Asegurando tu red con Linux

Gunnar Eyal Wolf Iszaevich
gwolf@gwolf.org
Instituto de Investigaciones Económicas — UNAM

Seminario Admin-UNAM
30 de junio, 2005

Afortunadamente, la época en que era indispensable hacer entender a los usuarios de Internet que hay más peligros acechando a su conexión de los que pueden imaginar ya pasaron — hoy todo mundo se conecta a Internet por lo menos con un granito de cautela y paranoia. La situación actual no es buena aún: Incluso con esta paranoia en su lugar, muchos usuarios no saben qué hacer respecto a los siempre inminentes virus, troyanos, gusanos y atacantes más que entrar en pánico. Claro está, hoy ya no sólo tenemos que defendernos contra atacantes humanos, hay cualquier cantidad de virus, gusanos y troyanos esperando que dejemos la más mínima puerta abierta para adueñarse de nuestro sistema y posiblemente de nuestra información. Por si esto fuera poco, por más cuidadosos que seamos con nuestro sistema, es muy difícil dictaminar qué tan bien hemos hecho nuestra tarea, qué tanto podemos confiar en la seguridad que hemos implementado.

Hay una gran cantidad de herramientas libres que podemos usar mejorar la seguridad de nuestra red, a muy diferentes niveles — Prevención, monitoreo y detección de intrusos. El espacio del que aquí disponemos es demasiado corto para entrar en detalle en cada uno de estos puntos, por lo que en este artículo presentaremos una visión general de cada uno de estos aspectos, y en futuras ediciones entraremos más a detalle en cada uno de ellos.

Prevención

Uno de los puntos en los que con mayor frecuencia encontraremos pequeñas máquinas con Linux en una gran cantidad de redes medianas y grandes es en la entrada, actuando como firewall. Un firewall es una suerte de policía de las comunicaciones, que inspecciona a grandes rasgos cada uno de los paquetes entrantes, descartando todo aquello que no cumpla con los patrones de tráfico que esperamos para nuestra red.

En Linux, un firewall se configura a través de IPtables. Podemos hacerlo a mano a través de una serie de comandos simples pero a veces algo engorrosos, o podemos utilizar asistentes como Firestarter `http://www.fs-security.com/`, muy simple de utilizar y suficientemente poderoso para configurar una red mediana. Una característica muy atractiva de Firestarter es que, además de ayudarnos a configurar el firewall, puede ayudarnos con el monitoreo de nuestra red en tiempo real.

Para configuraciones más complejas de lo que firestarter sabe manejar, podemos utilizar Shorewall `http://www.shorewall.net/`, describiendo nuestra red a través de archivos de configuración bastante simples de entender, o directamente aprender la lógica de IPtables. Uno de los mejores documentos para aprender acerca de IPtables es el tutorial creado por Oskar Andreasson `http://www.faqs.org/docs/iptables/`.

Cabe mencionar que el software que utilizamos para configurar un firewall global para nuestra red

Figure 1: Pantalla principal de Firestarter

Figure 2: El asistente de configuración de Firestarter

es el mismo que el que utilizaremos si queremos configurar un firewall personal, y que viene incluído en todas las distribuciones de Linux.

Monitoreo

Si sentimos que el rendimiento de la red o de nuestra computadora no está en niveles normales, es fundamental que podamos revisar exactamente qué está viajando por la red. El programa más simple y socorrido para este tipo de monitoreo es tcpdump `http://www.tcpdump.org/`, una simple utilería de consola que nos muestra un volcado de la actividad de red.

Sin embargo, para hacer un verdadero diagnóstico, es mucho más cómodo trabajar con un programa como Ethereal `http://www.ethereal.com/`, un analizador de protocolos muy completo y muy simple de utilizar, que nos permite aislar los diversos factores que afectan a nuestra conexión.

