20. Seguridad en Redes.

20.1. Niveles de seguridad:

Para poder determinar el grado de seguridad de una red, se impuso la clasificación propuesta por el Departamento de Defensa de los Estados Unidos de Norte América, acorde a la especificaciones que hace referencia en su "Libro Naranja", estos niveles imponen los límites y condiciones que debe reunir un sistema completo para alcanzar un esquema determinado de seguridad tanto en Hardware, Software o Datos. Los niveles son D, C, B y A, de menor a mayor seguridad, teniendo a su vez algunas subdivisiones que se detallan brevemente a continuación:

20.1.1. Nivel D1:

Este constituye la seguridad más básica, sus características esenciales son:

- No existe protección del Hardware.
- El sistema operativo es fácilmente vulnerable.
- Los usuarios no poseen autenticación de red, ni derechos.
- Ej: MS-DOS, Windows (3.x, 95 y 98), Apple, etc.

20.1.2. Nivel C1:

Este subnivel es llamado nivel de seguridad discrecional, es característico de un sistema operativo tipo UNIX en su implementación básica, sus características principales son:

- Existe algún nivel de protección para el Hardware.
- Los usuarios deberán registrarse en el sistema por medio de nombre y contraseña, y por medio de estos tendrá los derechos de acceso.
- La cuenta de Administrador del sistema no posee ninguna restricción.

20.1.3. Nivel C2:

Incluye algunas características adicionales de seguridad, como son:

- Refuerza las restricciones de los usuarios en la ejecución de algunos comandos de acceso.
- Permite especificar niveles de acceso a los archivos y/o recursos.
- Requiere auditorías del sistema con la creación de sus registros correspondientes.
- Windows NT fue reconocido para alcanzar este nivel.

20.1.4. Nivel B1:

Este es el primero de esta clase, también llamado Protección de Seguridad Etiquetada, sus características son:

- Reconoce seguridad multinivel: Confidencial, secreta, ultrasecreta, etc.
- Trabaja bajo el control de acceso a "Objetos", cuyos cambios si se desea sólo pueden ser realizados por su dueño.

20.1.5. Nivel B2:

Este nivel es conocido también como Protección Estructurada, sus características son:

- Cada objeto debe encontrarse etiquetado, acorde a la protección necesaria.
- Cada dispositivo podrá tener un nivel de seguridad sencillo o múltiple.
- Establece las pautas de comunicación de un Objeto de nivel más elevado de seguridad con otro de nivel inferior.

20.1.6. Nivel B3:

También llamado nivel de Dominios de Seguridad, sus características son:

- Impone Hardware de seguridad.
- Establecimiento de rutas seguras en toda comunicación de usuario.

20.1.7. Nivel A:

También llamado Nivel de Diseño Verificado, es el más alto de seguridad, sus característica son:

- Niveles de diseño, control y verificación de Hardware y Software.
- Exige Distribución Confiable de Hardware y Software, es decir desde el fabricante hasta su destino final deberá contar con la seguridad exigida.
- Los diseños deberán verificarse en forma matemática.

20.2. Intrusos:

Si bien no es la única responsable, es sin duda Internet con su crecimiento exponencial, y a través de sus bajos costos la responsable de fomentar a muchas personas que poseen tiempo libre, otras por investigación, por diversión, por desafío personal, por tareas de inteligencia o simplemente por robo, a navegar a través de la red obteniendo información de los millones de personas que la emplean con otros fines. Una vez obtenida bastante información podrán seguir o no con otros pasos en sus tareas.

Como se puede apreciar, no todas estas personas tienen malas intenciones, y la realidad es que quizás sean las menos, pues muchas de estas son justamente las precursoras de las medidas de seguridad y quienes descubren las vulnerabilidades de los distintos sistemas, para que esta gran red mundial puede seguir creciendo día a día.

El gran peligro está en que la masa de la información de las fallas de seguridad descubiertas es de dominio público, y se puede encontrar en varios sitios de Internet, como así también todo tipo de programas para poder vulnerar las medidas de seguridad de una red.

Y lo que ya es casi catastrófico es que la gran mayoría de los administradores de las grandes redes, poseen mucho menos tiempo de dedicación para actualizarse que cualquier persona que como se dijo al principio POSEE TIEMPO LIBRE. Aquí tal vez radica el problema más crítico de seguridad: **"La Carrera de la Vulnerabilidad"**. En la carrera armamentista todo tipo de arma por más secreta que sea es eficiente en tanto y en cuanto no pueda ser neutralizada, y este fenómeno se repite a lo largo de la historia en todas las grandes potencias. Una red o un sistema es seguro en tanto y en cuanto no se descubra la forma de acceder a este sin autorización, y de suceder (Hecho no alarmante), es el **Administrador el primero que debería enterarse cómo sucedió**, y todos los propietarios de sistemas similares para poder contrarrestarlo.

