Redes de ordenadores

Firewalls y seguridad

Grupo de sistemas y comunicaciones
Juan Jesús Muñoz Esteban
jjmunoz@gsyc.inf.uc3m.es

10. Seguridad en redes internet

Qué es seguridad: Tener la confianza suficiente de que las cosas son como creemos que son.

Aspectos de seguridad:

Autenticación: sabemos quienes somos.
Por certificación de una entidad: DNI
Por redes de confianza: me lo presenta un conocido.
Confidencialidad: Nadie puede ver información ajena.
Integridad: La información no se ha visto alterada por terceros. Esto incluye la secuencia de entrega (que no eliminen ni inserten otros mensajes).
Autenticidad: Además de integridad, se garantiza la autenticación del autor.
No repudiación: Que no se pueda negar la autoría.
Disponibilidad: Que no nos puedan negar el acceso al servicio.

Técnicas:
Autenticación: Posesión de información o características físicas.
Certificaciones
Infraestructura PKI de CAs
Confidencialidad:
Control de accesos: Sniffers, Firewalls, TCPwrappers
Cifrado:
Clave privada: DES...
Clave pública: RSA, curvas elípticas...
Integridad: Funciones HASH (MD5, SHA1)
Autenticidad: Firma Digital

Estrategia: Se suele recomendar que como norma general, todo lo que no está expresamente permitido está prohibido por defecto.

10.2 Internet, intranets y extranets

La tecnología de comunicaciones de Internet permite la interconexión de todos los ordenadores entre sí, pero no se ocupa, en principio, de otros temas como distinguir calidades de servicio o prestaciones, la imputación de costes, la fiabilidad de enlaces o, lo que puede ser más peligroso, la seguridad.

En ciertos entornos (en concreto entre una red corporativa con infraestructura *internet* y conectada al resto de Internet) es fundamental la inserción de sistemas que implementen una política de control de acceso entre redes de manera que se prohiba o se permita explícitamente un determinado flujo de información y se garantice disponibilidad y e integridad.

Internet: la red basada en protocolos *internet* (TCP/IP) de ámbito mundial.

Intranet: red privada constituida por protocolos y aplicaciones internet.

Extranet: acceso a (parte) de una *intranet* desde puestos remotos (de otras redes ajenas a las que se otorgan ciertos permisos extra, o desde puestos cualesquiera) mediante la infraestructura de Internet. Habitualmente un producto de encriptación acuerda una clave de sesión y cifra los paquetes de esa conexión, encapsulandolos sobre IP (tunneling: IPSEC, ssh, ssl, skip).

Cualquier ataque que pueda aparecer en los medios de comunicación, haya o no producido daños a los sistemas o adulterado la información, puede causar tanto daño en ocasiones como una verdadera filtración o alteración. El coste de tan evento es muy superior incluso al coste del sistema informático, por lo que debe alcanzarse un grado de confianza suficiente, mediante procedimientos de homologación, de que no se va a producir tal evento, amén de prever un sistema de respuesta a incidentes y evaluar los distintos riesgos.

10.3 Contexto general

Desde el momento en que una máquina queda conectada a Internet, está accesible desde el resto de ordenadores de cualquier parte del mundo (en general tanto ella como el resto de máquinas de la organización conectadas en la misma red), y por lo tanto expuesta a posibles accesos no controlados. Esto da lugar a que cualquier fallo de seguridad ese ordenador, si también está conectado a la red corporativa, pone en peligro al resto de máquinas y a la información almacenada en ellas, que puede no sólo ser obtenida por personas no autorizadas, sino incluso ser modificada con resultados aún más graves.

Este espacio abierto ha dado lugar a que aficionados de gran capacitación técnica y dedicación, y pocos prejuicios morales, se dediquen a intentar vulnerar los sistemas de seguridad de los equipos conectados a Internet. Pero lo más grave es que también hay personas e incluso organizaciones financiadas por grupos de interés o por servicios de inteligencia de otros países, y dedicadas por completo a intentar irrumpir en los equipos.

