PED: Red de Equipos Trampa de REdIRIS

Francisco Jesus Monserrat Coll

Resumen

El análisis forense o estudio detallado de las acciones realizadas por los atacantes en un equipo informático es una de las ramas de la seguridad informática que más interés esta despertando en los últimos tiempos.

Este análisis es crucial a la hora de determinar los motivos por los que se produjo el ataque al sistema informático y evaluar el alcance de los daños que el atacante ha podido realizar en el equipo. Este análisis permite detectar nuevos patrones de ataque y herramientas antes de que tengan una mayor difusión, de forma que se pueda advertir rápidamente a los usuarios de los equipos. Sin embargo, muchas veces no es posible realizar este análisis ya que los propios administradores del sistema invalidan gran parte de la información al proceder a la reinstalación del equipo.

El proyecto de máquinas trampas de RedIRIS tiene como objetivo la instalación de una serie de equipos trampas monitorizados adecuadamente donde se puedan registrar los ataques que se producen a estos sistemas, para así poder obtener información sobre los nuevos ataques y patrones de comportamiento de los atacantes. Esta red de equipos trampa proporciona además banco de pruebas que pueden ser empleados después para otros proyectos de detección de intrusos

Palabras Clave: seguridad en redes e internet, seguridad en los sistemas operativos, análisis forense, redes trampa

1 Introducción

Una de las funciones del grupo de Seguridad de RedIRIS [1] IRIS-CERT, es la coordinación en incidentes de seguridad cuando están implicados universidades y centros asociados, así como la detección y alerta a estos centros de los posibles problemas de seguridad que puedan ir surgiendo.

En este contexto se ha establecido en coordinación con varias Universidades Españolas un proyecto para la creación de un sistema de máquinas trampas dentro de las Universidades que permita detectar y analizar los ataques informáticos.

Los ataques informáticos en los que un atacante consigue tener acceso remoto a cuantas de administración de los sistemas conectados a Internet, siguen siendo uno de los problemas de seguridad que con más frecuencia se siguen produciendo en Internet.

Gran parte de los ataques se producen con el único objetivo de obtener máquinas vulnerables para la creación de redes de equipos comprometidos que puedan ser usados en ataques de denegación de servicio contra otros usuarios o servidores, aunque la posibilidad de intentos de acceso a equipos con información confidencial (servidores de comercio electrónico, bases de datos corporativas, etc) es cada vez más alta y en el futuro es lógico pensar que este tipo de ataques, con el fín de obtener equipos "puente" desde los que lanzar estos ataques diriguidos sera cada vez más frecuente.

Debido a la complejidad y escasez de tiempo muy pocas veces es posible realizar un análisis detallado de las acciones que realiza el atacante en el equipo, siendo la reinstalación total o parcial del sistema el único procedimiento de actuación por parte de los administradores del equipo, destruyendo las trazas que pudiera haber dejado el atacante en el equipo.

Por otro lado el análisis forense es todavía un conjunto de técnicas todavía incipiente, en el cual se mezclan a partes iguales el empleo de herramientas especificas con un conocimiento pormenorizado de las interioridades de los sistemas operativos, enfrentándose muchas veces los administradores de los sistemas atacados a estos

[1] RedIRIS es la red académica y de Investigación Española, financiada por el Ministerio de Ciencia y Tecnología, que proporciona conectividad a Internet a más de 250 universidades y centros de investigación españoles

problemas por primera vez cuando se produce el ataque, por lo que se suelen cometer errores que pueden impedir una posterior acción legal.

Para intentar mejorar la respuesta ante estos incidentes de seguridad y poder proporcionar un sistema de alerta temprano que puede detectar estos nuevos patrones de ataque y por otro lado servir de fuente de información sobre los procedimientos de análisis forense en RedIRIS se inicio a mediados del año pasado un proyecto de creación de una red de equipos trampas, que pudieran ser víctima de estos ataques, pero con un control y monitorización que permitiera controlar las acciones realizadas por el atacante.

2 Equipos y Redes trampas

La instalación de equipos y redes trampas es una medida de seguridad que se ha venido aplicando desde hace bastante tiempo como una forma de evaluar las posibles acciones de los atacantes.

Inicialmente los equipos trampas eran sistemas atacados en los que una vez detectado el acceso de los atacantes a las cuentas privilegiadas del sistema se introducían aplicaciones modificadas que pudieran enviar información sobre las acciones realizadas por los atacantes, así como a la captura del tráfico.