Al estudiar las distintas redes de magnitud considerable y de importancia en el manejo de información clasificada se refuerza más la teoría de los tiempos, pues la experiencia demuestra fehacientemente que todo elemento dedicado exclusivamente a la investigación, análisis e

implementación de medidas de seguridad en una Empresa, a lo largo del tiempo termina desvirtuándose de sus tareas fundamentales para dedicar gran parte de su tiempo a otras.
Tengamos en cuenta que un INTRUSO dedica todo o la masa de su tiempo a nuestra red, pues es esta su actividad, y casi con seguridad está al tanto de las últimas novedades encontradas en Internet.
La mejor comparación (Sin ofender a "los buenos") es el caso inverso que plantea una prisión; todo el personal de seguridad día a día analiza el problema de seguridad global, es más, se nutre de los desarrollos realizados en otras entidades similares de todo el mundo, pero dentro de cada una de ellas existen muchas personas que les SOBRA TIEMPO y que observan no lo global, sino el detalle fino, esas muy pequeñas cosas que se pueden llegar a pasar por alto, a esto le dedican todo su tiempo pues vulnerarlas es su desafío, y tarde o temprano lo logran.

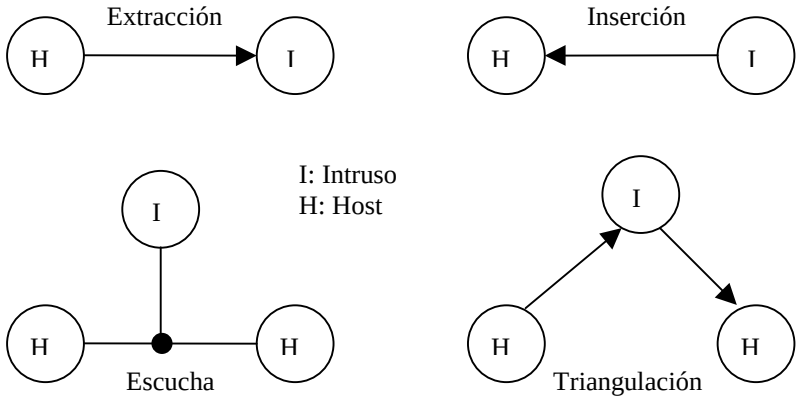
En general las razones por las que un intruso desea ingresar a un sistema son las siguientes:

- Por Diversión.
- Para mirar o investigar.
- Para robar.
- Para alterar información.
- Por desafío personal.

Uno de los primeros desafíos de un intruso una vez que ha logrado penetrar en una red es obtener las listas de usuarios y contraseñas, los cuales si bien suelen estar criptografiadas, al obtenerse una copia de estas es sólo cuestión de tiempo el resolverlas. En general se suelen utilizar programas "buscadores" que en virtud del diccionario que posean y la velocidad de la CPU empleada, demoran más o menos en realizar esta tarea. La gran ventaja es que estos tiempos no suelen ser lo breves que se desean siempre y cuando la estrategia de contraseñas está bien implementada.

20.2.1. Actividades generadas por intrusos:

20.2.1.1. Modos de operación:



20.2.1.2. Problemas que pueden ocasionar:

- Destrucción de Software y datos.
- Extracción de información.
- Análisis pasivo de tráfico.
- Generación de tráfico, ocasionando baja performance o paralización de la red.

- Negación de servicios o recursos.
- Inserción de virus.
- Modificación de información.
- Modificación de rutas.

20.3. Sistema de autenticación Kerberos:

Este sistema nace en el Instituto Tecnológico de Massachusetts y su nombre se remonta a la mitología Griega donde así se denominaba el perro guardián de los Dioses. Este sistema de autenticación hoy es soportado por la masa de los sistemas operativos y componentes de red.
El sistema Kerberos está basado en un "Servidor despachador de boletos", al cual se encarga de validar la identidad de los "Principales" los cuales pueden ser:

- Usuarios.
- Servicios.

En cualquiera de los dos casos, un "Principal" queda definido por un "Trío" cuyos componentes son:

- Nombre primario: Nombre de persona o servicio.
- Instancia: Para usuarios es nula o contiene información de ésta. Para un servicio es el nombre de la máquina
- Reino: Define distintos Dominios de autenticación.

Si un "Principal" obtiene un boleto, este tendrá un tiempo de vida limitado por el Servidor, y a partir de este poseerá una clave privada que sólo conocerán el Principal y el Servidor, por lo tanto será considerada auténtica y a través de esta podrá acceder a los recursos del sistema.

20.4. Política de seguridad:

Dentro de las actividades de planeamiento e implementación de una red, en virtud de la importancia relativa de la información que se maneje, una de las actividades más importantes es la implementación de una Política de Seguridad, la que definirá las acciones de administradores y usuarios para resguardar la información. Un detalle muy significativo es que este resguardo es tenido en cuenta tanto para INTRUSOS como para PERDIDA de información causada por cualquier factor, lo que realmente **suma dos de los riesgos más grandes que sufre un Administrador de red**.
La política de seguridad de un "Sitio" está bastante tratada en la RFC 1244.

El hecho determinante de esta política pasa por la relación Costo/Beneficio entre lo que se desea resguardar y cuánto se invertirá para esto. Un mal balance llevará al fracaso por uno u otro motivo, por eso para iniciar con la misma es sumamente importante plantearse determinados interrogantes básicos como:

- ¿Cuáles recursos hay que proteger, cuáles no y cuántos niveles de protección se desean?
- ¿Cuál es el peligro real de amenazas?
- ¿Cuáles son las personas de las cuales necesita protegerse?
- ¿Cuál es la importancia de cada recurso?
- ¿Qué capital se dispone exclusivamente para seguridad?
- ¿ Qué personal se cuenta para esta actividad?

