Seguridad y Configuración de Redes de Computadoras con GNU/Linux

Enrique Bonilla Enríquez y 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 expondrán los mecanismos que hemos usado en la Sección de Computación del CINVESTAV para la seguridad y mantenimiento de nuestros laboratorios de cómputo: a través de cortafuegos y zonas militarizadas (redes con direcciones IP privadas), el arranque del sistema vía red (usando PXE ó Etherboot) y usando un sistema de archivos distribuido (NFS y AFS). Estos mecanismos nos han permitido optimizar el uso de los recursos en la red: facilita el mantenimiento de la misma red, el uso de discos duros y la implantación de políticas de respaldo.

1. Introducción

Actualmente en la red de la Sección de Computación se tienen cinco subredes, dos redes con computadoras Linux, dos redes de computadoras Windows, una red de computadoras MaC y también una red inalámbrica; conjuntamente suman en total unas cincuenta computadoras fijas con unas dos docenas de computadoras que accesan la red inalámbrica.

También tenemos que dar servicio a cerca de 80 estudiantes de posgrado, 12 investigadores, varios servidores generales (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, monitoreo de redes y redes inalámbricas.

En este escenario existen dos preocupaciones básicas: seguridad y facilidad de mantenimiento de toda nuestra red.

La seguridad es básica porque hemos establecido que los estudiantes solo deben acceder a los servicios que les tiene permitido (se ha establecido la política de que que los laboratorios son para realización de trabajo, pero no para recreación), se deben de proteger los servidores centrales y también se debe proteger toda la red de los posibles ataques externos.

El mantenimiento también es un punto básico porque tener en estado óptimo a tantas computadoras aisladas se había convertido en un trabajo arduo y difícil.

En este artículo describiremos las soluciones encontradas para conseguir tanto seguridad como facilidad de mantenimiento de nuestra red usando el sistema GNU/Linux. Se ha usado el sistema operativo libre GNU/Linux [1] debido a que ha demostrado ser altamente eficiente y confiable, además ha permitido un enorme ahorro en gastos de licencias que se tendrían que pagar si se usara

software propietario. Todos los servidores de la Sección, por ejemplo, funcionan desde hace más de cuatro años con GNU/Linux.

2. Seguridad

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. Históricamente se han tenido los siguientes problemas. Los estudiantes en su trabajo de tesis se les asigna una computadora propia e instalaban servidores propios, como chat o música, que consumían todo el ancho de banda de la red; esto es, el tráfico era tan intenso que Internet se volvía inexistente para todos los demás usuarios. Otro problema fue que los estudiantes cometían fallos al empezar a trabajar en redes TCP/IP; y si se realiza una mala configuración se veía afectada toda la red. Y 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.

La solución encontrada fue aislar los laboratorios y las redes experimentales de nuestra red local. El esquema general puede verse en la Fig. 1. Los laboratorios se aislaron con un cortafuegos con el servicio de traducción de direcciones (NAT, del inglés Network Address Translation) activado. Esto nos permite poner direcciones IP inválidas [1] Esta característica hace casi imposible acceder a las máquinas de la red interna (solo es posible accesarla si directamente se ingresa al cortafuegos, lo que podría ser un hueco de seguridad), pero a su vez todas las computadoras en la red interna pueden acceder la los servidores generales e Internet. La interface de red del cortafuegos que se conecta a la red local tiene una dirección IP válida (no mostrada en la figura) y la otra interface de red tiene una dirección IP inválida El esquema de la red privada, con números IP inválidos, lo hemos llamado *red militarizada*.

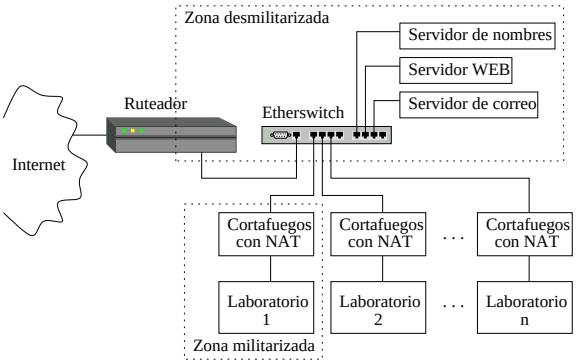

Figura 1: Esquema general de la red de la Sección de Computación del CINVESTAV. El ruteador es inteligente, lo que nos permite crear políticas de acceso para toda la red, lo que crea un esquema de *zona desmilitarizada*. Dentro de cada cuadro de *laboratorio n* existe otro etherswitch con varias computadoras conectadas a él.