A continuación se expone una breve cronología de conocidos fallos de seguridad, que han tenido como protagonistas a las tecnologías de la información y las comunicaciones, y que pueden servir para concienciarnos del problema:

1973 Un cajero de la entidad Dime Savings, de Nueva York, utiliza un ordenador para desfalcar más de un millón de dólares.

1978 El Wells Fargo Bank es víctima de un golpe de 21,3 millones de dólares por un fraude informático.

1982 Mitnick se hace famoso al meterse en el ordenador de mando de la defensa aérea norteamericana. Asimismo, se hace temporalmente con el control del teléfono central de tres oficinas de Manhattan y logra acceder a los centros de conmutación telefónica de California.

1985 Una investigación pone al descubierto una red de 30 estudiantes pertenecientes a la Universidad del Sur de California que alteraban las licenciaturas y confeccionaban títulos fraudulentamente.

1987 Unos miembros de Chaos Computer Club se introducen en la red mundial SPAN de la NASA. El incidente acaba en una debacle de relaciones públicas, tanto para la NASA, como para DEC, su suministrador de sistemas.

1988 Alemania inicia su proyecto Rahab. Basándose en técnicas de intrusión informática, un equipo que forman especialistas en ordenadores y altos cargos de la inteligencia lleva a cabo una investigación sobre las irrupciones en la red que se producen en Estados Unidos y en cualquier otra parte. Asimismo catalogan las direcciones de red y establecen canales para un uso futuro.

1993 El CERT informa que desde el año 1982 se ha registrado un aumento del 73% de incidentes que tienen que ver con la seguridad de Internet.

1994 Un profesor de Texas A&M recibe amenazas de muerte después de que un intruso se identificara en su ordenador desde fuera del campus y enviara por correo electrónico 20.000 mensajes de carácter racista.

1995 Unos estudiantes detectan una versión vulnerable de un programa en el servidor WWW de la-moncloa (Presidencia de Gobierno. España). Afortunadamente el ordenador sólo contiene información general y no está conectado al resto de la intranet. A partir de ese momento se instala una versión segura de correo electrónico, pero la noticia aparece en los medios de comunicación como si de un acceso incontrolado se hubiese tratado.

No sólo hay peligro de que información privada pueda filtrarse al exterior, o que desde el exterior puedan dañarse sistemas, eliminarse o alterarse datos o simplemente utilizar los equipos. Las repercusiones de un ataque, pese a sus mínimas consecuencias objetivas, podrían ser gravísimas en la opinión pública.

Internet se ha ocupado tradicionalmente de lograr conectividad, pero ahora se le exige garantizar el control del acceso y la confidencialidad de la información que viaja en los datagramas IP. El comercio electrónico necesita que los números de las tarjetas de crédito no puedan utilizarse de forma fraudulenta y que las empresas que utilizan Internet para conectar sus redes privadas e interactuar automáticamente con seguridad

10.4 Conexiones incontroladas

La puesta en marcha de un servidor de Internet, supone la integración de dicho equipo como un nodo de Internet como una simple una dirección IP. A partir de este momento los servicios que estén habilitados para aceptar una conexión desde el exterior permiten que se pueda producir un acceso incontrolado aprovechando cualquier laguna, ya sea por defectos en el protocolo, errores en la implementación de los programas de los servidores o la configuración de los mismos, por la debilidad de las contraseñas o por la asignación de permisos.

No obstante, el peligro de estas conexiones no se limita al hecho en sí y sus efectos no se producen necesariamente sobre los servicios ofrecidos o sobre lo que se ha definido de antemano. Depende de lo que se pretenda realizar una vez logrado ese acceso, que puede servir de mero trampolín para otros fines.

