Aseguramiento de la privacidad (Seguridad informática)

Métodos para asegurar la privacidad de la información transmitida

El método más extendido para garantizar la privacidad a la hora de transmitir información es el uso de certificados TLS/SSL. Un certificado de SSL (acrónimo de Secure Sockets Layer) es un tipo de seguridad digital que permite la comunicación cifrada entre un sitio web y un navegador web. Cabe destacar que esta tecnología ha pasado a estar en desuso y ha sido reemplazada completamente por TLS.

TLS significa Transport Layer Security (seguridad en la capa de transporte) y garantiza la privacidad de los datos de la misma manera que SSL. Dado que SSL ya no se usa, este es el término correcto que la gente debería comenzar a usar.

Los sitios web que instalan y configuran un certificado TLS/SSL pueden usar el protocolo HTTPS para establecer una conexión segura con el servidor. El objetivo del protocolo HTTPS es hacer que sea seguro transmitir información confidencial, incluyendo datos personales, o información de pagos o de inicio de sesión.

Fraudes informáticos y robos de información

El fraude informático se refiere al fraude realizado mediante uso de un ordenador por ejemplo a través de Internet.

Algunos ejemplos de fraudes son:

- Timos
- Uso de herramientas para acceder a ordenadores remotos
- Intercepción de comunicaciones
- Robo de información como contraseñas, información bancaria, identidad, etc.

Más información

- https://www.jesusninoc.com/01/12/cadena-de-mensajes-de-un-timo-para-alquilar-una-casa-spam-y-scam/
- https://www.jesusninoc.com/scam/
- https://www.jesusninoc.com/spam/

Control de la monitorización en redes cableadas

Una herramienta básica para observar los mensajes intercambiados entre aplicaciones es un analizador de protocolos (packet sniffer). Un analizador de protocolos es un elemento pasivo, únicamente observa mensajes que son transmitidos y recibidos desde y hacia un elemento de la red, pero nunca envía él mismo mensajes. En su lugar, un analizador de protocolos recibe una copia de los mensajes que están siendo recibidos o enviados en el terminal donde está ejecutándose.

Está compuesto principalmente de dos elementos: una librería de captura de paquetes, que recibe una copia de cada trama de enlace de datos que se envía o recibe, y un analizador de paquetes, que muestra los campos correspondientes a cada uno de los paquetes capturados. Para realizar esto, el analizador

de paquetes ha de conocer los protocolos que está analizando de manera que la información mostrada sea coherente. Es decir, si capturamos un mensaje HTTP, el analizador de paquetes ha de saber que este mensaje se encuentra encapsulado en un segmento TCP, que a su vez se encuentra encapsulado en un paquete IP y éste a su vez en una trama de Ethernet.

Más información

- https://www.jesusninoc.com/05/29/introduccion-wireshark/
- https://www.jesusninoc.com/02/06/rawcap-analizador-de-red/
- https://www.jesusninoc.com/02/06/enviar-un-mensaje-udp-a-un-ordenador-desde-powershell-y-analizar-con-rawcap-analizador-de-red-que-utiliza-sockets-sin-formato/
- https://www.jesusninoc.com/07/20/softperfect-network-protocol-analyzer/
- https://www.jesusninoc.com/softperfect-network-protocol-analyzer/
- https://www.jesusninoc.com/08/09/colasoft-packet-player/
- https://www.jesusninoc.com/01/24/ejercicios-de-routerboard-de-mikrotik-conectarse-a-un-routerboard-de-mikrotik-establecer-una-direccion-ip-en-el-dispositivo-y-capturar-trafico-con-la-herramienta-packet-sniffer/

Seguridad en redes inalámbricas

El problema de las redes WiFi es la seguridad. Existen varias alternativas para garantizar la seguridad de las redes que usan estos estándares.

Consejos que fortalecen la seguridad de las redes inalámbricas:

- Evitar conexiones abiertas.
- Cambiar las contraseñas de acceso.
- Evitar que se pueda tener acceso a través de Internet al router.
- Filtrado de direcciones MAC y direcciones IP.
- Revisar los logs.

Sistemas de identificación: firma electrónica, certificados digitales y otros

La firma electrónica es el archivo o documento electrónico resultante. Este es el documento válido a efectos legales y el que debes conservar. Cualquier impresión o representación gráfica que se haga de él solo es válido en los términos que determine el destinatario de la firma. En general, en este caso, la firma impresa deberá contener un CSV o Código Seguro de Verificación que permite contrastar la copia impresa con la original electrónica.

El proceso básico que se sigue para la firma electrónica es el siguiente:

- El usuario dispone de un documento electrónico (una hoja de cálculo, un pdf, una imagen, incluso un formulario en una página web) y de un certificado que le pertenece y le identifica.
- La aplicación o dispositivo digital utilizados para la firma realiza un resumen del documento. El resumen de un documento de gran tamaño puede llegar a ser tan solo de unas líneas. Este resumen es único y cualquier modificación del documento implica también una modificación del resumen.
- La aplicación utiliza la clave privada para codificar el resumen.
- La aplicación crea otro documento electrónico que

contiene ese resumen codificado. Este nuevo documento es la firma electrónica.

El resultado de todo este proceso es un documento electrónico obtenido a partir del documento original y de las claves del firmante. La firma electrónica, por tanto, es el mismo documento electrónico resultante.

Un certificado de SSL (acrónimo de Secure Sockets Layer) es un tipo de seguridad digital que permite la comunicación cifrada entre un sitio web y un navegador web.

Un certificado SSL pueden usar el protocolo HTTPS para establecer una conexión segura con el servidor. Los certificados SSL/TLS funcionan al vincular digitalmente una clave criptográfica a la información de identificación de una empresa. Esto les permite cifrar las transferencias de datos de tal manera que no puedan ser descifrados por terceros.

El protocolo TLS funciona al tener tanto una clave privada como una pública, así como claves de sesión para cada sesión segura única. Cuando un visitante escribe una dirección con seguridad HTTPS en su navegador web o navega a través de una página segura, el navegador y el servidor web se conectan.

Durante la conexión inicial, las claves pública y privada se utilizarán para crear una clave de sesión, que luego se utilizará para cifrar y descifrar los datos que se transfieren. Esta clave de sesión seguirá siendo válida por un tiempo limitado y solo se utilizará para esa sesión en particular.

Cortafuegos en equipos y servidores

Un cortafuegos es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.Los cortafuegos. pueden ser implementados en

hardware o software, o en una combinación de ambos