DEP y *DIDS*: Sistemas para proveer Seguridad en Redes de Computadoras

C. Alaniz, R. Apolloni, H. Zalazar, G. Aguirre, F. Piccoli *
Departamento de Informática
Universidad Nacional de San Luis
Ejército de los Andes 950
5700 - San Luis
Argentina
e-mail: {mpiccoli}@unsl.edu.ar

Resumen

La incorporación y el uso masivo de las redes de computadoras en los distintos ámbitos de la vida, unido a los grandes avances de las tecnologías, hacen que la administración de una red no sea una tarea simple y menos aún su seguridad.

Tener redes seguras significa definir políticas de seguridad y tener herramientas capaces de detectar y prevenir distintos ataques. En este trabajo nosotros presentamos la motivación y una descripción de dos sistemas, cada uno de los cuales permite resolver uno de los dos ataques más frecuentes a los que están expuestas las redes de computadoras. *DEP* es un sistema que permite detectar y prevenir la exploración de los puertos de una computadora Linux en una red , y *DIDS* es un sistema de detección de intrusos a nivel de host, dinámico y adaptativo para redes Windows, construido a través de un sistema multiagente.

1. Introducción

Durante estos años hemos podido comprobar que las redes de computadoras facilitan el trabajo, la comunicación y la coordinación de diferentes ámbitos de desarrollo. Esto, unido a la expansión de Internet y al número de clientes potenciales que ofrece, hace que lo que eran redes de computadoras pequeñas y de fácil administración se transformen en redes extensas y complejas.

Hablar del hardware o del software de una red es remitirse a aspectos bien definidos, con normas que los rigen y fáciles de analizar, decidir e implementar[2],[13],[14]. Un aspecto importante y que con el correr de los tiempos está cobrando relevancia es la seguridad de los nodos conectados a las redes, en este caso la tarea no es simple, no existen normas o una herramientas válida que hacen segura todas las redes [12].

*Grupo subvencionado por la UNSL y ANPCYT (Agencia Nacional para la Promoción de la Ciencia y Tecnología)

Cuando nos referimos a seguridad en redes, debemos hablar en forma particular y circunscritos a una red especifica. Siempre para obtener una red segura, primero se debe considerar qué es lo que se debe proteger y de quien, luego definir la política de seguridad a aplicar y, finalmente implementar la red segura.

La seguridad de las redes de computadoras depende de la vulnerabilidad del software disponible y de los ataques que sufren, tanto internos como externos. Las vulnerabilidades son los caminos para realizar los ataques.

Como todas las vulnerabilidades no son conocidas, así como tampoco son conocidos los posibles ataques, estos últimos años se han desarrollado productos para detectar tanto las posibles vulnerabilidades de los sistemas y de los servicios de red, como los posibles ataques que se pueden perpetrar.

Si bien existen muchas formas de vulnerar y atacar una red de computadoras o a una computadora de ella, los dos ataque más comunes son la exploración de los puertos de una computadora perteneciente a la red en busca de servicios y la intromisión en una red o un nodo de la misma por parte de intrusos con el objetivo de hacer una mal uso de los sistemas de información a acceder.

2. Detección y Prevención de Exploración de Puertos en LINUX

Generalmente, un aspecto común considerado en la seguridad de la mayoría de las redes de computadoras es la restricción de los accesos no autorizados a la red de personas ajenas a la organización y cuyo único objetivo es dañar, husmear o sustraer información. Estos accesos se producen, principalmente, a través de los puertos, puertas de acceso a los servicios que brindan las computadoras a la red. Impedirlos o controlarlos es tarea del administrador de la red.

La seguridad de una red incluye varios aspectos, la presente propuesta tiene como objetivo desarrollar una herramienta que permita detectar la exploración de los distintos puertos de una computadora para el acceso externo y tratar de evitarlo, no sólo en el momento sino también en el futuro.

Contar con un sistema que detecte y prevenga la exploración de los puertos, proveerá a los administradores de redes de computadoras de una herramienta capaz de implementar un protocolo, el cual en base a la información obtenida en los intentos de acceso no autorizado, tomará decisiones y acciones en consecuencia.