- ¿ Qué nivel de capacitación posee el personal o se le puede brindar?
- ¿ Que topología, accesos, hardware y protocolos se emplean?
- ¿ Qué horarios se disponen para esta actividad?
- ¿ Se posee soporte técnico o fuentes de consulta?

Al resolver estos cuestionamientos automáticamente irá surgiendo documentación sobre la cual existe buena base en la RFC 1244, pero lo que se considera realmente importante es la flexibilidad y dinamismo con que debe ser llevada cotidianamente, pues día a día irá cambiando haciendo que lo que hoy sea seguro, mañana ya no. Es más **es casi una regla que una carpeta de seguridad que no evoluciona permanentemente NO SIRVE**, pues es altamente probable que ya esté desactualizada.
Una vez definida la política a seguir, se deberá confeccionar una guía de seguridad que basada en esta política, permita a cada usuario entender en detalle cuáles son sus obligaciones y derechos. Es de suma importancia aclarar estrictamente lo que está permitido y lo que está prohibido, y sobre este detalle es para tener en cuenta el concepto de VANDALISMO DE USUARIO; muchas Empresas admiten y fomentan (y hasta a veces premian) entre sus miembros la investigación de las debilidades de sus sistemas pues es sumamente positivo que las mismas sean descubiertas tempranamente y por personal propio y no por extraños. Este último punto si bien es muy tentador debe ser tratado con cuidado pues también puede generar serios inconvenientes.
Esta guía deberá ser controlada en su cumplimiento y distribuida en cada actualización, pues un solo usuario que no respete las medidas debilita toda la estructura.

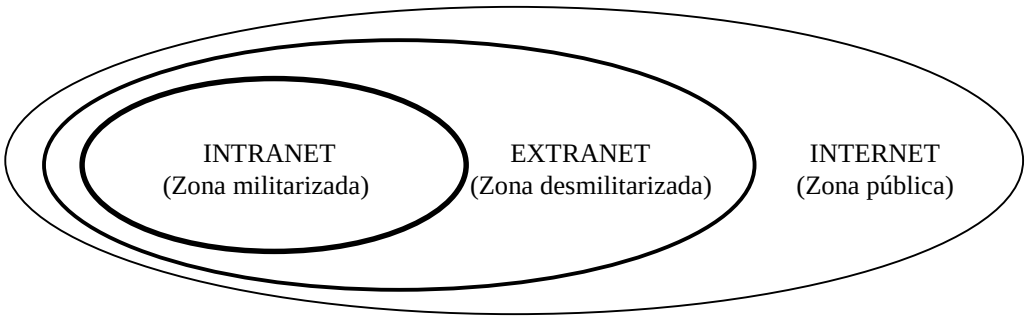
20.5. Zonas:

En el caso de establecer un sistema que opere en los tres tipos de red actuales:

- Intranet: Red propia bajo todo el potencial del protocolo TCP/IP.
- Extranet: mismo potencial pero con acceso a usuarios “Conocidos” como ser clientes, socios, Empresas afines, proveedores, etc.
- Internet: Ya conocido.

Se debería establecer por lo menos tres zonas, en este texto se las tratará como:

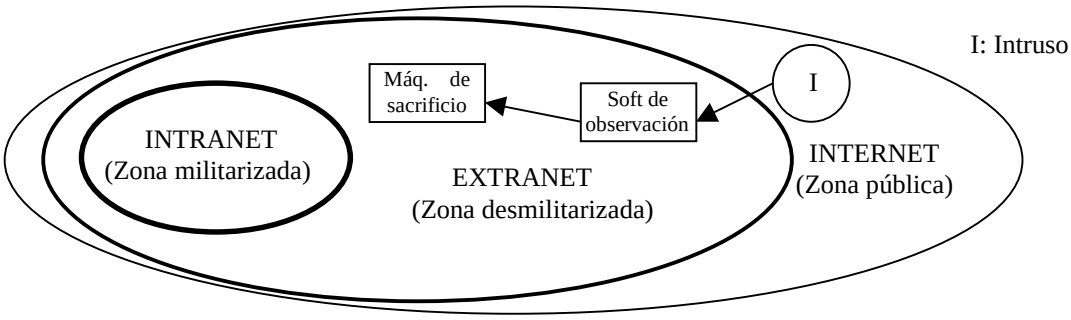
- Zona militarizada: Máxima seguridad, sólo ingresarán los usuarios de Intranet.
- Zona desmilitarizada: Nivel intermedio de seguridad, accederán también los usuarios de Extranet.
- Zona pública: Sin medidas de seguridad, en este esquema lo representa todo Internet.



En este sistema es un buen hábito realizar **"medidas de engaño"** (muy utilizadas en la guerra, y téngase en cuenta que en esto hay muchas similitudes). Si se es realmente consciente que lo que se debe proteger con máximo esfuerzo está seguramente en la Intranet, entonces el razonamiento que se desprende por lógica es que entonces **¡hay ciertas medidas de seguridad en la Extranet que no se cumplen¡** (Sigan con mucha atención este razonamiento), un principio básico es que jamás se debe subestimar al enemigo, que en este caso son los INTRUSOS, por lo tanto no deben caber dudas que aquel que realmente sepa penetrar a una red, a la Extranet es casi seguro que logrará hacerlo. Este es un planteo realista y una buena posición para enfrentar las zonas, por lo tanto todo el sistema que funcione dentro de este ámbito es saludable desarrollarlo con dos medidas:

- Ninguna información crítica puede estar aquí.
- Crear medidas de engaño.