Contemplando la topología de conectividad implantada en el servidor de Internet (servidor aislado de otras redes departamentales o conectado a alguna o varias de dichas redes), las accesos incontrolados podrían efectuarse para conseguir diferentes objetivos:

- Consultar y examinar la estructura/contenido del equipo. Esta situación normalmente no es el objetivo final, sino el inicio a partir del cual se establecen otros nuevos.
- Obtener información diferente a la exclusiva que desea suministrar el Servidor. Se trataría de conseguir programas, ficheros de datos, palabras claves u otras identificaciones de diferentes usuarios. Este objetivo no produciría una alteración en el funcionamiento del equipo(salvo una mínima perdida de prestaciones y algún consumo), pero se darían actividades de piratería informática o de otro tipo dependiendo de la información afectada.
- Alterar o destruir la información existente, así como crear puertas falsas, "superusuarios" dentro del equipo o saturar su funcionamiento por capacidades de proceso o de almacenamiento. Con este objetivo podría lograrse desde alterar el funcionamiento normal del equipo, hasta su paralización, incluso logrando la propagación de virus informáticos.
- Utilizar como puerta de entrada para otros equipos, accesibles a través de otras redes. Una vez alcanzados estos segundos equipos, los posibles objetivos perseguidos serían los detallados anteriormente. El objetivo puede ser simplemente utilizar los recursos informáticos sin pagar por ellos.

Todas estas posibilidades de conexiones incontroladas generan la necesidad de incorporar al enlace con Internet una serie de elementos adicionales, que serán tanto más numerosos y precisarán una gestión más dedicada en función de cuantos más servicios se ofrezcan y en función de la importancia que se de a la seguridad en la organización.

Frente a las posibles conexiones incontroladas existen dos líneas de acción:

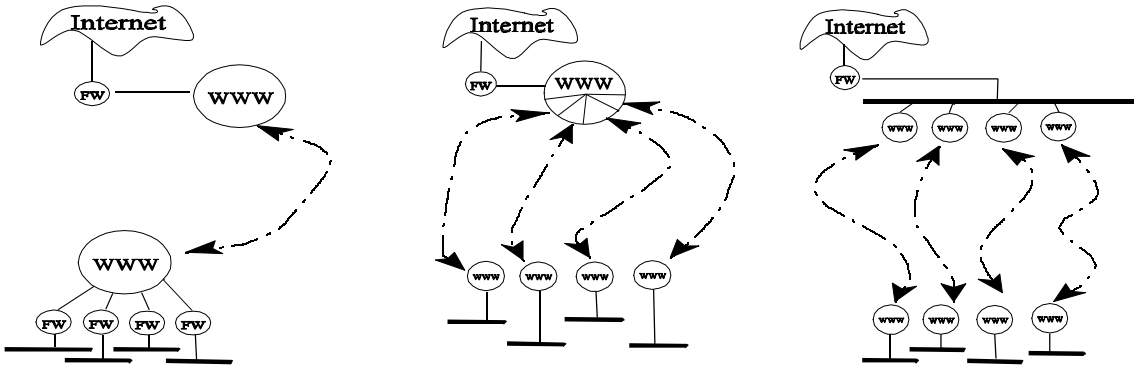
Prevención, mediante instalación de firewalls, configuración de los atributos de directorios y ficheros (lectura, ejecución, escritura, etc.), utilización de programas para el mantenimiento de palabras clave, utilización de criptografía (para prestaciones de carácter departamental), correo electrónico con pasarelas intermedias, conversores de direcciones para evitar accesos hacia redes departamentales. Una medida muy importante en este ámbito de la prevención, es la utilización de versiones de software suficientemente probadas (nunca al 100%). También es importante deshabilitar cualquier servicio no estrictamente necesario, inhibir conexiones desde el exterior en la medida de lo posible, y sustituir los programas de sistema susceptibles de ataque por versiones que no realicen su tarea sino que generen avisos de alarma.