Actualmente se está desarrollando una herramienta, *DEP*(**D**etección de **E**xploración de **P**uertos), con las características enunciadas anteriormente para redes LINUX[1], [5], [7], [11]. La figura 1 muestra la ubicación de *DEP* y su relación con los módulos encargados de atender y satisfacer los requerimientos de servicios.

Como puede observarse, todo requerimiento de servicio es captado por el sistema operativo, quien lo remite a *DEP* para su análisis. Éste analiza el mensaje recibido y el tipo de servicio solicitado consultando en la base de datos, *BD*, la historia de solicitudes y accesos de la dirección origen del requerimiento. Si de la información analizada, el requerimiento resulta no válido, automáticamente *DEP* actualiza el archivo de configuración *Servicios Denegados* y alarma al administrador de la red de un intento de ataque. Finalmente envía la solicitud de servicio al módulo de *Atención de Servicio*, quien, en base a la información brindada por los archivos de configuración *Servicios Habilitados* y *Servicios Denegados*, resuelve satisfacerlo o

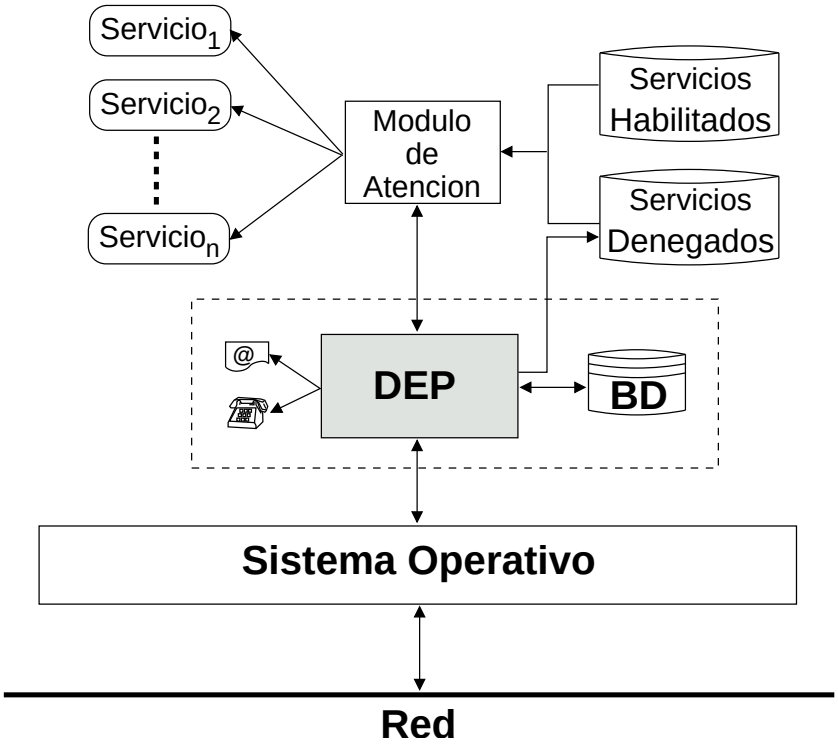

Figura 1: DEP: Ubicación y Relación con el Sistema Operativo y los Servicios

denegarlo[3].

3. Sistema de Detección de Intrusos

Un Sistema de Detección de Intrusos [9], *IDS*, es un sistema que intenta detectar y alertar sobre la existencia de intrusos intentando acceder o accediendo a un sistema o en una red. Se considera intidoruso a toda actividad no autorizada o que no debería ocurrir en el sistema.

Un IDS es un software que monitorea tanto el tráfico de una red, como los sistemas de una organización en busca de señales de intrusos. Algunas de las características deseables para un IDS son:

- Debe estar continuamente en ejecución con un mínimo de supervisión.
- Debe poder recuperarse de las posibles caídas o problemas con la red.
- Debe poderse analizar él mismo y detectar si ha sido modificado por un atacante.
- Debe utilizar los mínimos recursos posibles.
- Debe estar configurado acorde con la política de seguridad seguida por la organización.
- Debe adaptarse a los cambios de sistemas y usuarios y ser fácilmente actualizable.