La primer medida es sumamente clara. La segunda en general se implementa por medio de las llamadas "Máquinas de sacrificio", a través de las cuales mediante un Software de observación, se trata de determinar la posibilidad de accesos de intrusos, los cuales se los rutea hacia éstas, en las cuales se almacena información ficticia, cuyo secreto es que parezca ser absolutamente cierta, dando la impresión al intruso que logro llegar al corazón de todo el sistema (Muchos de los casos famosos fueron de este tipo, a los cuales por supuesto las víctimas no dieron a luz la verdad pues renovarían con creces los ataques)



20.6. Criptografía:

Si bien un canal de comunicaciones en línea o fuera de línea se puede considerar seguro si se respetan ciertas medidas, los datos altamente críticos o muy secretos no es común que se transmitan igual que cualquier otro. El proceso de transformar información a otro formato cuya única interpretación pueda ser realizada revirtiendo el proceso a través de uno o varios parámetros (generalmente conocidos como clave), se llama criptografía. Esta actividad se puede emplear también para el almacenamiento de datos.
La criptografía se corresponde con el nivel seis del modelo OSI, pues justamente opera sobre la semántica (significado) de los símbolos, y se puede implementar por medio de Hardware a través de dispositivos especiales o placas de PC, o a través de Software propietario y también gratuito de amplia difusión en Internet.

20.6.1. DES (Date Encriptation Standard):

Como su nombre lo indica este es un estándar generalizado del cual existen varias implementaciones en Soft y Hard, que emplea los conceptos de clave pública y privada para este proceso.

20.6.2. Crypt:

Este es un comando que se encuentra disponible en el sistema operativo UNIX, basado en un algoritmo desarrollado para encriptar datos en la segunda guerra mundial, el cual en la actualidad no es de los más seguros.

20.7. Actualización:

Como se mencionó dentro de las políticas de red, es imprescindible estar permanentemente al tanto de las novedades descubiertas en tema de seguridad pues es altamente probable que alguna de ellas afecte a la red propia. Para esta actividad lo más importante, y es el factor excluyente de tener o no tener una red segura, es **contar con PERSONAL DEDICADO CON EXCLUSIVIDAD A LA INVESTIGACION**. Sin tener esto se aconseja no perder tiempo, ni creerse que se pueden implementar medidas para asegurar recursos críticos.
Si se cuenta con esta invalorable ventaja, puede recurrir a muchos sitios dónde recabar información, como son:

20.7.1. Listas de correo:

El concepto de listas de correo es el de corresponsales que acuerdan agruparse para recibir en forma generalizada los mail que envíe cada uno de ellos, en general son sobre temas específicos, pero no necesariamente es así.

Los postulantes a una de ellas, solicitan su inclusión a la dirección que regula la lista, que desde ya no es la de la lista en sí, sino recibirían todos los integrantes del grupo cada nueva petición. Una vez incorporado a esta, se comenzará a recibir toda la información que cada miembro genere a través del correo electrónico dirigida a la lista, y se enviará a todos lo que éste decida remitir.
Un tema interesante es que existen listas:

- Moderadas: Uno o varios miembros actúan como moderadores, filtrando la información de interés de la que no lo tiene.
- Sin moderación: Se recibe la totalidad de la información generada.

Un ejemplo de estas listas es la que trata el tema de seguridad en UNIX cuya suscripción se realiza por correo electrónico ante:

Security-request@cpd.com

Otro ejemplo es la lista del foro de riesgos, la cual es una lista moderada que realiza análisis de riesgo y también aspectos de seguridad de carácter particular e internacional, su dirección es:

Risks-request@csl.sri.com

Si está interesado en el tema virus una buena opción es:

Listserv@lehiibm1.bitnet

Por fallas, bugs o lagunas de seguridad un lugar a recurrir es la lista Bugtraq que justamente discute estos temas, su dirección es:

Bugtraq-request@crimelab.com

Para investigar herramientas y técnicas de seguridad, existe la lista CERT-TOOLS, cuya dirección es:

Cert-tools-request@cert.sei.cmu.edu

Si el tema es TCP/IP otra opción es:

Tcp-ip-request@nisc.sri.com

20.7.2. Grupos de noticias:

Los grupos de noticias también permiten formar núcleos de discusión, pero se diferencian de las listas en que se emplean programas especiales que permiten intercambiar información en forma más dinámica, estos programas existen de varios tipos, tanto gratuitos como comerciales. De la misma forma que las listas de correo estos pueden ser moderados e inmoderados, y algunos de los relacionados con seguridad son:

- misc.security
- alt.security
- comp.security.announce

20.7.3. Equipo de respuestas de emergencia de la computadora (CERT):

Para el estudio de la seguridad en Internet, la Agencia de Investigación de Proyectos Avanzados para la Defensa (DARPA) de EEUU, creó este equipo con capacidad para conferenciar con expertos y dar respuestas en breves intervalos de tiempo, la operación efectiva del mismo es llevada a cabo por la Universidad de Carnegie Mellon.
Este centro proporciona apoyo a usuarios que lo requieran, el cual puede ser telefónicamente (1-412-268-7090), o a través de la lista:

Cert-request@cert.sei.cmu.edu

O a través del grupo de noticias USENET:

Comp.security.announce

También se accede vía FTP anónimo al servidor:

Cert.sei.cmu.edu

20.7.4. Instituto Nacional de Estándares y Tecnología (NIST):

Este instituto de EEUU, independientemente de lo relacionado a estándares, también posee un centro de investigación de computación, dentro del cual existe el Centro de Respuesta y Recursos de Seguridad de Computadoras (CSRC), el cual se aboca a problemas relacionados con seguridad, su línea telefónica es: 1-301-975-5200, en la cual opera las 24 horas.
Mediante FTP se accede al servidor:

Csrc.ncsi.nist.gov

20.7.5. Páginas Web:

http://escert.upc.es (Barcelona, España)

http://www.rediris.es/cert/ (España)

http://www.mxcert.org.mx (Méjico)

http://www.cert.org (EEUU)

http://first.org (Mundial)

http://www.cert.dfn.de/eng/csir/europe/certs.html (Europeo)

http://www.arcert.gov.ar/ (Argentina)

ftp://ftp.auscert.org.au (Australia)

http://www.netcraft.co.uk/security/diary.html
Muy útil para ponerse al día con los últimos problemas encontrados en la red, especialmente si se ha estado unos días desconectado.

http://www.rootshell.com
"La casa de los exploits"

http://www.hispasec.com
Un nuevo web dedicado a noticias acerca de seguridad informática en castellano

http://www.trinux.org
Una distribución de Linux en disquete. Pensado para cuando se necesita disponer de una máquina Unix con programas de seguridad y no hay ninguna a mano.

http://www.cs.purdue.edu/coast
Casa del laboratorio COAST de la Universidad de Purdue.

http://www.cisco.com

http://www.core-sdi.com/Core-SDI/spanish/FreeSoft.html

http://www.alw.nih.gov/Security/fist-papers.html

http://www.underground.org

http://www.rootshell.com - (exploits)

http://csrc.nist.gov

http:/in-contact.com/internet/seguridad

http://www.core-sdi.com/Core-SDI/spanish/FreeSoft.html (Casa del Secure Logger).

http://iss.net (Internet Security System).

http://dixguard.com.

http:/moon.inf.uji.es

20.8.Firewall.

Un Firewall es un sistema de defensa ubicado entre la red que se desea asegurar y el exterior, por lo tanto todo el tráfico de entrada o salida debe pasar obligatoriamente por esta barrera de seguridad que debe ser capaz de autorizar, denegar, y tomar nota de aquello que ocurre en la red.

Aunque hay programas que se venden bajo la denominación de Firewall, un Firewall NO es un programa. Un Firewall consiste en un conjunto de medidas HARDWARE y SOFTWARE destinadas a asegurar una instalación de red.

Un Firewall **actúa en los niveles 3 (red) a 7 (aplicación) de OSI**. Sus funciones son básicamente las siguientes:

* Llevar *contabilidad* de las transacciones realizadas en la red.

* *Filtrar accesos* no autorizados a máquinas (mediante filtrado de paquetes, o bien observando el contenido de las unidades de protocolo de Transporte, Sesión, Presentación, y aplicación).

* *Alertar* en caso de ataques o comportamiento extraño de los sistemas de comunicación.

¿ Qué tipos de Firewall existen ?

Cualquier Firewall puede clasificarse dentro de uno de los tipos siguientes (o como una combinación de los mismos):

* *Filtros (Packet Filters).*

Su cometido consiste en filtrar paquetes dejando pasar por el tamiz únicamente cierto tipo de tráfico. Estos filtros pueden implementarse a partir de router (p.ej: en un Cisco, podemos definir access-lists asociadas a cada uno de los interfaces de red disponible, por esta razón no se trató con anterioridad este tema, y se tratará en detalle en 6.4. Otras medidas, pues justamente puede abarcar varios niveles).

Problemas: No son capaces de discernir si el paquete cuya entrada se permite incluye algún tipo de datos “maliciosos". Además, cualquier tipo de paquetes no permitidos puede viajar en el interior de tráfico permitido (ej: IP sobre IP). Desgraciadamente son difíciles de definir y depurar.

* *Proxy (Circuit Gateways)*

En este caso la pasarela actúa del mismo modo que un simple cable (vía software) conectando nuestra red interna con el exterior. En general se requiere que el usuario esté autorizado para acceder al exterior o interior y que tenga una cuenta de salida en el Proxy . En general hoy se suele emplear el Servidor Proxy independientemente del Firewall pues aparte de incrementar las medidas de seguridad, también por medio del empleo de la memoria caché del Proxy, se agilizan mucho las consultas a las páginas Web más bajadas por la red. La gran diferencia con un Firewall es que un Servidor Proxy, solo actúa a nivel de Aplicación, por lo tanto, "no ve paquetes", recién comienza a interpretar el más alto nivel.

Problemas: Ciertos sistemas como SOCKS necesitan programas cliente modificados para soportarlo.

** Pasarelas a nivel de Aplicación (Application Gateway)*

Estas pasarelas se ocupan de comprobar que los protocolos a nivel de aplicación (ftp, http, etc) se están utilizando de forma correcta sin tratar de explotar algunos problemas que pudiese tener el software de red.

Problemas: Deben estar actualizados; de otro modo no habría forma de saber si alguien está tratando de atacar nuestro sistema.