Detección, mediante programas de monitorización en máquinas inalcanzables, que generen alarmas al descubrir repetidos intentos de conexión fallidos, recogida de los eventos y actividades en las líneas de comunicación para el posterior análisis de aquellas incidencias sospechosas, monitorizaciones de actividad en línea, comprobación de los sistemas de ficheros (tamaños, permisos, fechas), etc. Es fundamental registrar la actividad desarrollada por el intruso por inocua que sea, para conocer el alcance de sus acciones y saber cómo actuar en consecuencia. No debe olvidarse que los ataques pueden producirse en cualquier momento (incluidos festivos por la noche), pueden estar camuflados entre infinidad de otros accesos (y falsos ataques).

10.5 Estructuras técnicas y organizativas

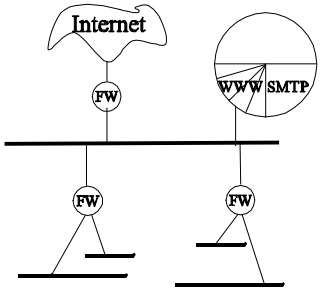
1. Sin conexión entre Internet y las redes corporativas

La seguridad sería máxima para los datos de los usuarios internos, al tener servidores físicamente aislados para el servicio al exterior, pudiéndose tener réplicas totales o parciales, o con información adicional, para dar servicio interno. En este caso puede considerarse poner la información en servidores de ISPs.



El servidor Internet actualizaría su información a base de copias que podrían realizarse mediante cintas magnéticas o por conexiones temporales. En todo caso el problema de la seguridad sigue existiendo: Un ataque al servidor por parte de usuarios de Internet podría hacer salir en prensa noticias que desprestigiarían a la organización y alarmarían a sus directivos.

2. Modelos con conexión a Internet



El mismo servidor que ofrece información hacia Internet está conectado al resto de las redes corporativas. En este caso los ataques podrían suponer una amenaza para la información de la empresa. Con este esquema algunos usuarios de las redes privadas podrían salir a Internet, adecuando las direcciones (NAT) que usan internamente según la RFC 1597. La infraestructura se comparte para recibir correo...

10.6 Conexiones a Internet

El procedimiento habitual para que un usuario particular o empresa acceda a Internet es la contratación de este servicio (ancho de banda según las necesidades, y con coste plano o variable con el tiempo) a un proveedor (ISP), que dispone de una infraestructura (routers, modems, enlace con Internet) y direcciones IP para delegar (obtenidas de InterNIC o de su proveedor).

Mediante enlaces físicos (lineas dedicadas o telefonía, facturada aparte) se accede a la infraestructura del proveedor, se autentica el usuario (obteniendo una dirección IP para esa sesión: chap, radius) y se intercambian datagramas hacia Internet encapsulandolos sobre PPP.

Además hay que contar con un nombre de dominio, si no se quiere que las páginas empiecen por www.miproveedor.es/miempresa. Esto se realiza en www.nic.es, pagando una cuota anual a Rediris.

Una vez seleccionado el proveedor e implantada la infraestructura de comunicaciones, hay que poner la información. Pero además, hay que configurar las aplicaciones (salvo que se utilice el servicio de hospedaje del proveedor) según una política de seguridad definida de antemano para todos los servicios y aplicaciones.

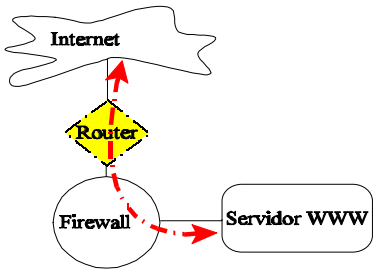
El éxito del servidor dependerá de la información (utilidad), apariencia (la primera impresión retiene o repele) y grado de actualización, de manera que habrá de auditar la calidad que percibe el usuario (ver si demasiada riqueza lo hace lento).El mercado exige estudiar los accesos y adecuar la oferta a la demanda.

Pero además hay que evitar incidentes que afecten a la imagen de la empresa, e incluso a su supervivencia (la dependencia de la misma respecto a la información puede ser definitiva). Esto significa asegurarse de que nadie ha accedido donde no se quería, y que la información que tenemos no ha sido corrompida ni alterada por nadie. Es necesario por tanto establecer mecanismos de seguridad preventiva y de control periódico (auditorías).

