Comprensión de la necesidad de la seguridad

Conocer los fallos potenciales y las necesidades de protección de su red es un tema importante. Esta toma de conciencia es relativamente reciente. Por ejemplo, muchos de los protocolos que se utilizan no se diseñaron originalmente para ser protocolos seguros. Entre ellos, la mayoría de los relacionados con TCP/IP.

Las interconexiones entre los sistemas se multiplicaron, especialmente a través de la red pública Internet, donde aparecieron numerosos fallos. No se puede pensar en eliminar absolutamente todos los riesgos, pero se pueden reducir conociéndolos y adoptando las medidas adecuadas.

1. Garantías exigidas

La seguridad en red se basa en cuatro puntos clave:

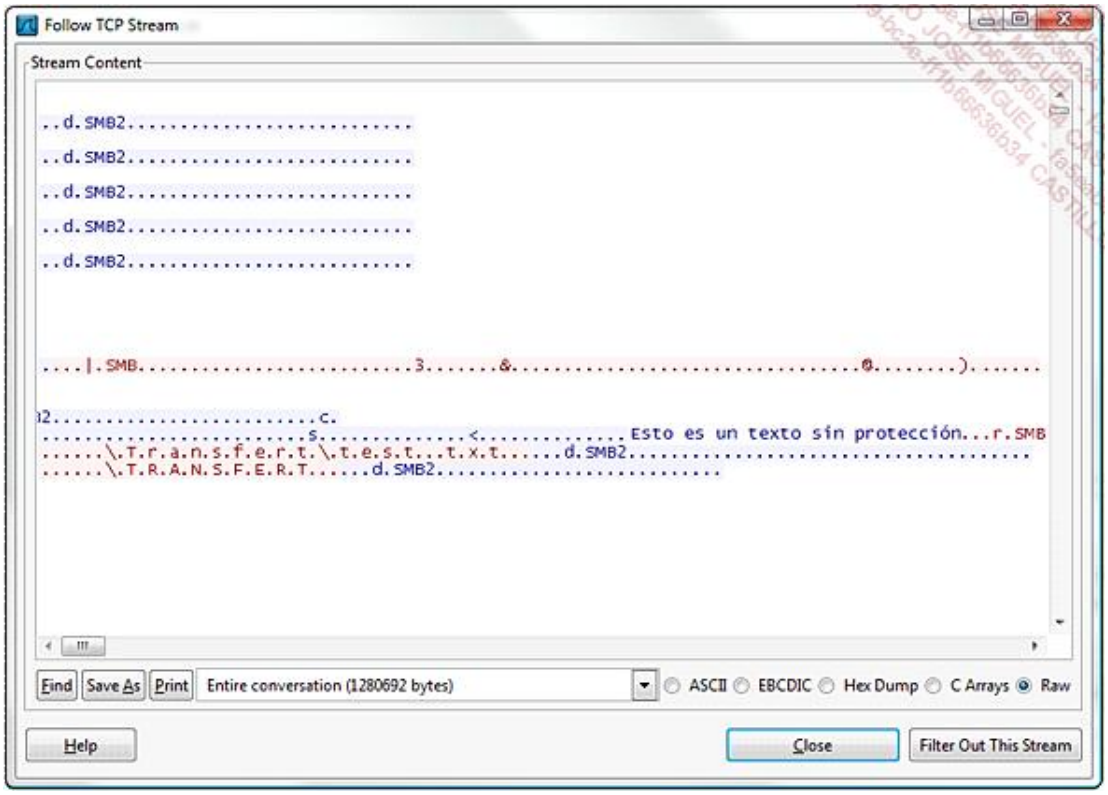
- La **autentificación**, que permite asegurar la identidad para conocer el origen de las comunicaciones.
- La **confidencialidad**, que tiene por objetivo evitar cualquier fuga de información.
- La **integridad**, para prohibir o conocer las modificaciones y evitar pérdidas de información.
- La **disponibilidad**, que permite asegurar un servicio en todo momento.