20.9. Filtrado de paquetes:

Un filtro de paquetes consiste en una asociación <regla, acción> aplicada a los paquetes que circulan por una red. Generalmente estas reglas se aplican en los niveles OSI de red, transporte, y sesión definiendo mecanismos mediante los cuales se deniega o se otorga el acceso a determinados servicios.

¿ Dónde se puede instalar un filtro de paquetes ?

El mejor sitio para instalar un filtro de paquetes es en el router que conecta nuestra red con el exterior (Como medida primaria, pues se debe recordar que también se implementa por medio de Firewall) de este modo ponemos una primera línea de defensa en nuestra red.

Si se dispone de dos router, o una combinación router/ firewall, se puede utilizar un doble filtro de paquetes (dual screened subnet) .

La implementación de filtros requiere como primera medida **agregar al Plan de seguridad de la organización una tabla** que contenga los siguientes apartados: Permitido, Servicio, sentido, y Host. Esto va a ser de mucha ayuda a la hora de codificar en el router las listas de acceso o las reglas en el Firewall.

Ejemplo de tabla:

Interfaz: Internet /eth0

Permitir	Servicio	Sentido	Hosts
SI	*	entrada/salida	*
NO	ftp	entrada	172.125.9.9/24
NO	smtp	entrada/salida	172.125.9.8-14
SI	smtp	entrada/salida	172.125.9.10

En la mayoría de los router y Firewall estas reglas se verifican en el orden en el que aparecen en la tabla hasta que puede aplicarse una de ellas. Esto obliga a ordenar las entradas en la tabla de forma que aparezcan primero las de menor ámbito de aplicación y después las de mayor ámbito. Por ejemplo:

Interfaz: Internet/eth0

Permitir	Servicio	Sentido	Hosts
SI	smtp	entrada/salida	172.125.9.10

NO	ftp	entrada	172.125.0/24
NO	ftp-data	entrada	172.125.9.0/24
NO	smtp	entrada/salida	172.125.9.8-14
SI	*	entrada/salida	*

Como programar un filtro en un router Cisco.

En este ejemplo se va a partir de la tabla que se confeccionó en el ejemplo anterior. Se asume que se dispone de un router SIN NINGUNA lista de acceso (access-list) definida, y que se encuentra en funcionamiento con sus interfaces configuradas y activas (no shutdown).

Tras haberse conectado al router (Vía consola o Telnet) se debe entrar en modo privilegiado. Para ello se debe escribir:

router>*enable*
Password: *password (escribir la clave de enable)*

Si la clave que se ha introducido es correcta, en este momento se puede acceder a la configuración del router y modificarla. No se asuste si el prompt cambia (#): eso significa que se ha cambiado a modo privilegiado.

Para modificar la configuración ello se debe escribir la instrucción:

router#*conf term*

router(config)# <--- Se ha entrado en modo de configuración.

En primer lugar se debe definir las listas de acceso para cada uno de las interfaces (en este caso solo es una). Se debe tener cuidado al introducirlas ya que cometer un error podría hacer que no se pudiese volver a alcanzar el router al aplicar las listas de acceso (si se accede vía Telnet).

Para ello se debe convertir cada entrada en la tabla que se había preparado antes en una entrada como esta:

access-list lista_acceso {permit|deny} protocolo (tcp,udp,icmp...)
dir_ip mascara_red
[dir_ip mascara_red ...]
{eq, gt, lt} {puerto, servicio}
{in, out, any }
{established,...}

De este modo, la tabla quedaría de la siguiente forma:

Permitir	**Servicio**	**Sentido**	**Hosts**
SI	smtp	entrada/salida	172.125.9.10

access-list 102 permit tcp 172.125.9.10 host eq smtp
o bien: access-list 102 permit tcp 172.125.9.10 255.255.255.0 eq 25

Permitir	**Servicio**	**Sentido**	**Hosts**

NO	ftp	entrada	172.125.9.0/24
NO	ftp-data	entrada	172.125.9.0/24

access-list 102 deny tcp 172.125.9.0 255.255.255.0 eq 21
access-list 102 deny tcp 172.125.9.0 255.255.255.0 eq 22

Permitir	**Servicio**	**Sentido**	**Hosts**
NO	smtp	entrada/salida	172.125.9.8-14

access-list 102 deny tcp 172.125.9.8-14 255.255.255.0 eq smtp

Permitir	**Servicio**	**Sentido**	**Hosts**
SI	*	entrada/salida	*

access-list 102 permit tcp any host gt 0

Resumiendo, se tendrá la siguiente lista de acceso:

access-list 102 permit tcp 172.125.9.10 255.255.255.0 eq 25
access-list 102 deny tcp 172.125.9.0 255.255.255.0 eq 21
access-list 102 deny tcp 172.125.9.0 255.255.255.0 eq 22
access-list 102 deny tcp 172.125.9.8-14 255.255.255.0 eq smtp
access-list 102 permit tcp any host gt 0

Una vez definida y revisada la lista de acceso, se debe aplicar a uno (o varios) de las interfaces de la siguiente forma:

router(config)# *interface ethernet0*

router(config-int)# *ip access-group 102 in*

En este momento el router ya está aplicado el filtro que se ha especificado para cada uno de los paquetes que atraviesan la interfaz Ethernet 0.