El ruteador mostrado en la Fig. 1 es tan inteligente que nos permite poner reglas de acceso (es si, forma otro cortafuegos) para nuestros servidores y cortafuegos con NAT, que tienen números IP válidos. Este esquema de una red, con números IP válidos, protegida con un cortafuegos lo hemos llamado *red desmilitarizada*.

Los usuarios de los laboratorios pueden accesar a todo Internet con los servicios de WEB y ssh (puertos 80 y 22). También tienen acceso a los servicios de POP3 e imap para el servidor local de correo electrónico. Cualquier otro servicio es denegado.

Las máquinas que hemos usado para los cortafuegos con NAT de la Fig. 1 han sido máquinas con procesador Pentium, de 190 MHz a 300 MHz, y con 64MB en RAM. Esto a sido suficiente para mantener a alrededor de 40 usuarios, aunque no hemos pruebas exhaustivas de cuantos usuarios podría sostener

[1] Direcciones IP *inválidas* son las especificadas en el RFC1918 [2, 3, 4] 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 $192{,}168.*.*$.

una configuración dada.

Hemos usado tanto *IP-Chains* [2] y últimamente se ha emigrado a *IP-Tables* [5, 6] para la realización de los cortafuegos con NAT. La configuración para IP-Tables se ha tomado de [7]. Para el acceso a nuestra red inalámbrica se ha configurado un *Punto Caliente* en el mismo cortafuegos como se describe en [8] realizado con el software NoCat [8], se usa una autentificación de usuarios con un servidor LDAP en nuestro servidor WEB.

3. El Problema en la Red de la Sección de Computación

En cada una de las redes de la Sección de Computación no existe una homogeneidad en el acceso a sistemas de archivos: dos de las redes (Linux) se pueden accesar con un mismo login y password, pero no se tiene acceso a los mismos sistemas de archivos, al accesarse cada una de las redes se tiene un contenido de archivos diferente. Se pretende realizar un esquema con el cual, desde cualquier red, del tipo que sea, cualquier persona registrada en algún servidor central de la sección pueda ver sus archivos de una forma transparente. Actualmente este es un tema de tesis de maestría [9] que se desarrolla en la Sección.

Con la disposición de un mismo árbol de directorios a todos los usuarios de la red, se conseguiría eficientar el uso de los recursos. En específico, se obtendría lo siguiente:

1. Cada usuario, al poder accesar su cuenta desde cualquier punto de la Sección evita tener que enviar archivos vía e-mail o utilización de otros medios para poder mover información de un laboratorio a otro.

2. Al contar con una centralización del servicio de acceso a disco, se podrá tener una solución eficiente para el respaldo de la información almacenada en los discos duros.

3. Al tener un servidor central de archivos, se eficientará el uso de discos duros. Actualmente ya no se pueden adquirir discos de baja capacidad (abajo de 10GB) para almacenar solo el sistema operativo de arranque, como actualmente se usa en un laboratorio Linux. El servidor central evita que las computadoras tengan fracciones grandes de disco duro sin utilizar.

4. Se pretende eliminar el uso de discos duros por parte de las máquinas cliente, habilitando el arranque remoto vía red.

5. Se incrementará la seguridad de acceso. Se desea que ahora se valide al usuario que intenta accesar los archivos y no a la máquina que quiere accesar al archivo; ahora se busca autenticación a nivel de usuario.

Con el punto 4, el arranque vía red, pretendemos solucionar el problema de la administración del tipo de sistema operativo y las aplicaciones instaladas en cada computadora dentro de un laboratorio. Esto puede llegar a ser una tarea compleja y costosa, dado que se tiene que realizar la misma tarea por cada cliente, ó computadora. Por ello es deseable tener el control de ambas cosas, tanto el tipo de sistema operativo a ejecutar en una máquina, como las aplicaciones a las que ésta puede acceder.