Algunas de estas modificaciones podían consistir, por ejemplo en modificaciones a los interpretes de comandos para que almacenaran en un fichero de logs todos los comandos introducidos, o la modificación del servidor de logs para el envío de la información a un sistema remoto

La captura en otro equipo del tráfico de acceso de los atacantes presentaba en estos momentos problemas debido a las limitaciones de procesamiento y espacio de los equipos de red, que impedían almacenar todo el tráfico del atacante.

El problema de estos enfoques es que para poder estudiar las acciones del atacante se le estaba proporcionando acceso completo a los sistemas atacados, pudiendo los atacantes causar daños importantes a los datos existentes en el equipo si detectaban que habían sido descubiertos.

Otros tipos de sistemas trampas que se instalaban inicialmente consistían en "falsos" servicios habilitados en los equipos y que permitieran capturar los intentos

de ataque, para poder así analizar que tipo de ataque se estaba intentando emplear.

2.1 Proyecto HoneyNet

En el año 2000 se presento la idea de los modernos equipos trampas o "honeypot"[4] sistemas autónomos independientes monitorizados continuamente que permitieran realizar un análisis posterior de las acciones realizadas por los atacantes, empleando técnicas modernas de análisis forense como las mencionadas por Wietse Venema y Dan Farmer[3].

Estos equipos trampas no presentaban diferencias en la configuración a los sistemas que podrían estar instalados en producción en muchas redes, con la ventaja de no tener usuarios "legítimos" del sistema que pudieran sufrir interrupciones en el servicio debido a la detección de un ataque.

Entro los resultados de este proyecto destacan la puesta en Internet de un informe mensual de los ataques más frecuentes sufridos por estos equipos y la publicación de un libro con estos resultados [2].

3 PED: Máquinas trampas en RedIRIS

La red de máquinas trampas instaladas en RedIRIS consta en varios sistemas autónomos situadas en distintas redes de forma que los equipos no fueran atacados por un mismo atacante al realizar un barrido buscando equipos que estuvieran corriendo una determinada versión de un servicio vulnerable.

Estos sistemas autónomos están formados por dos equipos, uno es el equipo víctima, al que se le instalaban sistemas operativos de los que se conocía que existía una vulnerabilidad reciente y que estuvieran en uso en las Universidades[2]

El otro equipo funcionaba como equipo de control y almacenamiento de datos, empleándose para almacenar el tráfico que pudiera generar y almacenar la información del equipo víctima cuando se produjeran los ataques.

[2] Para averiguar las versiones se consultaban las estadísticas sobre incidentes de seguridad enviados a IRIS-CERT, para comprobar cuales eran las vulnerabilidades más usadas para acceder a los equipos

El equipo de control estaba configurado para funcionar como un puente Ethernet, conectado por un extremo al equipo víctima y por otro a la red de la organización. Esta configuración presentaba las siguientes ventajas con respecto a la configuración en red separada de los equipos trampa:

1. Permite la instalación de los equipos trampas en cualquier dirección interna de la red, sin tener que realizar ninguna modificación en el direccionamiento IP de la red.
2. A pesar de que el equipo trampa esta dentro de la red interna de la organización esta separado de la red principal, por lo que desde este equipo no se puede capturar el tráfico de la red externa desde el equipo trampa, solamente las tramas de broadcast llegan a este.
3. El equipo de control no aparece como un elemento dentro de la red de máquinas trampas. Al funcionar como puente a nivel Ethernet es posible configurar el equipo sin que tenga direccionamiento IP de la red trampa.

En la siguiente figura aparece una esquema de un sistema trampa con estas características:

Para la primera fase del proyecto tanto los equipos de control como equipos víctima son sistemas intel con Linux como sistema operativo en los equipos de control a los que se les configura el núcleo para el funcionamiento en modo puente Ethernet con captura de tráfico.

En uno de los proyectos desarrollados en colaboración con la Universidad de Murcia [1] aparece comentado con más detenimiento la configuración de uno de estos sistemas de máquinas trampas.

El empleo del equipo de control funcionando en modo puente Ethernet presenta las siguientes ventajas con respecto a una máquina trampa tradicional:

Captura de tráfico El proyecto realiza una captura de todo el tráfico con origen o destino las máquinas trampas y no solamente las alertas generadas por los sistemas de detección de intrusos. El tener todo el tráfico capturado permite analizar los escaneos e intentos de conexiones que puede que el IDS no detecte.

