Redes Seguras Usando el Sistema GNU/Linux

Luis Gerardo de la Fraga

Sección de Computación
Departamento de Ingeniería Eléctrica
CINVESTAV-IPN
Av. Instituto Politécnico Nacional 2508. 07300 México, D.F.
E-mail: fraga@cs.cinvestav.mx

Resumen

Se presenta la experiencia de trabajo en la seguridad de la red de la Sección de Computación del CINVESTAV. Se describirán dos soluciones para la construcción de redes seguras: una por división de redes usando puertas (gateways), cortafuegos (firewalls), lo que generan los esquemas de redes militarizadas y redes desmilitarizadas; y otra por monitoreo de paquetes de la red. Los esquemas aquí presentados permitirían formalizar un esquema de pago por uso de red a usuarios con máquinas propias (laptops).

Palabras clave: Redes, Seguridad en Redes, Puertas (Gateways), Cortafuegos, Monitoreo de Red.

1 Introducción

Este es el escenario en que laboramos en la Sección de Computación del CINVESTAV: cerca de 80 estudiantes de posgrado, varios laboratorios de cómputo, varios servidores (correo, WEB, nombres [DNS], disco, etc) a los que hay que proteger; y algunos de nuestros estudiantes están trabajando en sus tesis con redes y servicios experimentales, tal como IPv6. En este escenario se requiere de esquemas que nos permitan laborar a todos. Los requerimientos de estos esquemas pueden resumirse en tres ideas: a) Que los estudiantes solo puedan acceder a los servicios de red permitidos, b) Que los trabajos experimentales con programas o redes no dañen nuestra red, c) Hacer frente a los ataques externos a nuestra red.

Es fácil imaginarnos que una configuración de red "normal" – cada computadora dentro de nuestra red con una dirección IP estática –, no nos permitiría trabajar a todos armoniosamente. El punto (a) fallaría porque todas las máquinas reservadas para los estudiantes podrían acceder directamente a Internet. Históricamente esto no es permisible porque los estudiantes han instalado servidores propios, como chat o música, que han consumido todo el ancho de banda de la red; esto es, el tráfico es tan intenso que Internet se vuelve inexistente a los profesores. El punto (b) es obvio ya que en el proceso de aprendizaje para configurar redes TCP/IP se pueden cometer fallos; si se realiza una mala configuración se ve afectada toda la red. Y el punto (c), la seguridad de toda la red contra ataques provenientes de Internet, nos pone en una actitud defensiva en que debemos contar con una plataforma que nos permita, tanto saber que está pasando en nuestra red, como corregir sus posibles fallos.

En este trabajo se describirán de forma general las soluciones realizados para controlar nuestra red. Estas soluciones pueden servir

para otras redes en que se tienen escenarios semejantes. No se describirán aquí en detalle las configuraciones, ya que esto sería motivo de otro artículo. Las configuraciones en detalle pueden encontrarse en los archivos COMO (en inglés, HOWTO) en [1, 2, 3] y en varios otros artículos [4, 5, 6, 7].

El sistema operativo libre GNU/Linux [8] se usa en las soluciones de seguridad de redes aquí presentadas por varias razones: se tiene acceso al código fuente, y esto permite encontrar soluciones a los posibles problemas; usándolo en simples computadoras personales permite contar con soluciones de software, en vez de hardware que es muy caro, de ruteadores y cortafuegos; y otro punto más importante, la arquitectura de GNU/Linux (tiene el subsistema de control de red dentro del mismo núcleo del sistema operativo) lo hace muy eficiente en los servicios de red, tanto como para rivalizar con el hardware especializado de ruteadores y cortafuegos.