3.1. Los sistemas de archivos distribuidos

Un sistema de archivos distribuido [10] es una aplicación del tipo cliente-servidor la cual permite al usuario usar sus archivos como si estos estuvieran localmente, todo el intercambio de información necesaria entre el cliente y el servidor es transparente para el usuario. La siguiente lista muestra diferentes tipos de sistemas de archivos distribuidos:

AFS - Andrew Filesystem [10]. Protocolo utilizado para redes LAN y WAN.

CODA - Protocolo experimental para equipos desconectados (wireless) [11].

NFS - Network filesystem (Unix). Protocolo utilizado en sistemas Unix [10].

NCP - NetWare Core Protocol (NCP, de Novell NetWare) [12]. Protocolo utilizado en sistemas Novell.

SMB - Server Message Block Protocol(Windows 3.x/9x/NT) [12]. Protocolo utilizado en sistemas Windows.

INTERMEZZO - Protocolo experimental de un sistema de archivos distribuido [13].

La implantación del sistema que se pretende realizar [9] es con OpenAFS [14], debido a que es el protocolo que más usuarios concurrentes soporta, pues los demás protocolos (NFS, Intermezzo, SMB) soportan menos de cincuenta usuarios. Aún cuando otros tienen mejores características como poder trabajar en redes inalámbricas, como CODA e Intermezzo, estos se encuentran en desarrollo experimental, por lo que no es adecuado para su uso diario, algunos otros (NCP) son comerciales y hay que pagar licencias de software para su uso.

3.2. La solución al problema en la Sección de Computación

Resumiendo, para resolver el problema en nuestra red se pretende realizar lo dos puntos siguientes:

1. Arranque vía red de las máquinas cliente.
2. Centralización del servicio de disco.

La solución al punto 1 ha sido realizada en nuestros laboratorios Linux usando el protocolo PXE (Preboot eXecution Environment) [15], que viene incluido en las tarjetas madres más nuevas. Para el arranque de las máquinas que no tienen intercontruido PXE se ha usado Etherboot [16] que permite el arranque desde un CDROM o diskete. El archivo de arranque fue generado en www.rom-o-matic.net.

Tanto PXE como Etherboot necesitan configurar los servicios de un DHCP y de tftp (Trivial Transfer Protocol). Brevemente, el arranque remoto funciona de la siguiente manera: El DHCP relacionada la dirección ethernet (ó MAC) de la tarjeta de red con una dirección IP, además que le indica los demás parámetros de red y la dirección del servidor de disco y donde se encuentra el núcleo del sistema. Se carga el núcleo usando el tftp y lo ejecuta. Dentro del servidor de disco existe una raíz separada para cada máquina cliente donde se almacena su configuración (en /etc) y los archivos de auditoría (bajo /var).

El punto número 2 lo tenemos implantado con la solución directa de usar NFS para cargar tanto el archivo raíz, los paquetes instalados y el directorio de *casa* del usuario. Esto conlleva recompilar el núcleo del sistema (en especial que tenga dentro del cliente de NFS y la ópción de cargar la raíz vía NFS). La red de máquinas Windows carga el directorio *casa* de los usuarios a través de SMB, por lo que también el servidor de disco tiene instalado SAMBA.

Esta solución es proveída por el proyecto de Servidor de Terminales Linux [17] aunque nosotros hemos querido usar nuestra propia solución con la distribución GNU/Linux de RedHat tal como se describe aquí.

Ahora, a trabajo a futuro se quiere implantar en la Sección el sistema de archivos AFS en vez de NFS. En la tabla 1 se presentan algunas instituciones alrededor del mundo donde se ha implantado satisfactoriamente OpenAFS [14].