Dependiendo de sus características, existe distintas clasificaciones de los IDS, según cual sea su función: Detección de Intrusos a nivel de Red o Detección de Intrusos a nivel de Nodos, según el tipo de detección: por mal uso o por uso anómalo, y según su naturaleza: Pasivos o Reactivos.

Las arquitecturas que implementan sistemas de detección de intrusos fueron modificándose y mejorando con el paso del tiempo y con la experiencia. Los primeros IDS eran herramientas de software rígidos, diseñados y realizados bajo la supervisión de un experto en seguridad de redes y basándose en la experiencia personal. Eran sistemas rígidos, dónde la actualización ante nuevos tipos de ataques requería verdaderos esfuerzos de análisis, programación y reconfiguración, eran un único programa que realizaba todo el trabajo, no se pensaba en sistemas distribuidos.

Las nuevas tendencias en el desarrollo de los IDS se basan fundamentalmente en dos principios básicos[4], [6], [8], [10]:

- La utilización de Agentes Autónomos, quienes recogen información por separado para luego analizar una parte de esta información ellos y la otra una entidad central coordinadora.
- Las arquitecturas basadas en la exploración de los datos en tiempo real.

En estos momentos se está trabajando en el desarrollo de un IDS dinámico, *DIDS*, mediante la utilización de agentes autónomos y un sistema multiagente para redes Windows. El objetivo final del trabajo es un sistema de detección de intrusos dinámico, adaptivo, capaz de detectar posibles ataques a un nodo en particular de la red (detección de intrusos a nivel de nodo) por mal uso o uso anómalo del nodo y reaccionar ante una actividad ilegal.

4. Conclusiones

Si bien existen varios trabajos realizados en esta temática, el desarrollo de los sistemas *DEP* y *DIDS* permitirán no sólo proveer a los administradores de redes Windows y Linux de herramientas capaces de detectar y reaccionar ante distintos ataques, sino también de analizar las características y vulnerabilidades de ambos sistemas operativos. También será posible analizar la portabilidad a otro sistema operativo de ambas herramientas y de las técnicas de computación utilizadas en cada caso.

Referencias

[1] Beck, M., Bohme, H., Dziadzka, M., Kunitz, U., Magnums, R., Verworner, D.. *Linux Kernel Internal* - Second Edition. Addison-Wesley - 1998 - ISBN: 0-201-33143.8

[2] Comer, D. E.. *Computer Networks and Internet* - Second Edition - Prentice Hall - 1999 - ISBN: 0-13-083617-6

[3] Comer, D. E.. *Internetworking with TCP/IP Principles, Protocols and Architecture*. Prentice Hall - ISBN: 0-13-468505-9.

[4] Crosbie, M., Spafford, G. - Active Defense of a Computer System using Autonomous Agents - Technical Report Nº 95-008. Purdue University. 1995

[5] Drake, J.. Linux Networking HOWTO. Commandprompt, Inc - 2000.

[6] Frank, J. - Artificial Intelligence and Intrusion Detection: Current and Future Directions. - Division of Computer Science. University of California.

[7] Glass, G. *UNIX For Programmers and Users A Complete Guide*. Prentice Hall - ISBN: 0-13-480880-0

[8] Koza, J. - Genetic Programming: On the Programming of Computers by means of Natural Selection. MIT Press. 1992.

[9] Kurmar, S., Spafford, G. - A Pattern Matching model for Misuse Instrusion Detection. Proceedings of the 17th National Computer Security Conference. October 1994.

[10] Maes, P. - Modeling Adaptive Autonomous Agents - Artificial Life, Vol 1, Nº 1 / 2. MIT Press. 1993.

[11] Matthew, N., Stones, R.. *Beginning Linux programming*. Primera edición. Wrox.

[12] Scambray, J. , McClure, S., Kurtz, G.. *HACKER: Secretos y soluciones para la Seguridad de Redes*. McGraw Hill. 2001.

[13] Stallings, W.. *Data and Computer Communications*. Fourth Edition. ISBN: 0-02-415441-5

[14] Tanenbaum, A. S.. *Computer Networks*. Fourth Edition, Prentice Hall - 2002 - ISBN: 0-13-066102-3.