10.7 Elementos de conexión

Las figuras representan los elementos funcionales, que no reflejan ninguna disposición física de máquinas ni programas

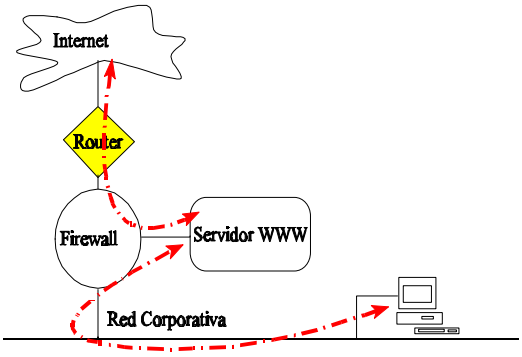
Modelo 1. Servidor separado



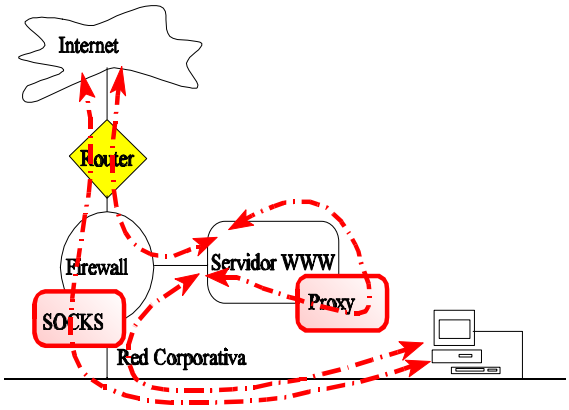
No hay conexión entre el servidor y la intranet. Físicamente puede ser un único servidor (correctamente configurado) o varios (en este caso conviene que una única máquina firewall se responsabilice de toda la seguridad). La oferta interna de esos mismo servicios se logra replicando la información a servidores de la intranet.

Modelo 2. Servidor en dos redes

La oferta externa y la interna son idénticas y simultáneas. El servidor puede actuar de puerta para el correo.



Modelo 3. Salida controlada



Aprovechando la infraestructura anterior se ofrece a los ordenadores de la red corporativa salida (parcial?) a Internet.

Es necesario un elemento “traductor” de direcciones (socks) del dominio privado a otras válidas, o bien usar un agente proxy en el servidor WWW.

10.8 Acceso a la información o a los servicios

Los ordenadores conectados a redes corren más riesgos: son accesibles a personas y ordenadores de ubicación desconocida. A cambio tienen acceso a más servicios e información. Hay que alcanzar un compromiso entre la seguridad y la accesibilidad de los ordenadores.

A nivel de enlace: ¿pueden pincharnos un sniffer?
A nivel de red: spoofing (un ordenador usa una dirección ajena)
Nunca sabes por donde pasa tu tráfico -> cifrar
A nivel de puerto: ¿qué servicios tienes activados?¿Desde dónde?
A nivel de aplicación: ¿cómo se garantiza el acceso? (passwords)
Fallos conocidos en las aplicaciones (sendmail)
Limitaciones de los protocolos (UID en NFS)
Soluciones:
Cableado: Hubs activos que se aprenden las MAC
Evitan beholders o sniffers
Evitan que se pinches otros ordenadores
Usar fibra óptica
Nivel de red: Filtrado de direcciones
Rutas estáticas
Nivel de transporte: Qué servicios están habilitados
Desde dónde se permiten.
Aplicaciones: Versiones probadas
Estudian efectos perversos como qué ocurre cuando de desborda un buffer (ping de 64K, mensajes de correo con direcciones muy largas) o cómo se tratan los parámeros de entrada (CGI).
Verificar los passwords
Afinar la configuración: no exportar a todos... (NFS)
usar Kerberos...