Creemos que AFS es la solución a nuestro para resolver el problema de tener un solo sistema de archivos para cada usuario en cualquier parte de nuestra red, por las siguientes razones:

Universidad	Sistema Operativo	Usuarios
KTH Royal Institute of Technology (Suecia)	Compaq's Tru64 UNIX (Alpha Server)	200-400
Dr. Wilhelm Andre Gymnasium (Alemania)	Linux	1500
New Jersey Institute of Technology University (USA)	Linux, Solaris	17000

Cuadro 1: Instituciones donde se ha implantado satifactoriamente AFS

- Uso de cache a nivel cliente, el cual evita accesos frecuentes al servidor [10].
- Seguridad de envío de password, al usarse kerberos para encriptar el password que viaja en la red [18].
- Independencia en ruta, al evitarse que cada máquina cliente necesite saber la localización del servidor [10].
- Escalabilidad, al permitir transparentemente agregar clientes y servidores sin tener que detener el servicio [19].
- Servicio para LAN y WAN, donde la relación número de clientes por servidor puede llegar a ser de doscientos clientes a uno [18].

En el CONSOL-2005 esperamos presentarles los pormenores de nuestra implantación de AFS y las pruebas de rendimiento, entre varias configuraciones del sistema, que realizaremos con [12] y con lo que esperamos demostrar que AFS se comporta mejor que NFS.

4. Conclusiones

En este trabajo se describen las soluciones usadas en la Sección de Computación de CINVESTAV para:

1. Contar con una red segura. Hemos usando 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.

2. Optimizar el uso de recursos. Aquí hemos implantado el arranque en red de las máquinas cliente y la centralización del uso de disco duro. Esto nos ha permitido eficientar el uso de los discos duros (no se tienen muchos discos grandes, uno en cada máquina cliente) y facilitarnos la administración de nuestra red (se mantiene un servidor por cada laboratorio).

Para los cortafuegos hemos usado computadoras personales simples, que pueden ser máquinas viejas de baja velocidad, con el sistema operativo GNU/Linux. Nosotros hemos usado la distribución de RedHat.

Actualmente usamos el arranque remoto vía PXE en las máquinas cliente con tarjetas madres nuevas y se arranca en CDROM usando Etherboot para las máquinas sin PXE interconstruido. Se una NFS para centralizar el uso de disco duro.

Se ha planteado que AFS puede dar la solución para mostrar una misma *casa* a todos los usuarios de forma transparente. En el siguiente congreso pretendemos presentar los resultados de la implantación de AFS en nuestra red.

Los detalles de las implantaciones descritas en este artículo pueden encontrarse en los archivos COMO (ó HOWTO) en la URL http://www.tldp.org. Los detalles específicos pueden encontrarse en la página WEB http://delta.cs.cinvestav.mx/~fraga/Programas

Referencias

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

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

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

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

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

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

[7] G. Mourani. *Securing & Optimizing Linux: The Ultimate Solution*. July 2002. Disponible en http://www.tldp.org.

[8] M. Kershaw. Linux-powered wireless hot spots. *Linux Journal*, (113), Sep 2003.

[9] Enrique Bonilla Enríquez. Implantación de un sistema de archivos distribuido usando afs. Master's thesis, CINVESTAV, 2004. En proceso.

[10] E. Levy and A. Silberschatz. Distributed file systems: Concepts and examples. *ACM Computing Surveys*, 22(4), Dec 1999.

[11] El sistema de archivos coda. En http://www.coda.cs.cmu.edu.

[12] Iozone file system benchmark. http://www.iozone.org.

[13] El sistema de archivos intermezzo. En http://www.inter-mezzo.org.

[14] Sitio de openafs. En http://www.openafs.org.

[15] Preboot execution environment (pxe). http://www.intel.com/labs/manage/wfm/wfmspecs.htm.

[16] Proyecto etherboot. http://etherboot.sourceforge.net.

[17] The linux terminal server project. www.ltsp.org.

[18] Preguntas más frecuentes (faq) sobre afs. En http://www.angelfire.com/hi/plutonic/afs-faq.html.

[19] R. Többicke. Distributed file systems: Focus on andrew file system/distributed file service (afs/dfs). *Thirteenth IEEE Symposium on Mass Storage Systems*, 1994.