Existen varias posibilidades para la definición de entrada/salida, declararla como *in o out*, o también no especificarlo y realizar una lista para cada Interfaz. La segunda opción es en realidad la más segura pues se filtra antes de ingresar al router, por lo tanto en el ejemplo en realidad se debería realizar una lista distinta para la Interfaz Internet y aplicarla al puerto WAN, y otra para la Ethernet y aplicarla a la Interfaz LAN

Finalmente, se debe almacenar la configuración del router escribiendo:

#*wr* (en IOS posterior a 11 o Copy running-config startup-config en anteriores)

20.10. Empleo práctico:

Se deja como último tema esta serie de medidas prácticas a implementar:

1) Informar a los usuarios: Notificar permanentemente a los usuarios las medidas de seguridad que deben respetar y los mecanismos que se encuentran implementados, mentalizarlos de la importancia del uso de contraseñas en forma individual y secreta. Reciba y fomente el flujo de información desde los usuarios acerca de sospechas o detección de anomalías o fallas.

2) Crear conciencia de seguridad: Basada en la importancia de la confiabilidad del sistema, como así también en las medidas de responsabilidad contra virus.

3) Respaldar siempre: Determinar los niveles de importancia de la información, tiempos óptimos para resguardo y recuperación, periodicidad del resguardo y verificación de integridad. (¡Toda medida en este tema es siempre insuficiente!).

4) Almacenar Todos los reportes, planes y medidas de seguridad FUERA DE LINEA: Es decir en una PC que se encuentre físicamente desconectada de la red.

5) Realizar verificaciones no predecibles: Evitar la rutina, tratando de aleatoriamente generar auditorías.

6) Leer los registros: Es de suma importancia saber que registrar, pues si es todo, es muy difícil de interpretar y termina no siendo controlado. Por el contrario si se registra poca información, faltarán elementos de juicio. Independientemente del volumen, SIEMPRE revise los registros pues de nada sirve registra si se archiva y nada más.

7) Mantener siempre las últimas versiones: Tanto en los Firewall, router, sistemas o herramientas, a medida que se descubren bugs o nuevas tecnologías, aparecen “Parches” o versiones actualizadas que ofrecen mayores posibilidades o solucionan fallas o vulnerabilidades existentes. Por lo tanto si un determinado elemento se puede mejorar, es importante hacerlo.

8) Manténgase actualizado sobre seguridad: Este es el tema más caro, difícil, costoso y escaso de encontrar en la masa de las redes, pues involucra el recurso humano, el cual es el más preciado. Es muy raro encontrar en un grupo de administración de red, a personas que se dediquen con exclusividad a este tema, y realmente es uno de los flancos más vulnerables de un sistema. Sobre este tema es tanta la información que se puede obtener, que se debe seleccionar muy bien donde buscarla para no desperdiciar tiempo innecesario.

   Una de las medidas más importantes en este tema es subscribirse a alguna lista de correo de seguridad, alguna de las cuales pueden ser:

   Security-request@cpd.com

   Risks-request@csl.sri.com

   Listserv@lehiibm1.bitnet

   Bugtraq-request@crimelab.com

   Cert-tools-request@cert.sei.cmu.edu

   Tcp-ip-request@nisc.sri.com

   seg-l@securenetworks.com

   También en Grupos de noticias: Estos también permiten formar núcleos de discusión, pero se diferencian de las listas en que se emplean programas especiales que permiten intercambiar información en forma más dinámica, estos programas existen de varios tipos, tanto gratuitos como comerciales. De la misma forma que las listas de correo estos pueden ser moderados e inmoderados, y algunos de los relacionados con seguridad son:

   - misc.security
   - alt.security
   - comp.security.announce

- comp.protocols.tcpip (Discusión sobre la pila de protocolos TCP/IP)

9) Consulte organismos de seguridad: Existen muchos y su tarea es investigar y dar respuestas ante problemas ocasionados en el tema de seguridad en redes. Suelen responder a la denominación de equipos de respuesta (CERT: Computer Emergency Response Team o IRT: Incident Response Team) algunos de ellos son los mencionados en el punto 20.7.5.

10) Consulte novedades de seguridad en Internet (Anteriormente detalladas las páginas Web).

20.11. Ataques en TCP/IP:

En general , en todo sistema de computación existe un flujo de información desde una fuente hacia un sumidero. Estos roles en la arquitectura cliente/servidor, se pueden ir modificando dinámicamente entre los distintos Host de la red. Este flujo normal puede ser alterado por cuatro tipos de ataques, los cuales si bien guardan relación con lo mencionado en el punto 20.2.1. aquí se tratarán más en detalle. Estos son:

- **Interrupción**: Un recurso del sistema es destruido o se vuelve inutilizable. Este es un ataque a la *disponibilidad*.
- **Interceptación**: Un tercero no autorizado obtiene acceso a un recurso. Este es un ataque a la *confidencialidad*.
- **Modificación**: Un tercero sin autorización, no solo obtiene acceso sino también corrompe el recurso. Este es un ataque a la *integridad*.
- **Fabricación**: Un tercero no autorizado inserta objetos falsos en el sistema. Este es un ataque a la *autenticidad*.