10.9 Cortafuegos o Firewalls

Uno de los principales problemas de seguridad son los accesos externos no autorizados a la información almacenada en los ordenadores, ya estén dedicados a servir información a Internet o bien estén en las redes privadas conectadas a Internet aunque sin intención de ser accedidos desde ella. Por ello hay que definir una política de accesos e implementarla, a ser posible en un punto único (es más fácil vigilar una puerta que cien) que deseablemente debe ser invisible e inaccesible desde el exterior.

Los cortafuegos (*firewalls*) son sistemas o grupos de sistemas que implementan una política de control de acceso entre dos redes, prohibiendo o permitiendo explícitamente una determinada comunicación, en función del lugar de procedencia, el tipo de servicio o los parámetros que se configuren.

Estos dispositivos se colocan en el acceso de una red considerada segura a otra que se considera insegura (como Internet), de modo que se controlan los mensajes que pasan de una a otra y se permite su progresión o no. Este control se realiza de muy diversas maneras (por tipo de servicio, por usuario, por direcciones de origen y/o destino...). Además, la mayoría de los cortafuegos informan de los intentos de acceso no permitido, estableciendo acciones de alarma al detectarse actividades sospechosas, y generan estadísticas varias.

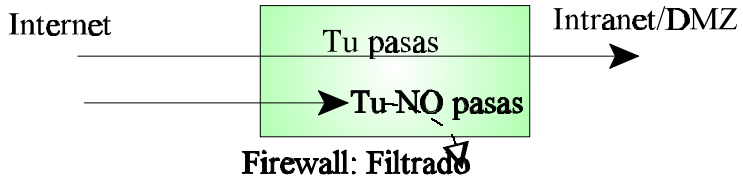
El firewall constituye un punto único donde fijar toda la seguridad, en lugar de obligar a una más cuidadosa gestión de todos los sistemas. Por ello debe ser un elemento de la máxima confianza, cuestión fundamental a la hora de su elección.

Por ser los elementos más expuestos a ataques (deberían ser transparentes para evitarlo), deben someterse a auditorías periódicas, de manera que sean realmente eficaces en una detección precoz de problemas que puedan afectar a la integridad (accesos fraudulentos) o a las prestaciones (tráfico que deteriore la capacidad del enlace con Internet).

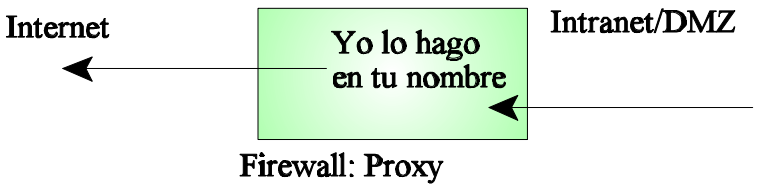
10.10 Tipos de cortafuegos

Se podrían clasificar de la siguiente manera (aunque los productos concretos pueden cumplir varias de estas funciones simultáneamente):

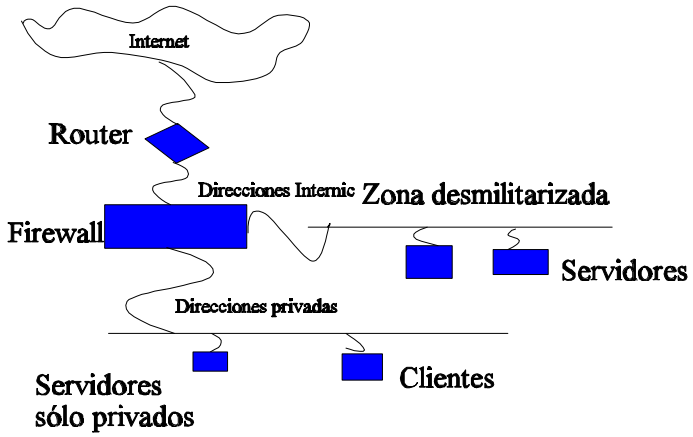
Filtrado de paquetes (*screening*). Se trata de routers con reglas que permiten o impiden pasar a datagramas según ciertas características (entrantes, a puertos no deseados). Son muy rápidos (trabajan a muy bajo nivel). Los más sofisticados incluso entienden los protocolos (ftp...) comprobando la secuencia de mensajes y el estado de las conexiones. Los routers bien configurados hacen esto.