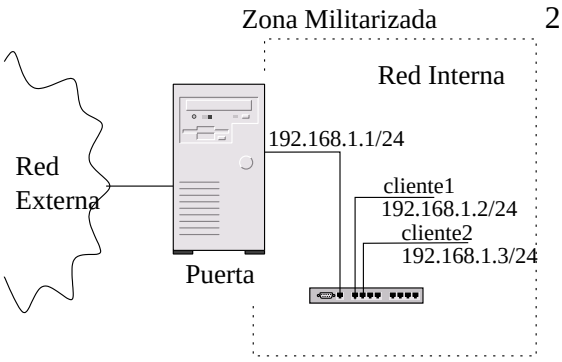

Figura 1: Esquema de uso de una puerta (gateway)

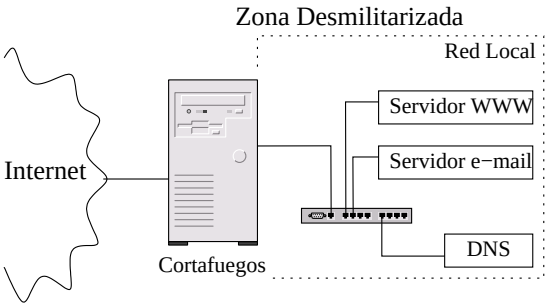

Figura 2: Esquema de uso de un cortafuegos

2 Puertas, cortafuegos, zonas militarizadas y zonas desmilitarizadas

El esquema principal usado para aumentar la seguridad en nuestra red fue particionar nuestra red usando *puertas* (gateways). Un *puerta* es una computadora con dos interfaces de red y que sirve para conectar dos redes diferentes. El esquema de uso de una puerta puede verse en la Fig. 1

La Fig. 1 muestra como puede realizarse una red interna con direcciones IP *no válidas* con una puerta. Direcciones IP *no válidas* son las especificadas en el RFC1918 [1, 9, 6] para diseñar redes privadas o intranets, y son las recomendadas para usarse cuando se experimenta con redes. Estas direcciones son $10.*.*.*$, $172.16.*.*$ a $172.31.*.*$ y $192.168.*.*$. Todos los ruteadores actuales filtran estas direcciones por lo que no es posible accesar estas direcciones desde Internet. Esta característica hace casi imposible acceder a las máquinas de la red interna, pero a su vez todas las computadoras en la red interna pueden acceder la red externa e Internet. Un controlador de la puerta en la Fig. 1 tiene una dirección IP válida (no mostrada en la figura) y el otro controlador tiene una dirección IP inválida (192.169.1.1 en la misma figura 1). Toda el esquema de la red y la red interna se conoce como *red militarizada*.

La definición de un *cortafuegos* [10] es semejante a una puerta –una máquina que tiene dos interfaces de red que sirve unir dos redes diferente–, solo que ahora es necesario configurar *reglas* de acceso en cada interfaz. Estas reglas pueden ser por red, por dirección IP y/o por protocolo, y con esto definen lo puede pasar (o bloquear) por cada una de sus interfaces. El esquema de uso de un cortafuegos se muestra en la Fig. 2

Entonces, el cortafuegos de la Fig. 2 es una puerta (en la Fig. 1), con reglas de acceso en cada una de sus interfaces. Esto nos permite

realizar el esquema de una *red desmilitarizada* [11]. A diferencia de una red militarizada, la red desmilitarizada tiene dirección IP válidas en todas las máquinas de la red local. En la red local de la Fig. 2 se mantienen los servidores locales (WWW, e-mail, DNS, etc.) que deben ser visibles desde Internet. En este caso la dirección IP de la conexión del cortafuegos a Internet puede no existir desde Internet, esto es lo que se llama un *cortafuegos transparente*

Las puertas y cortafuegos que hemos utilizado han sido máquinas con microprocesador pentium, con discos duros de menos de 1GB y 64MB de memoria RAM, con tarjetas de red ethernet 100TX. Estos nos han bastado para controlar redes internas de hasta 40 computadoras, estos es hasta de 40 clientes, sin notar pérdida de eficiencia. Como se puede notar en los diagramas de las Figs. 1 y 2, las puertas y cortafuegos utilizados son computadoras personales sin monitor ni teclado. La consola de acceso se ha puesto a través del puerto serial y si es necesario abrir la consola se utiliza el puerto serial de la computadora más cercana al cortafuegos, usando un cable serial nulo y el programa *minicom*. El acceso más común al cortafuegos es a través de la misma red, para ello se usa el SSH (Secure SHell) y solo se abre la entrada de este protocolo. Las reglas puestas en los cortafuegos han sido permitir la salida al exterior de los servicios de SSH, WEB, WEB seguro (https), FTP, IMAP y POP3 (estos dos últimos para poder checar correo en los servidores generales). Todos los demás servicios de red han sido denegados, implicando que el chat, messanger y otros no se pueden realizar. Estas reglas de uso de la red se han ido cambiando según las circunstancias y de observar como nuestros estudiantes hacían uso de la red.