Tipo de ataque	Qué ataca?
Interrupción	*disponibilidad*
Interceptación	*confidencialida*
Modificación	*integridad*
Fabricación	*autenticidad*

Los ataques pueden clasificarse también en:

- **pasivos**: el objetivo es obtener información que está siendo transmitida, pueden ser:
  - * Análisis de tráfico: Se emplea para determinar protocolos, puertos direcciones de hardware y Software, nombres, contraseñas, servidores, bases de datos, horarios, dispositivos, segmentos, subredes, permisos, etc.
  - * Obtención del contenido de los mensajes: Para interpretación de los mismos.
- **activos**: involucran tomar participación en la transmisión; modificando o generando datos falsos, estos pueden ser de cuatro tipos:
  - * Falsificación de la identidad: Previamente se debe obtener cuentas, permisos o identidades de usuarios de una red para posteriormente hacerse pasar por ellos. Se debe tener en cuenta especialmente que cuanta mayor autoridad administrativa posea su identidad, mayor será la capacidad de este ataque.

* Retransmisión: Se trata de obtener un mensaje (Triangulándolo), para luego colocarlo nuevamente en el canal de comunicaciones. Esta actividad puede llevar involucrada o no la modificación, como así también podrá ser retransmitido al destino real o algún otro.

* Modificación de mensajes: Alterar los datos del mismo.

* Negación de servicio: Tomar medidas para que un determinado servicio no esté accesible en la red, generalmente se basa en la generación de un alto tráfico aparentemente legítimo. Se los conoce como *"ataques de inundación*".

  Una vez que este ataque se ha producido, existen una serie de medidas que pueden ser llevadas a cabo

  1) Registrar el horario del ataque.

  2) Registrar la dirección IP en el momento del ataque.

  3) No intentar contestar el ataque.

  4) Buscar cuál es el dominio en el que se encuentra la dirección IP del atacante.

A continuación se tratará en detalle cómo se llevan a cabo estos ataques tratando de clasificarlos con un nombre adecuado.

20.11.1. Ataques de negación de servicio:

20.11.1.1. Ataques LAND: Si se recuerda el Header de TCP, para establecer una sesión TCP, el primer segmento debe tener en 1 el bit SYN. Si se envían paquetes con el bit SYN en 1, con la dirección IP del "blanco" (Así se llamará desde ahora el Host atacado) tanto en el campo origen como destino, y a su vez con el mismo puerto origen y destino; el receptor de los mismos entrará en un Loop infinito para tratar de resolver este inicio de sesión con el mismo.

20.11.1.2. Inundación de SYN: Si se satura un host con segmentos falsos con el bit SYN en 1, comenzará con la secuencia de establecimiento de sesión, es posible que le responda con el bit SYN y ACK puesto a 1 y que deje abierta esta sesión durante un tiempo considerable hasta recibir el tercer paso del establecimiento de sesión (segmento con bit ACK a 1), el cual por supuesto nunca recibirá, una sesión así se llama a medio abrir (Half-open). El servidor en este momento lleva construida una estructura en su memoria que describe todas las conexiones pendientes. Esta estructura es de tamaño finito, por lo tanto puede hacerse desbordar.

20.11.1.3. Ataques Tear Drop: Este ataque se lleva a cabo por medio del uso de la fragmentación y reensamble. Se envían series de paquetes que al intentar ser reensamblados, sus identificadores no coinciden con lo que los Header de TCP/IP creen que debería ser. Esto puede causar la caída del blanco, o la rotura de sesiones anteriormente establecidas.

20.11.1.4. Ataques Nuke o Fuera de banda: En las redes Microsoft, sis e emplea el protocolo TCP/IP es necesario activar la "Resolución NetBIOS sobre TCP/IP", esto permite que a través de los puertos 137, 138 y 139 se activen los servicios NetBIOS,

y a través de estos se pueda operar con "Entorno de Red, Mensajería, etc." en forma individual y grupal. Recordar que este protocolo asocia Direcciones IP con nombres NetBIOS. Si se envían segmentos falsos a estos puertos, pueden causar que no operen adecuadamente, dejando fuera de servicio la red o al Host blanco. Como el Sistema de Nombres NetBIOS no se emplea en Internet, una muy buena medida es negar el acceso a estos puertos en los router, a través del empleo de listas de acceso extendidas.

20.11.1.5. Ping de la muerte: Se lleva a cabo por medio del protocolo ICMP con una solicitud de eco (Tipo 0, conocido como ping) pero de longitud superior a lo que una red soporta. Al ser recibido, el host no sabe como tratarlo y se bloquea. Cabe aclarar que hoy la masa de los sistemas ya no lo permiten.

20.11.1.6. Ataques Bonk: Se produce por medio del envío de paquetes corruptos al puerto UDP 53 es decir al asignado a DNS. Este ataque suele dejar fuera de servicio al host destino.

20.11.1.7 Ataque BrKill: Se lleva a cabo por un atacante que envía paquetes de reinicialización, obligando al blanco a cerrar todas sus conexiones.

20.11.1.8. Ataque NT - MsgBox: Si un atacante se encuentra en una máquina cliente de la red Windows NT y envía una gran cantidad de Message Boxes al servidor dentro de un período de tiempo relativamente corto, provoca que el servidor deba esperar hasta que los mismos sean cerrados MANUALMENTE. Esto aprovecha un seteo que posee Windows NT que configura una cantidad máxima de ventanas, si el mismo está activado y se supera este límite, se produce el detenimiento del servidor.

20.11.2. Ataques ARP:

20.11.3. Ataques ICMP: