Gestión y seguridad en puertos

Management and security in ports

Gustavo Adolfo Herazo Pérez[*]
Héctor Arturo Flórez Fernández[**]

Fecha de recepción: 10 de diciembre de 2008
Fecha de aceptación: 15 de marzo de 2009

Resumen

El presente artículo trata de visualizar los esquemas más relevantes y complejos que se presentan en la gestión de redes TCP/IP, su dimensionamiento en el protocolo de transporte TCP y las incidencias que conllevan a los problemas de intrusión y virus troyanos. Conocer los puntos vulnerables y cómo solucionarlos representan decisiones que a menudo se tienen que tomar para fortalecer los perímetros de seguridad informática. Actualmente, las grandes compañías de este país tienen como prioridad establecer modelos de ingeniería social y de gestión de seguridad, aplicados a control de puertos y servicios de red, como solución a la detección y control de intrusos internos y externos en una red de información. Sin embargo, los patrones de seguridad que conllevan a estructurar valores de control en los canales de ancho de banda para las redes emergentes están dando un giro vertiginoso que involucra diversas pruebas de penetración, específicamente con el protocolo TCP, para tener una visión clara de los alcances y protección en la cual una red se considera vulnerable.

[*] Ingeniero de sistemas de la Universidad Autónoma de Colombia, especialista en Sistemas Gerenciales de la Pontificia Universidad Javeriana, especialista en Telecomunicaciones Móviles de la Universidad Distrital Francisco José de Caldas, magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Docente Investigador Fundación Universitaria Konrad Lorenz, docente Universidad Autónoma de Colombia. Correo electrónico: gustavoherazo@hotmail.com.

[**] Ingeniero electrónico de la Universidad El Bosque, ingeniero de Sistemas de la Universidad El Bosque, especialista en Alta Gerencia de la Universidad Militar Nueva Granada, magíster en Ciencias de la Información y las Comunicaciones de la Universidad Distrital Francisco José de Caldas, candidato a magíster en Gestion de Organizaciones de la Universidad Militar Nueva Granada. Docente investigador Fundación Universitaria Konrad Lorenz, docente Universidad Distrital Francisco José de Caldas. Correo electrónico: hectorarturo@yahoo.com.

Palabras clave: TCP (Protocolo de Control de Transmisión), IP (Protocolo Internet), UDP (protocolo de datagrama de usuario), ACL (lista de control de acceso), firewall (cortafuegos), SOCKET (puerto asociado al servicio), TRACE (trazado de rutas), ICMP (protocolo de control de mensajes de Internet).

Abstract

The present paper tries to visualize the most excellent and complex schemes than appear in the management of networks TCP/IP, their sizing in the transport protocol TCP and the incidences with the problems about viruses and Trojans intrusion.

To know the soft spots and as to solve, represent them decisions that often must take to fortify the perimeters of computer science security. At the moment the great companies of this country, must like priority establish models of social engineering and management of security applied to control of ports and services of network, like solution to the detection and control of internal and external intruders in an alert network. However the security patterns who entail to structure values of control in the channels of bandwidth for the emergent networks are giving a vertiginous turn that specifically involves diverse tests of penetration with protocol TCP, to have a clear vision of the reaches and protection in which a network is considered vulnerable.

Key words: TCP (Transport Control Protocol), IP (Internet Protocol), UDP (User Datagram Protocol), ACL (Access Control List), firewall (control of security), SOCKET (port between of services), TRACE (trace route), ICMP (Internet Control Message Protocol).

Introducción

EL monitoreo de redes en conjunto con la seguridad informática forman uno de los elementos primordiales en la gestión de redes convergentes del siglo XXI. Las empresas comienzan a valorar la verdadera conciencia de promover la gestión en las redes de telecomunicaciones. Hoy en día, tener un sistema que cumpla con los estándares de gestión de la seguridad es sinónimo de calidad de servicio.

Actualmente, nuestra era informática se ve acorralada por cientos de virus, gusanos y troyanos y se toma conciencia del peligro

que nos acecha como usuarios de PC, servidores y cualquier otro elemento de red que se encuentre conectado a Internet. Adicionalmente, comienzan a proliferar diversos ataques a sistemas informáticos. La palabra hacker aparece incluso en prensa.

En nuestra era actual, los acontecimientos fuerzan a que se tome muy en serio la seguridad informática, como pilar de investigación y desarrollo.

Tipos de seguridad

Dentro de los lineamientos de seguridad informática, algunos proyectos de I+D forman su eje dentro de los estándares de seguridad física y otros se aplican a la seguridad lógica de los sistemas de información.

La seguridad física analiza los controles que se pueden asociar a la protección de los sistemas ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas, etc.

La seguridad lógica comprende la protección de la información en su propio ámbito, mediante el enmascaramiento de ésta usando técnicas de criptografía.

Puntos vulnerables

Las nuevas empresas que se relacionan con las emergentes Tecnologías de la Información y Comunicación hacen uso de diversas técnicas y herramientas de redes para el intercambio de datos como son: la transferencia de archivos vía ftp, la transferencia de datos e información a través de Internet por el servicio de red http y las conexiones remotas a máquinas y servidores a través de telnet; todo lo anterior representa los protocolos de mayor riesgo a la hora de transmitir información y ante esto se derivan algunos entes que entran en el panorama de control de riesgo de los puertos que son controlados por los diversos sistemas operativos de redes.

Actualmente, un computador con sistema operativo Windows XP instalado tiene riesgo de infectarse por un virus en menos de 10 minutos de estar en línea, si no decide activar su firewall nativo de su sistema operativo. Esto conlleva a pensar en la necesidad primordial de conocer sus riesgos y, más aún, tener un control detallado de sus puertos y estar consciente de la importancia de descargar información de la Web, con un alto nivel de seguridad. Para 2006, tres amenazas conforman los pilares de los mayores ataques para provocar ingreso de virus, gusanos y troyanos.

Cabe mencionar la importancia que regula los sistemas operativos como la familia unix (Linux, HP-UxX, AIX y otros), que desagregan su sistema de protección de puertos, con base en su sistema jerárquico de privilegios, opción por la cual se está trabajando fuertemente la versión Windows Vista, para obtener este mismo esquema de seguridad y el control total de puertos, sin ningún problema.

El control de puertos en Web

El control de puertos abiertos en entorno Web es mucho más peligroso. Fácilmente un enlace puede lanzar un programa que se ejecute en el cliente e infecte la máquina, dejándola abierta para otros ataques o bien dejarla como un zombie que colabore en la ejecución de otros ataques.

El punto más vulnerable es la constante transmisión por el puerto http (8080) de Internet que representa siempre una puerta abierta a los intrusos. Ante esto equivale la política del bloqueo de algunos servicios de red de la maquina origen, permitiendo sólo el control de aquellos que son absolutamente necesarios.

Prevención de ataques por intrusos

De acuerdo con los estándares internacionales, los troyanos casi siempre están relacionados en su desarrollo e implantación a familias genéricas que van asociadas a determinados puertos de red (Sockets) con conexiones TCP o UDP.

El monitoreo de puertos basados en los servicios http, ftp, telnet y smtp, representan las instancias más vulnerables que utilizan los intrusos en la apertura de puertos restringidos para lograr su objetivo. Por esta razón, a través del monitoreo de puertos constante, estamos restringiendo que éstos protocolos de transmisión de datos no se conviertan en una puerta trasera a la invasión de intrusos.

Se hace necesario que protocolos como Telnet y FTP, aparte de utilizar su propias técnicas de transporte seguro, se haga necesario que se decodifiquen los datos de salida y entrada a la redes con formatos seguros como ASCII o binario.

El principio de menor privilegio dice que cada proceso que realice alguna acción debe tener la menor cantidad posible de privilegios exigidos para realizar las tareas dadas. La aplicación de este principio ayuda, en gran medida, a mitigar la amenaza de intrusos. Las versiones posteriores de Windows 2000 basadas en NT ofrecen un servicio que ayuda a alternar entre contextos privilegiados y no privilegiados y para ello se cuenta con el servicio secundario de acceso (SLS).

El problema de TCP frente al escaneo de puertos

En el proceso de transferencia de datos por puertos TCP, se generan una serie de mecanismos que determinan la inestable fiabilidad y robustez del protocolo. Entre ellos, está incluido el uso del número de secuencia para ordenar los segmentos TCP recibidos y detectar paquetes duplicados, *checksums* para detectar errores y temporizadores para detectar pérdidas y retrasos. En este proceso, los temporizadores generan un tiempo en milisegundos que determina el estado de la ventana deslizante cuando se cierra y nuevamente se abre. Este tiempo forma parte de un timeout que permitirá que hackers inhabiliten un puerto determinado de conexión de la red.

Si se trata de escanear en este tiempo *timeout*, posiblemente la respuesta sería que el sockets presenta un estado cerrado y sin ningún intruso en la red; desafortunadamente, los principios de la ventana deslizante del protocolo de la versión 4, tiene este inconveniente y aunque se trata de unos solos milisegundos, representa de todos modos un riesgo en el estado del puerto.

Durante el establecimiento de conexión TCP, los números iniciales de secuencia son intercambiados entre las dos entidades TCP, hecho que resulta bastante riesgoso en entornos Internet. Estos números de secuencia son usados para identificar los datos dentro del flujo de bytes, y poder identificar y contar los bytes de los datos de la aplicación o la página en curso

Dimensionamiento de puertos TCP para control de intrusos

El protocolo orientado a conexión TCP usa los números de puerto para identificar las aplicaciones emisoras y receptoras en una red. Cada lado de la conexión TCP tiene asociado un número de puerto (de 16 bits sin signo, con lo que existen 65536 puertos posibles) asignado por la aplicación emisora o receptora.

