan a los binarios originales del equipo

En este punto, si fuese necesario, se procedería al desensamblado de los ficheros ejecutables para determinar como mayor exactitud su funcionalidad.

Recogida y analizada esta información básica (que puede dar una idea muy aproximada de lo que ha pasado en el sistema), se procederá al estudio del fichero de tiempos MAC que se generó anteriormente. Este análisis tratará de establecer una línea temporal que muestre la secuencia de acontecimientos ocurrida en el sistema.

A continuación se muestra un extracto de los datos que genera el programa mactime, y una pequeña reseña de la información que se puede obtener de estos (la salida ha sido ligeramente modificada para ajustarla a la página).

Como ejemplo se muestra la información que aparece cuando se modifica el fichero ps. Obsérvese la creación del fichero de configuración (dev/xmx) que se había detectado anteriormente.

```
Aug 06 01 09:57:55  \
    627271 ..c -rw-r--r-- root root <raiz-hda4-dead-2404>
Aug 06 01 09:58:00    \
      4096 m.c drwxr-xr-x root root home/analisis/disco/bin
      1195 .a. -rwxr-xr-x root root home/analisis/disco/bin/chown
     35300 ..c -rwxr-xr-x root root home/analisis/disco/bin/netstat
     33280 ..c -rwxr-xr-x root root home/analisis/disco/bin/ps
     36864 m.c drwxr-xr-x root root home/analisis/disco/dev
       241 m.c -rw-r--r-- root root home/analisis/disco/dev/xdta
       145 m.c -rw-r--r-- root root home/analisis/disco/dev/xmx
     19840 ..c -rwxr-xr-x root root home/analisis/disco/sbin/ifconfig
     21816 .ac -rwxr-xr-x root root home/analisis/disco/usr/bin/crontab
     21816 mac -rwsr-xr-x root root home/analisis/disco/usr/bin/ct
     53588 ..c -rwxr-xr-x root root home/analisis/disco/usr/bin/top
      4096 m.c drwxr-xr-x root root home/analisis/disco/usr/sbin
     27055 .ac -rwxr-xr-x root root home/analisis/disco/usr/sbin/in.rexedcs
    267360 ..c -rwxr-xr-x root root home/analisis/disco/usr/sbin/syslogd
     14224 ..c -rwxr-xr-x root root home/analisis/disco/usr/sbin/tcpd
```

En primer lugar, se puede observar que por la proximidad de las fechas en las que se modifican los ficheros es muy posible que se trate sde la ejecución de un script, ya que se crean varios ficheros en el mismo instante de tiempo –en el análisis completo de este ataque se pudo verificar esta hipótesis, recuperando el script empleado entre los ficheros borrados por el atacante–.

En la primera entrada de tiempos se accede a varios ficheros del sistema para obtener información del equipo. El fichero “raiz-hda4-dead-2404” es el fichero comprimido de la instalación que es borrado posteriormente por el atacante.

Por último se puede observar la creación y modificación de diversos ficheros en los directorios del sistema,que reemplazan a los binarios originales del equipo. Mediante la recuperación del script lanzado por el atacante, se pudo comprobar que algunos de estos ficheros eran las versiones reales de los demonios del sistema, como “/usr/bin/ct”, versión original del programa crontab.

Los ficheros instalados por el atacante en el directorio “/dev” contenían la configuración de los binarios del rootkit, indicando qué procesos y conexiones se debían ocultar a los administradores.

En la última fase del análisis –en realidad, no tiene por qué ser la última, puede ser incluso la primera o ir intercalándose– se procederá a examinar el flujo de tráfico capturado por un IDS. El objetivo es establecer y corroborar todos los datos hallados en el sistema.

En general, los pasos a seguir suelen dividirse en:

1.- Análisis de los flujos de datos para agruparlos según las distintas conexiones capturadas. En estos casos conviene la utilización de algún tipo de script que facilite y automatice esta labor, puesto que la cantidad de información con la que se puede llegar a trabajar (del orden de varios gigabytes) hace inviable un tratamiento manual.

2.- Almacenamiento de la información de cada conexión en un fichero donde sea fácilmente identificable: origen y destino de la conexión, fecha y hora de comienzo y finalización, puerto utilizado y tamaño de la misma.

3.- Establecer, en su caso, si existe algún tipo de desfase horario entre el sistema de control (IDS, Firewall, ...) y el equipo analizado. Esto es fundamental para poder comparar los datos de las conexiones almacenadas con la información que ha quedado registrada en el equipo atacado.

4.- Estudio de las conexiones y búsqueda de datos que faciliten la identificación del atacante. El orden seguido al examinar las conexiones puede disminuir el tiempo que es necesario emplear, por eso conviene empezar por las que parezcan más prometedoras.

Una vez analizada y clasificada toda la información almacenada en el IDS se pudo determinar que el ataque se produjo aprovechando una vulnerabilidad del proceso rpc.statd. Posteriormente, el atacante realizó una conexión ftp desde el propio equipo para bajarse los programas necesarios para completar la intrusión.