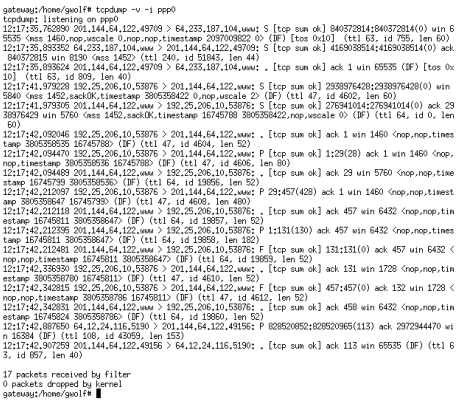

Figure 3: Corrida de TCPdump

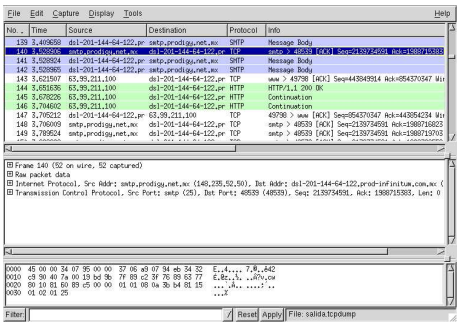

Figure 4: Pantalla principal de Ethereal

El monitoreo no sólo debe realizarse cuando sentimos que algo anda mal — El monitoreo debe ser una actividad constante, para poder encontrar a simple vista patrones de actividad anormal. Una de mis aplicaciones favoritas para este fin es el ya venerable MRTG `http://people.ee.ethz.ch/~oetiker/webtools/mrtg/`. Este programa reside en nuestro servidor y es ejecutado automáticamente cada cinco minutos. Depende de cómo lo hayamos configurado, recolectará los datos acerca de la carga de la red, el uso del CPU, memoria, o lo que le indiquemos. Es-

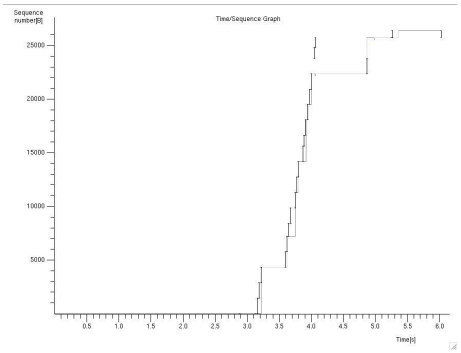

Figure 5: Gráfica de intercambio de paquetes sobre el tiempo en Ethereal

Figure 6: Ethereal reeensambla los paquetes y permite seguir una conexión TCP completa

tos datos nos son posteriormente presentados a través de nuestro navegador como una gráfica, guardando el histórico anual. Con esta información, tomada de un par de fuentes diferentes, es muy fácil determinar si el patrón de actividad actual es realmente normal o no.

Detección de intrusos

Un firewall es una parte fundamental de toda infraestructura de seguridad - Sin embargo, hay muchas cosas que un firewall es incapaz de hacer. Un firewall tiene que tomar decisiones extremadamente rápidas y basadas en tan poca información como sea posible, para evitar aletargar la red. Su tarea se limita a ver si una conexión es legal o no, pero no entra a revisar el contenido de cada una de estas conexiones - Para

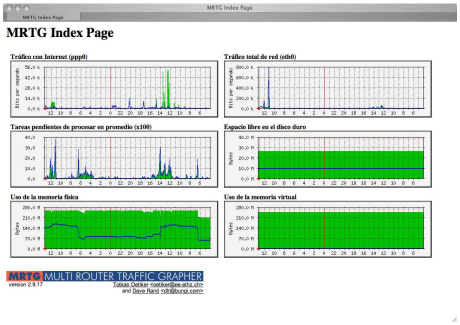

Figure 7: Página principal de MRTG

eso debemos emplear un sistema de detección de intrusos (IDS, por sus siglas en inglés). En el mundo del Software Libre, Snort `http://www.snort.org/` es definitivamente el motor de detección más potente y más utilizado.

Snort divide las tareas relativas a su trabajo de modo que —como es la norma en el Software Libre— puedan surgir varios proyectos relacionados, cada uno de ellos enfocándose en la excelencia de sus propias funciones específicas. Snort, además, simplifica la integración de un IDS completo en una red compleja, permitiendo colocar sensores independientes en los distintos puntos administrativos de la red, concentrando los datos en una base de datos central, la cual servirá de fuente de información a las consolas de alerta y de reporte.

Un recurso fundamental que nos proporciona Snort es, además, una muy completa serie de documentos relativos a la implementación de sistemas de detección de intrusos `http://www.snort.org/docs/`, tanto a nivel práctico como teórico, y tanto con Snort como con otros motores.