Estos puertos se dividen en tres grupos:

- Conocidos, asigandos por la Internet Assigned Numbers Authority y están en el rango de 0 a 1023. Son los puertos que involucran el sistema y los procesos privilegiados, Se caracterizan porque siempre están en "escucha". Normalmente, son servidores de redes y su monitoreo resulta casi obligatorio, ya que siempre están a la espera de recibir conexiones de otros usuarios. Entre ellos se destacan los protocolos de mayor riesgo en su control de puertos (ftp, telnet, ssh, smtp y http).
- Registrados, son utilizados por aplicaciones de aquellos usuarios de manera temporal cuando se producen las conexiones a los servidores Web.
- Dinámicos/privados: son los menos usados en las comunicaciones y su función se da a la espera de aquellos puertos que se consideran necesarios para máquinas virtuales.

Resultados del proyecto de investigación al control de puertos y transferencias seguras a través del protocolo FTP

Las exploraciones ping son casi siempre la primera indicación de un ataque o emisión de una petición de eco ICMP o UDP, es una forma de preguntar "¿estás ahí?". En este proyecto atizamos estas rutinas como medios de análisis de vulnerabilidad, dándonos un mapa de qué sistemas están conectados y responden. Normalmente, un bloqueo implica que una ACL (Access Control List) de un firewall o enrutador de frontera los está bloqueando. Si sabemos que una computadora tiene un servicio, como un servicio Web, por ejemplo, que rehúsa responder a un ping, podemos estar casi seguros de que existe algún tipo de refuerzo de la seguridad.

El trazado de rutas (*traceroute*) es otra herramienta de nuestro proyecto de investigación, para establecer pruebas de penetración que validen el análisis de rutas a través de los diferentes elementos de red, por el cual hace el trazado de rutas. Es una herramienta administrativa que nos da información sobre un sitio interno o externo en la red. Traceroute nos da una estimación aproximada de dónde va nuestro tráfico y da información interesante, como quién es uno de los proveedores de red de nuestro objetivo.

Por último, permitir que el proyecto de investigación tenga el control de puertos, es una tarea no tan fácil, para aquella persona que no tenga la suficiente experiencia en su conceptualización y fines pertinentes. Por ello, daremos a conocer cuáles serían las instancias clave en la administración de este tipo de controles.

- Determinar el nivel de importancia en la categorización de los servicios de red.
- Si se utiliza IIS (Internet Información Services), definir para el control de puertos, zona de militarización y dominios de grupo.
- Siempre al aplicar políticas de seguridad, para el puerto 21, codificar las transferencias en binario o ASCII, para obtener niveles de privilegios en seguridad, como los manejan los sistemas unix.

No olvidemos que dentro de las políticas de parametrización del proyecto de investigación se tienen que por norma internacional los puertos del 0 al 1024 quedan reservados para tareas, servicios y sistemas propios de la pila TCP/IP.

Conclusiones

Con base en la información suministrada en este documento se espera proporcionar nuevos conocimientos sobre el monitoreo de puertos y gestión de red y su importancia en los horizontes de la seguridad informáti-

ca. Las pruebas de penetración y de gestión a los puertos son algo a lo que no se debe temer y recalcar su nivel de importancia dentro de las organizaciones. Si se realiza gestión de monitoreo de puertos tenemos la posibilidad de cerrar muchos agujeros antes de que se vuelvan amenazas serias para la seguridad de nuestra red.

Las modalidades de gestión de servicios del proyecto de investigación ayudan a la prevención de los ataques, lo que permite escoger y parametrizar cada uno de los puertos, su incidencia en la red y los usuarios responsables del control de éstos. Cada uno de estos servicios, sin importar si son controlados por IIS, actúa como controlador de sockets, a bajo nivel, para que el administrador permita el bloqueo o activación de éste en cualquiera de los puntos de la subred.

Si se cuenta con un firewall, el aplicativo servirá de refuerzo, como barrera adicional al perímetro de seguridad informática, permitiendo filtrar las conexiones y las transferencias de ficheros entre cada uno de los puntos de nuestra red.

Referencias bibliográficas

[1] A. Barba Marti. *Gestión de Red*. Editorial Alfaomega.
[2] *Esquemas de Seguridad en Windows*. Editorial Prentice Hall.
[3] M.J. Palmer. *Una guía práctica. Redes de computadores*. Editorial Thompson Learning.
[4] J.M. Huidobro. *Fundamentos de telecomunicaciones*. Thomson Learning-Paraninfo.
[5] D. Roldán. *Comunicaciones TCP/IP*. Alfaomega RA-MA Grupo Editores.
[6] K. Adam. *Administración de información en Internet. Guía avanzada*. Prentice Hall.
[7] A.L. García. *Redes de comunicación- conceptos fundamentales y arquitecturas*. McGraw Hill.
[8] J. Schmidt. *Seguridad en Microsft Windows 2000- Guía avanzada*. Prentice Hall.