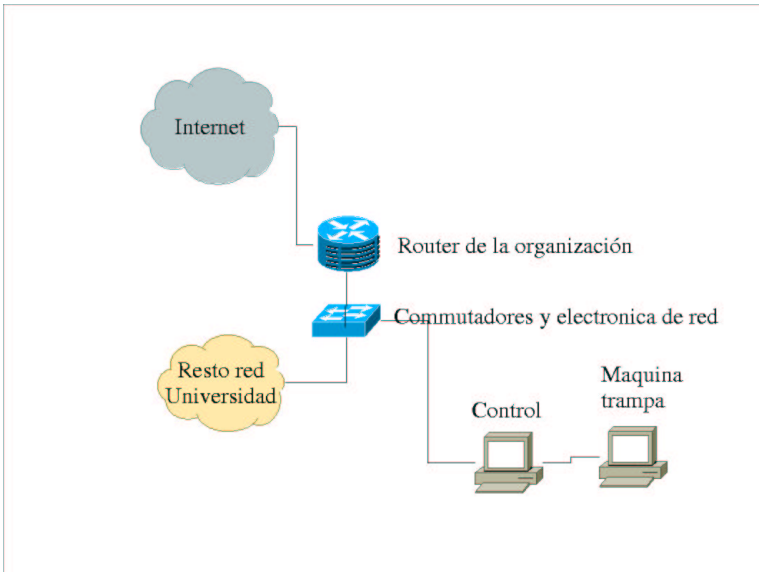

Figura 1: Esquema sistema trampa

Transparencia El sistema Trampa esta colocado de una forma transparente en la red destino, a nivel IP y MAC el equipo se encuentra en la mismo subred que el resto de equipos de la organización, aunque al estar tras el equipo de control no pueda capturar el tráfico generado entre dos equipos externos de la red.

Control de tráfico Es posible configurar el equipo de control para bloquear el tráfico una vez que se haya detectado el ataque, sin tener que tener acceso al router de la organización, lo que permite agilizar el bloqueo del equipo cuando se ha detectado que el atacante ha accedido al sistema.

Los primeros equipos trampas se instalaron en Agosto del año 2001, teniendo a finales de Septiembre tres equipos con sistemas Operativos RedHat Linux (6.2 y 7.0) y FreBSD (4.2). Estos equipos se situaron en dos redes IP distintas , una dentro de una red perteneciente a RedIRIS y otra en la Universidad de Murcia.

Estos equipos estuvieron funcionando durante estos meses, teniendo un total de tres ataques realizados con éxito por los atacantes.

El equipo de la Universidad de Murcia contaba con la protección adicional desde el exterior del filtrado de determinados servicios en el router de acceso, mientras que los equipos situados en la otra red no contaban con ningún filtro a estos niveles.

Durante estos meses se produjo a nivel global de incidentes de seguridad un aumento significativo de los ataques contra servidores IIS, motivada por la aparición de los gusanos CodeRED y NIMDA, como se desprende en las estadisticas publicadas por el CERT/CC[5] aunque esto no redujo el número de ataques contra servidores Unix empleando otras vulnerabilidades.

Debido al ritmo con el que se producían los ataques a los sistemas, a finales de Septiembre se bloquearon los sistemas para permitir el análisis de los datos obtenidos, evitar que los sistemas fueran atacados continuamente[3] y proceder a evaluar la continuación del sistema.

Para cada uno de los equipos atacados se procedió a analizar el ataque empleando diversas herramientas de análisis forense, y la metodología comentada en las páginas WWW del proyecto Honeynet[4], y un ejemplo práctico en el proyecto de la universidad de Murcia[1] comentado anteriormente.

En la siguiente tabla, aparecen reflejados el número de ataques que recibió una máquina trampa desde que fue conectada a la red hasta el momento en que un atacante obtuvo acceso al equipo. Este equipo fue conectado a la red sin ningún tipo de referencia , nombre en el DNS, o similar, y solamente una semana despúes un atacante consiguio acceder al sistema.

El sistema operativo, era una distribución del Sistema Operativo Linux aparecida un año antes del ataque, que presentaba varias modificaciones para evitar algunos de los ataques típicos de inyección de código, y aunque se conocía la existencia de posibles ataques contra este tipo de vulnerabilidad, sorprende la rápidez con que el equipo fue atacado.