Un esquema total de la red se presenta en la Fig. 3. El ruteador es necesario para prevenir ataques de fragmentación de paquetes a nuestra red. El ruteador puede construirse también con una máquina con GNU/Linux [12] aunque en nuestra red actual contamos

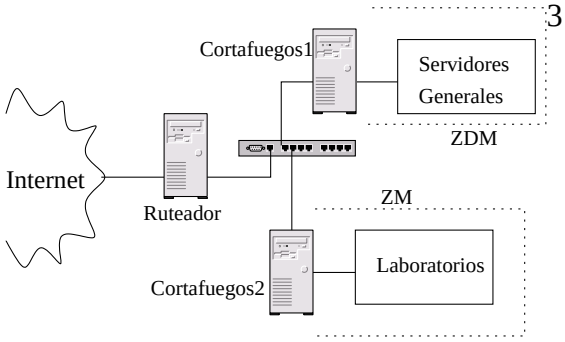

Figura 3: Esquema de una red segura.

con un ruteador comercial. Este ruteador es tan "inteligente" que permite colocar reglas de cortafuegos en él, y esto nos ha permitido prescindir del Cortafuegos1 en el diagrama de la Fig. 3. Nuestra red actual cuenta con varios esquemas de redes militarizadas, cada una con un cortafuegos propio, uno por cada laboratorio de cómputo con que contamos. Se tienen configurados DHCPs dentro de cada red militarizada para que los usuarios con máquinas portátiles, y en los salones de clase, puedan accesar automáticamente a la red.

3 Monitoreo de la red

Como viene especificado en la documentación del CERT [13] (Computer Emergency Response Team) , no es suficiente tener cortafuegos para garantizar la seguridad en una red. Es necesario contar además con técnicas activas para saber que está pasando en la red. Esto puede realizarse monitoreando la red.

En el esquema de la Fig. 3 los puntos que pueden servir claramente para el monitoreo son el ruteador y los cortafuegos. Las reglas de configuración de estos elementos de red permiten que se active el registro de los paquetes, ya sean aceptados o rechazados, y se generen *archivos de auditoría*. Se puede activar un servidor especial para guardar todos los archivos de auditoría, ya que en un ataque con la red se pueden borrar estos archivos para no dejar huellas del ataque. Este servidor de auditoría puede ser una puerta sin direc-

ción IP en una interfaz y la otra interfaz se requeriría para tener acceso a él a través de una red paralela para su administración [14].

Una vez que se cuentan con los archivos de autoría se hace necesario realizar un software que presente los resultados en forma gráfica. Aquí lo que hemos realizado es la presentación de gráficas de uso de la red en una página WEB interna, usando PHP y MySQL. Un sistema semejante, libre, para registrar el comportamiento del servidor de nombres, puede verse en [15].

4 Trabajo a futuro

Actualmente de están desarrollando dos tesis de maestría para la elaboración de software para la presentación y monitoreo de red [16, 17]. Eventualmente el software será liberado a la comunidad bajo la licencia GPL, esto es, será libre y podrá modificarse con la condición de que se agregue la licencia misma. En este año de deben tener disponibles las versiones usables. Se puede checar mi página WEB para tener noticias sobre ello [1].

También estamos migrando los cortafuegos, que están funcionando con IP-Chains [1], a IP-Tables [18, 19]. IP-Chains e IP-Tables son los programas que permite realizar las reglas del cortafuegos. Esta migración nos permitirá usar características propias de IP-Tables que no se encuentran en IP-Chains, en especial poner reglas de acceso por dirección ethernet (o dirección MAC). Hoy en día tenemos problemas debido al uso de computadoras móviles (laptops) en cualquier parte de nuestra red. Y esta característica de restringir el acceso por dirección MAC (la dirección debe ser única por cada computadora y es intrínseca a la tarjeta de red usada) solo a las laptops registradas. Debido al abuso del uso de red en horarios no habituales, se está pensando en llevar el registro de uso de red, primero para publicarlo a la vista de todos los usuarios y posiblemente para generar un cargo por uso de red.