Una de las consolas de reporte más populares es ACIDlab `http://acidlab.sourceforge.net/`. Esta aplicación se utiliza via Web, y nos permite un acceso simple y completo a la base de datos que los sensores Snort han llenado. Para cada tipo de ataque reportado, nos da ligas a una explicación completa al respecto, y nos permite incluso ver el detalle -byte por byte- de la conexión que generó esta alerta.

Sguil `http://sguil.sourceforge.net/` es otra consola de reporte que se ha ido popularizando por

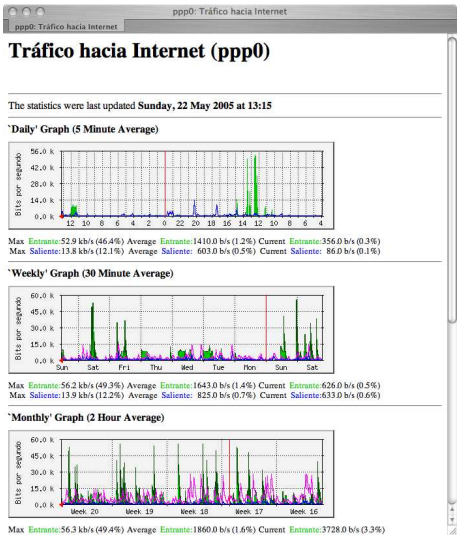

Figure 8: Monitoreo histórico de la conexión hacia Internet con MRTG

su mucho mayor interactividad que ACID. En vez de correr como un juego de scripts en un servidor Web, Sguil es una aplicación GUI escrita en tcl/tk, y que funciona nativamente en Linux, otros Unixes (*BSD, Solaris), MacOS y Windows. El único pero que podemos ponerle a Sguil es que no está tan maduro, y llega a presentar algunos problemas para correr en ciertos sistemas.

En resumen

En el mundo del Software Libre encontraremos una tremenda cantidad de herramientas que pueden ayudarnos a brindar seguridad a nuestra red, independientemente de qué sistemas estemos ejecutando en esta. Muchos de los programas aquí mencionados son multiplataforma (esto es, corren tanto en Linux y otros sistemas Unix como en Windows o Mac), y sin duda serán una gran ayuda para el mantenimiento de la seguridad de nuestras redes.

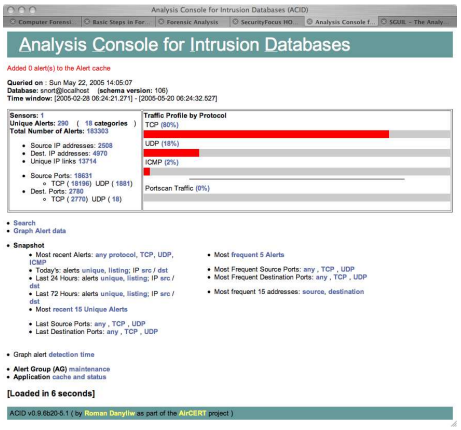

Figure 9: Pantalla principal de ACIDlab

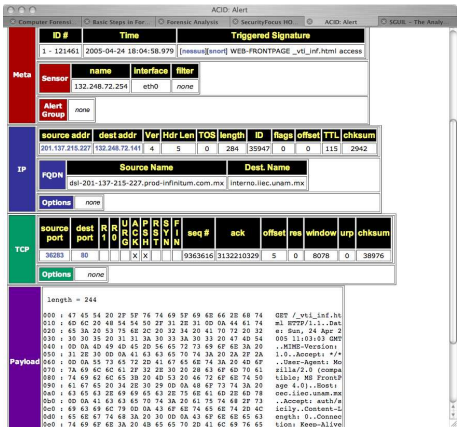

Figure 10: Detalles de una alerta en ACIDlab

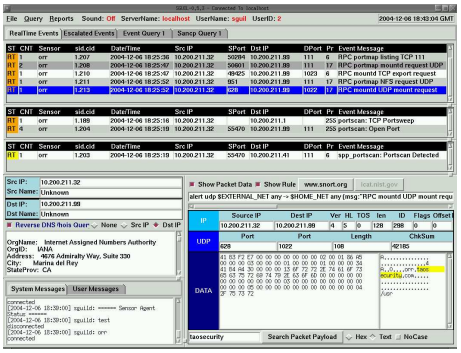

Figure 11: Pantalla principal de Sguil