[3] El sistema FreeBSD fue atacado por el mismo atacante una vez reinstalado, lo que podría indicar que los atacantes comprueban los equipos atacados, para ver si tras la reinstalación del Sistema operativo pueden volver a atacar

Puerto	Servicio	conexiones	Equipos	vulnerabilidad
0	icmp	4	4	Reconocimiento de equipos
21	FTP	23	15	Busqueda de servidores FTP con posibilidad de depositar ficheros en el incoming. Ataques contra el servidor FTP
22	SSH	1	1	Secure Shell vulnerabilidad muy extendida
53	DNS	2	1	Servidor de DNS. Varias vulnerabilidades.
80	HTTP	240	29	Servidor HTTP. varios gusanos que afectan a servidores IIS de Microsoft
111	Portmap	14	4	Empleado para acceso a servicios de RPC
137	Netbios	2	2	Compartición de ficheros en Windows
161	SNMP	1	1	Protocolo de gestión de Red, intentos de acceso publico, vulnerabilidades
1025	varios	7	4	Empleado por varios troyanos y rootkit como puerto de comunicaciones.
1433	MS-SQL	4	4	Conexiones de servidores SQL, nuevo gusano y vulnerabilides
1733		1	1	Desconocido , se trata de un solo paquete de conexión
12345	NetBus	1	1	Puerto por defecto del tronano NetBus de Windows
27374	Subseven	1	1	Puerto por defecto empleado por el troyano Subseven de Windows

Como se puede apreciar es bastante siginificativa el número de ataques, genera-

dos de forma aleatoria, que se producen debido a los problemas de seguridad en los servidores IIS de Microsoft. La no disminución de este tipo de ataques tras más de ocho meses desde que aparecieron las primeras versiones hay que encontrarla en la reinstalación de este tipo de equipos sin la actualización correspondiente de seguridad, lo que provoca una nueva infección de estos equipos.

4 Conclusiones y Viás futuras

5 Conclusiones

Las pruebas preliminares de estos sistemas trampas permiten indicar que estos sistemas pueden servir para detectar nuevos tipos de ataques y actividades por parte de intrusos en los sistemas, además de permitir comparar las efectividad de las herramientas de análisis forense en equipos con la información obtenida directamente de la red mediante la captura del tráfico que produjo el atacante, lo que permite un análisis completo y detallado de los ataques.

En los ultimos tiempos se ha planteado en diversos foros la posibilidad de emplear emulación software de equipos, como máquinas trampas, sobre todo para sistemas operativos, de forma que se pueda ampliar el tipo de sistemas operativos trampas dentro de una misma instalación, de forma que simplifique la gestión y mantenimiento de estos equipos.

Wlgunos tipos de ataques no pueden ser examinados completamente a nivel de red, ya que pueden involucrar conexiones encriptadas entre el equipo trampa y el atacante, por lo que una de las lineas de trabajo actuales es la modificación de las aplicaciones de almacenamiento de logs (syslog) y la creación de módulos de núcleo que permitan monitorizar el estado y funcionamiento del sistema, de forma las acciones que realice el atacante sean capturadas por el núcleo y aplicaciones del sistema y almacenadas para su estudio.

El análisis del tráfico obtenido por las máquinas de control es otra de las aéreas donde se debe profundizar, en coordinación con otros proyectos de detección de intrusiones que se está desarrollando ahora mismo en ReDIRIS, para poder detectar cuando se produce la intrusión y mantener un sistema de control inteligente que

permita el acceso del intruso al sistema pero evite que desde el equipo atacado se puedan llegar a producir ataques a otros sistemas.

Otro aérea de interés es la elaboración de herramientas que permitan un análisis de los equipos atacados, así como el almacenamiento fiable y seguro de la información de los equipos atacados, de forma que pueda ser utilizada en situaciones de intrusión real, en las cuales se desee realizar un análisis posterior del ataque.

Referencias

[1] Jose Manuel Navarra Meseguer *Seguridad en la Red y Analisis Forense*, Proyecto fin de carrera. Facultad de Informatica, Universidad de Murcia Murcia 2002.

[2] Varios, *Know Your Enemy: Revealing the security Tools, Tactics and Motives of the Black Hat Community* Addison-Wesley Pub Co. 2001

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

[4] The Honeynet proyect, *The honeynet proyect*, http://proyect.honeynet.org 2000

[5] CERT Coordination Center,, *CERT/CC Statistics 1988-2001* http://www.cert.org/stats/cert_stats.html 2002

Francisco Jesus Monserrat Coll Centro de Comunicaciones del CSIC RedIRIS
Consejo Superior de Investigaciones Cientificas
Calle Serrano 142
28006, Madrid.
E-mail: francisco.monserrat@rediris.es