Como complemento a estos cuatros temas, se puede mencionar el concepto de la **no-denegación**, cuyo objetivo es garantizar, en cualquier circunstancia, el origen de una comunicación o de una transferencia de datos. Para ello, recupera un concepto familiar de nuestra vida cotidiana, como es la firma, pero en formato electrónico.

2. Peligros latentes

a. La circulación de los datos

En muchas redes, la parte fundamental, o más bien la totalidad de las comunicaciones, transitan sin protección. El contenido es legible por cualquiera.



Extracto de la reconstrucción de una trama de red

El análisis de tramas anterior corresponde a una solicitud de apertura de un archivo almacenado en un servidor, hecha desde un equipo de trabajo. Podemos ver que su contenido, «esto es un texto sin protección», se ha reconstruido a través de la comunicación de red.

b. Protocolos de Red y Transporte

Los protocolos de comunicación de red pueden ser el objetivo de ataques dirigidos a sus componentes, es decir, a sus cabeceras.

Se conocen numerosos métodos para esto. Se han utilizado ampliamente las diferentes capas de un modelo como TCP/IP, en que los dos niveles, Red y Transporte, tienen algunas inconsistencias.

Por ejemplo, en *Internet Protocol* (IP), se puede suplantar la asignación lógica de direcciones. Igualmente se pueden manipular las operaciones de fragmentación/defragmentación.

Internet Control Message Protocol (ICMP), y el uso de los comandos «ping», fue objeto de numerosos ataques.

Se puede aprovechar el establecimiento de conexión (3-way handshake) del protocolo *Transmission Control Protocol* (TCP) para apropiarse de las comunicaciones.

Esto no son más que algunas operaciones, pero existen muchas más. Afortunadamente, la experiencia ha permitido convertir estos protocolos en más fiables. De hecho, el software que los controla tiene en cuenta desde hace algún tiempo los antecedentes de los numerosos ataques que se han intentado.

Aunque no estén al abrigo de nuevas tentativas, los riesgos se reducen cada vez más.

c. Protocolos aplicativos estándares

Las últimas amenazas contemplan sobre todo las capas altas. Protocolos aplicativos estándares de TCP/IP, como *HyperText Transfer Protocol* (HTTP), *Simple Mail Transfer Protocol* (SMTP), *File Transfer Protocol* (FTP), *Domain Name System* (DNS), están especialmente amenazados. De hecho, se utilizan con tanta frecuencia que encontrar fallos de seguridad es muy sencillo.

Estos protocolos aplicativos, como los de nivel inferior, presentan numerosos fallos de seguridad debido a que su diseño es antiguo. Incluso podemos decir que es la interpretación del software la que conlleva los principales problemas.

Por ejemplo, la utilización de páginas dinámicas en Internet, cada vez más avanzada, y la de los programas complementarios, implica una programación cada vez más compleja de los navegadores web. Constantemente se descubren nuevos fallos que se deben corregir.

El uso de archivos adjuntos en el correo electrónico permitió una nueva posibilidad de propagación de los virus.

d. Protocolos de capas bajas

En el nivel más bajo, la protección no debe dejarse de lado, cualquiera que sea el tamaño de la red. A nivel local, el uso de conmutadores, para la interconexión de ordenadores a Ethernet, implica la protección de este protocolo. También se debe implantar seguridad para Wi-Fi.

Si la comunicación sobrepasa el ámbito de la empresa, debe ser una prioridad atenuar los peligros potenciales.

e. Riesgos a nivel de software

Los equipos en la red se han vuelto complejos. Los conmutadores, como los routers, proporcionan funciones muy importantes. Son controlados por verdaderos sistemas operativos que, como cualquier aplicación informática de red, contiene fallos potencialmente aprovechables para un ataque.

Es necesario proteger los medios de administración y las cuentas asociadas.

Estos sistemas operativos se deben actualizar igual que los servidores y los equipos de trabajo.