Un análisis más en profundidad de las conexiones permitió obtener un listado de las actividades desarrolladas por el atacante: desde la conexión a un servidor para descargarse el archivo con los ficheros troyanizados, hasta la instalación de los mismos.

La instalación de “sensores” en forma de equipos vulnerables, pero aislados de la red en producción permite analizar los métodos empleados por los atacantes para acceder a los equipos sin comprometer la seguridad de la organización

5.- Conclusiones y vías futuras

La instalación de “sensores” en forma de equipos vulnerables, pero aislados de la red en producción permite analizar los métodos empleados por los atacantes para acceder a los equipos sin comprometer la seguridad de la organización.

Este sistema permite recuperar y analizar diversos programas instalados y empleados por los atacantes, pudiendo así determinar los fines que llevaron a la intrusión, detectando además los equipos desde donde se llevaban a cabo los ataques preliminares, así como obtener, para su posterior análisis, otros programas utilizados por el atacante.

El análisis del tráfico de red complementa perfectamente la información obtenida directamente de las máquinas, pudiéndose relacionar de forma inmediata la actividad en la red, como por ejemplo los escaneos desde determinados equipos, con los ataques realizados con éxito contra los equipos trampa.

La documentación generada sobre las actuaciones realizadas en los equipos víctima es de utilidad directa en situaciones reales en las que un equipo ha sido atacado, sirviendo de guía en los pasos a seguir para realizar un análisis del ataque

Asimismo, la documentación generada sobre las actuaciones realizadas en los equipos víctima es de utilidad directa en situaciones reales en las que un equipo ha sido atacado, sirviendo de guía en los pasos a seguir para realizar un análisis del ataque.

Para concluir, se puede establecer que los resultados alcanzados como consecuencia del trabajo efectudo abren las puertas de una nueva línea de investigación que no ha hecho sino empezar, y que ayudará, en un futuro no muy lejano, a conseguir sistemas más seguros y a poder luchar contra los ataques usando un marco de trabajo común: la Informatoscopia.

En base a lo desarrollado se pueden establecer varias vías de trabajo futuras, como por ejemplo:

- Realización de modificaciones a distintos niveles (núcleo, utilidades del sistema, comandos de usuario,...) que permitan monitorizar la actividad en los equipos víctima, aún en el caso de que el atacante emplee métodos criptográficos, como conexiones ssh, que eviten el análisis directo del tráfico de la red.

- Instalación de una red más amplia de "sensores", incluyendo una mayor variedad de sistemas operativos y configuraciones, de forma que permitan estudiar la vulnerabilidad de los sistemas operativos más utilizados dentro de la red, pudiendo servir estos sensores para detectar nuevos patrones de ataques, alertando así a los responsables de la red.

- Implementación de sistemas que permitan simular el tráfico normal de usuarios en la red de sensores, de forma que se pueda estimular al atacante a intentar el acceso a otros sistemas igualmente controlados, para así poder evaluar la gravedad del ataque y, en lo posible, el motivo por el cual se ha producido.

- Evaluación de distintas herramientas de análisis forense y desarrollo de aquellas otras que puedan hacer falta para facilitar el análisis de los ataques.

6.- Bibliografía

[Abe01] J. J. López Abellán. *Análisis de tráfico en una red conmutada basada en un "backbone" ATM*. *BOLETIN de RedIRIS* nº 57, septiembre.2001. http://www.rediris.es/rediris/boletin/57/enfoque1.html

[aDF99] Wietse Venema, Dan Farmer. *Computer Forensic Analysis Class*, 1999. http://www.porcupine.org/forensics/handouts.html

[Alm01] C. Coll Almela. *Sirius: Sistemas de detección en la red de intrusos. Aplicación en la Universidad de Murcia.* Proyecto fin de carrera, Facultad de Informática. Universidad de Murcia, 2001.

[Cen02] Cert Coordination Center. *Cert/cc Statistics 1988-2001*, 2002. http://www.cert.org/stats/cert_stats.html

[FS90] D. Farmer and E. H. Spafford. *The COPS Security Checker System*. *USENIX Summer*, pages 165–170, 1990.

[Inc01] VMWARE Inc. Vmware, 2001. http://www.vmware.com

[KS93] G. H. Kim and E. H. Spafford. *Experiences with Tripwire: Using Integrity Checkers for Intrusion Detection*. Technical Report, West Lafayette, IN 47907-2004, 1993.

[Mes01] J. M. Navarro Meseguer. *Hades: Seguridad en la red y análisis forense*. Proyecto fin de carrera, Facultad de Informática. Universidad de Murcia, 2001.

[pro00] The Honeynet Project, 2000. http://proyect.honeynet.org.

[Tec02] Recourse Technologies. Mantrap, 2002. http://www.recourse.com/product/ManTrap/.

[Var00] Varios. *Bochs: The Cross Platform ia32 Emulator*, 2000. http://bochs.sourceforge.net.

F. J. Monserrat Coll
(Francisco.Monserrat@rediris.es)
Miembro del equipo de Seguridad de RedIRIS

J. M. Navarro Meseguer
(jmnm@alu.um.es)
(jose.navarro@f-integra.org)
Alumno de tercer ciclo
Universidad de Murcia