Los mismos sistemas aquí presentados se extenderán a los laboratorios de red inalámbricos que se construirán.

Para terminar, el CERT [13] publica que un sitio ideal en seguridad debe contar con:

1. Estar al día en parches
2. Tener cortafuegos
3. Deben monitorearse la red.
4. Deben deshabilitarse los servicios y características que no son necesarios
5. Tener un software de antivirus instalado, configurado y al día
6. Un equipo entrenado y con capacidad de respuesta a incidentes.

Así que además de los sistemas aquí presentados es necesario contar con un equipo de trabajo dedicado a la seguridad de la red. Y nuestra experiencia es que se puede pensar en tener una red segura si se tiene un equipo de trabajo que lleve a cabo las ideas de seguridad.

5 Conclusiones

En este trabajo se describen las soluciones usadas para contar son una red segura en la Sección de Computación del CINVESTAV:

- Usar cortafuegos para dividir la red en zonas desmilitarizadas, donde se encuentran nuestros servidores generales, y zonas militarizadas para los laboratorios de estudiantes y laboratorios experimentales.
- Generación de archivos de auditoría y análisis de los mismos para presentar en forma gráfica, en páginas WEB el comportamiento que está teniendo la red.

[1] Página personal en: http://delta.cs.cinvestav.mx/~fraga/Programas

Estas soluciones están basadas en simples computadoras personales, que pueden ser viejas máquinas, con el sistema operativo GNU/Linux. También estas soluciones pueden implementarse en cualquier otra red. La seguridad el día de hoy es vital para el funcionamiento de una red, es por ello que estas soluciones son factibles de adoptarse en otros escenarios, debido al costo nulo del software y la muy eficiencia de estos sistemas para su trabajo en red.

Referencias

[1] The Linux Documentation Project. *IPCHAINS–HOWTO*.

[2] www.tldp.org. *Networking-Overview-HOWTO*.

[3] www.tldp.org. *Net-HOWTO*.

[4] L. Teo. Setting up a linux gateway. *Linux Journal*, (72):86–88, April 2000. www.linuxjournal.com.

[5] P.F. Crow. The linux home network. *Linux Journal*, (72):80–84, April 2000.

[6] J.D. Blair and L. Grinzo. Connected to the net. *Linux Magazine*, 2(5):50–59, 2000. www.linux-mag.com.

[7] C. Easwaran. Linux apprentice: A heterogeneous linux/windows 95 home network. *Linux Journal*, (76):62–67, August 2000.

[8] R. Stallman. Linux and the gnu project. http://www.gnu.org/gnu/linux-and-gnu.html.

[9] www.tldp.org. *IP–Masquerade–HOWTO*.

[10] Cert® security improvement modules, module: Deploying firewalls, 2002. http://www.cert.org/security-improvement/.

[11] M. Bauer. Designing and using dmz networks to protect internet servers. *Linux Journal*, (83):27–36, March 2001.

[12] K. Anwar, M. Amir, and A. Sa. The linux router. *Linux Journal*, Aug 2002.

[13] A. Householder, A. Manion, L. Pesante, G.M. Weaver, and R. Thomas. Managing the threat of denial-of-service attacks. v10.0. *CERT® Coordination Center*, Oct 2001. www.cert.org.

[14] J. B. Ullrich and W. Larmon. Administering a distributed intrusion detection system. *SysAdmin*, 11(8), Aug 2002.

[15] G. Heim. Maintaining dns sanity with hawk. *SysAdmin, the Journal for UNIX systems administrators*, 11(12), Dec 2002. http://www.samag.com/articles/2002/0212/.

[16] J. Lizárraga. Operación de cortafuegos con el sistema gnu/linux. Master's thesis, CINVESTAV, 2003. En proceso.

[17] J. E. Morfín Galván. Análisis de tráfico en una LAN. Master's thesis, CINVESTAV, 2003. En proceso.

[18] D.Ñapier. Iptables/netfilter – linux's next-generation stateful packet filter. *SysAdmin*, 10(1), Dec 2001.

[19] M. Bauer. Paranoid penguin: Using iptables for local security. *Linux Journal*, 2002.