Nivel de aplicación (*proxies*). Un host con dos interfaces (dual homed) pero que no encamina ofrece información al exterior y realiza las consultas que solicitan los clientes de la red privada como si partieran de él. Al ser intermediarios a muy alto nivel, han de configurarse para cada aplicación, y se consideran "más seguros", seguramente porque un fallo por omisión supone una falta de servicio, no una filtración.



10.11 Topología típica



Aspectos fundamentales:

1. El firewall debe ser invisible (no se ataca lo inalcanzable)
2. Debe estar bien configurado (dado que confiamos en su buena configuración en lugar de en la configuración máquina por máquina): deshabilitarlo todo y luego ir habilitando lo que vaya haciendo falta.
    - 2.1. A qué máquinas se puede acceder desde fuera (rutas, listas de control de acceso).
    - 2.2. Qué servicios ofrecen las máquinas accesibles y desde dónde
    - 2.3. Quienes pueden salir y cómo (proxies, socks...). Las direcciones origen, incluso desde la red privada, deben ser direcciones InterNIC.
    - 2.4. Pasarela de correo electrónico
3. Monitorizar el tráfico para detectar plantillas de ataques.
4. Almacenar logs de acceso y comprobarlos. (Si ocurre lo peor, aún puede serlo más si no sabes cuánto te ha afectado). Suele ser necesario un filtrado automático y programar eventos.
5. Definir procedimientos de auditoría y ejecutarlos periódicamente. ¿Estamos realmente haciendolo como lo pensamos?

10.12 Ayuda en la red

En el Instituto de Ingeniería del Software de la Universidad Carnegie Mellon se materializa el CERT Coordination Center definido en 1988 por DARPA, como centro expecializado en seguridad en Internet. Este organismo estudia diferentes problemas de vulnerabilidad, que generalmente se resuelven empleando utilidades como:

Herramientas de control y seguimiento de accesos:

- Control de accesos y anotación flexible de logs: TCP wrapper, xinetd.
- Trazado de tráfico: Netlog
- Auditoría del tráfico IP en busca de patrones especificados: Argus
- Vulnerabilidades de configuración y anotación de logs, filtrado y servicios de red: TAMU
- Identificación de plantillas en archivos para análisis e interpretación de logs: Swatch
- Monitorización de sistemas y redes: Nocol
- Pruebas automáticas de ataques conocidos: SATAN
- Detección de ataque de SATAN generando aviso en syslog: Courtney, Gabriel

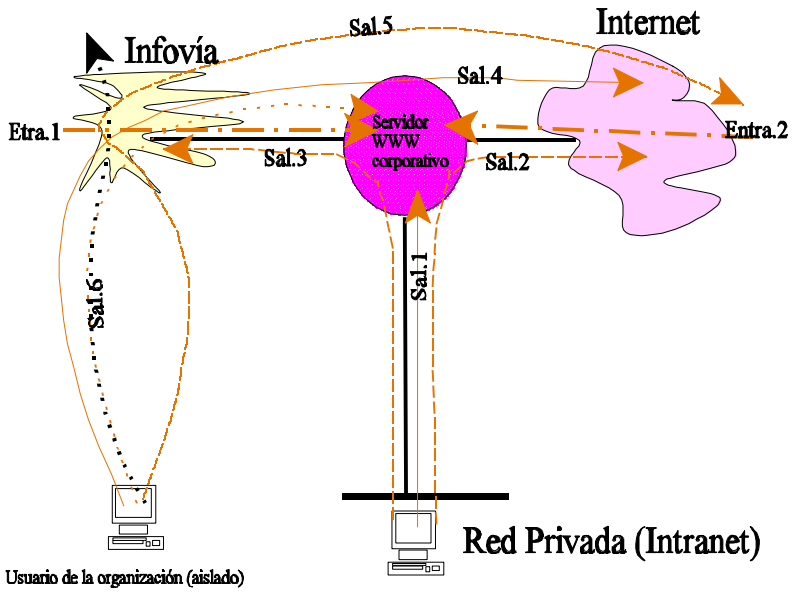
Herramientas que comprueban la integridad de los sistemas:

- Comprobación de puntos vulnerables y debilidades de configuración:COPS, Tiger, ISS
- Comprobación de la integridad del sistema de ficheros y binarios:Tripware
- Comprobación de contrasenas débiles: Crack
- Análisis del log de entradas anuladas: chkwtmp, chklastlog
- Auditoría de procesos en el sistema: Spar
- Auditoría de intentos de conexión a cuentas canceladas: noshell
- Comprobación de si alguna tarjeta de red se utiliza en modo promiscuo: CPM, Ifstatus

La mayoría de las herramientas anteriormente mencionadas están disponibles gratuitamente en Internet. También lo están diferentes versiones de firewalls y toolkits para construir un entorno de confianza.

10.13 Servicios a ofrecer

La infraestructura de acceso a Internet puede utilizarse para poner información en la red, obtener información de la red, intercambiar correo, o incluso ofrecer acceso a Internet a otras personas (empleados desplazados en clientes...)

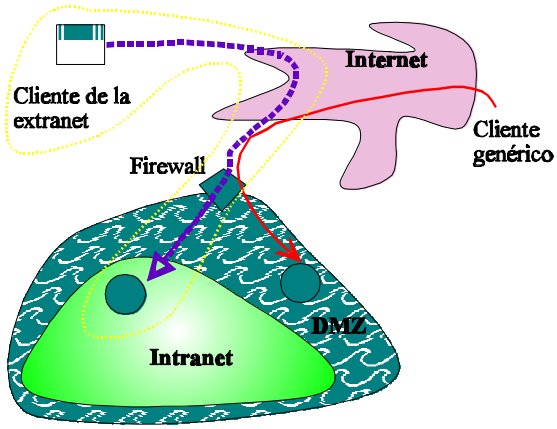


! Entra.1 Acceso por modem de público hispano al servidor corporativo, a través de Infovía
! Entra.2 Acceso de usuarios de Internet al servidor corporativo. Es en este enlace donde habría que situar las pasarelas de correo electrónico.
! Sal.1 Acceso desde de la red corporativa a sus propios servidores Internet/DMZ
! Sal.2 Acceso de usuarios de la red privada a servidores de Internet.
! Sal.3 Acceso de usuarios de la red privada a servidores de Infovía. A diferencia del caso Sal.2, no se puede utilizar el enlace permanente con Infovía. El procedimiento de conexión sería el equivalente al caso Sal.6, es decir, como si se tratase de un ordenador aislado, donde debe evitarse que el PC que accede al exterior por modem pueda encaminar datagramas hacia la intranet.
! Sal.4 Acceso de usuarios de unidades aisladas a Internet a través del servidor Infovía, que realiza funciones de proveedor de servicio de acceso a Internet.
! Sal.5 Acceso de usuarios de unidades aisladas a Internet a través de ISPs, (por Infovía).
! Sal.6 Acceso de usuarios aislados a servidores Infovía

10.14 Redes Privadas Virtuales

Mediante cifrado de los datagramas, éstos pueden transportar información confidencial permitiendo que la red pública se comporte de forma más segura que una red basada en enlaces privados (que pueden ser pinchados).

Hay cortafuegos que permiten que los clientes, dotados de software especial de encapsulación y cifrado, envíen sus datagramas de forma segura por la red y sean convertidos a datagramas normales en la intranet, de manera que pueden acceder a toda la información como si estuviesen dentro de ella.



Esto también puede aplicarse para clientes especiales, a los que se permita acceder a parte de la intranet como si fueran de la propia organización. Esto se conoce como extranet.

ÍNDICE