TECNOLÓGICO NACIONAL DE MÉXICO.

INSTITUTO TECNOLÓGICO DE TLAXIACO

INGENIERÍA EN SISTEMAS COMPUTACIONALES.

SEGURIDAD Y VIRTUALIZACIÓN

ACTIVIDAD:

INVESTIGACION DE CONTRASEÑAS Y CERTIFICADOS

INTEGRANTES DE EQUIPO:

LUZ ARLETH LOPEZ BAUTISTA

SAÚL LÓPEZ BAUTISTA

DOCENTE:

ING. EDWARD SALINAS OSORIO

SEMESTRE: SEPTIMO. **GRUPO:** 7 US

TLAXIACO, OAXACA A 29 DE AGOSTO DEL 2024.

Contenido

SEGURIDAD

1. Contraseña:

Es un mecanismo de autenticación crucial para proteger la integridad y confidencialidad de la información en sistemas y aplicaciones. Las contraseñas deben ser únicas y complejas, combinando letras mayúsculas, minúsculas, números y símbolos especiales, con una longitud mínima recomendada de 12 caracteres. Además, las contraseñas deben cambiarse regularmente y nunca reutilizarse en diferentes plataformas para evitar riesgos en caso de filtraciones.

2. Certificado Digital:

Un certificado digital autentica la identidad de una entidad, como un sitio web o un usuario, y cifra las comunicaciones para proteger la información. Es emitido por una Autoridad de Certificación (CA) y contiene detalles como el nombre del titular, clave pública, fecha de expiración y firma digital de la CA. Los certificados digitales son fundamentales para protocolos de seguridad como HTTPS y VPNs, y su validez depende de la confianza en la CA que los emite. Además, la revocación de certificados puede ocurrir si se compromete su seguridad.

3. Firma Digital:

Es una técnica de autenticación que garantiza la integridad y autenticidad de un mensaje o documento. Utiliza una clave privada para crear una firma que puede ser verificada con la clave pública correspondiente. Esto asegura que el documento no ha sido alterado y que proviene del remitente legítimo. Las firmas digitales son comunes en transacciones electrónicas, contratos digitales y correos electrónicos para prevenir fraudes y modificaciones no autorizadas.

4. Cifrado Simétrico:

Utiliza la misma clave para cifrar y descifrar datos, lo que lo hace rápido y eficiente para procesar grandes volúmenes de información. Sin embargo, su principal desafío es la gestión segura de la clave compartida. Algoritmos como AES (Advanced Encryption Standard) y DES (Data Encryption Standard) son populares. AES es el estándar actual debido a su resistencia a ataques criptográficos y su capacidad de usar claves de 128, 192 o 256 bits.

5. Cifrado Asimétrico:

Emplea un par de claves, una pública para cifrar datos y una privada para descifrarlos. Este tipo de cifrado facilita la gestión de claves, ya que la clave pública puede ser compartida abiertamente, mientras que la privada se mantiene en secreto. Aunque más lento que el cifrado simétrico, el cifrado asimétrico es fundamental para la transmisión segura de datos y la autenticación de usuarios. RSA es un ejemplo ampliamente utilizado, basado en la dificultad de factorizar grandes números.

6. Hash:

Una función de hash toma una entrada y genera un valor de longitud fija, conocido como hash, que es único para esa entrada. Los hashes son fundamentales para verificar la integridad de datos, ya que un pequeño cambio en la entrada produce un hash completamente diferente. Las funciones de hash deben ser resistentes a colisiones (donde dos entradas diferentes generan el mismo hash) y a preimágenes (dificultad para deducir la entrada a partir del hash).

7. Encriptación:

Es el proceso de convertir datos legibles en un formato cifrado para proteger la información contra accesos no autorizados. Utiliza algoritmos de cifrado para transformar datos originales en texto cifrado, que solo puede ser descifrado con la clave adecuada. La encriptación asegura la confidencialidad y la integridad de los datos tanto en tránsito como en almacenamiento. Existen dos tipos principales de encriptación: simétrica (misma clave para cifrar y descifrar) y asimétrica (clave pública y privada diferentes).

ALGORITMOS DE CIFRADO

1. AES (Advanced Encryption Standard):

AES es el estándar de cifrado simétrico utilizado en muchas aplicaciones por su robustez y eficiencia. Adoptado por el NIST en 2001, AES reemplazó a DES debido a la mayor vulnerabilidad de este último ante ataques de fuerza bruta. AES trabaja con bloques de 128 bits y utiliza claves de 128, 192 o 256 bits, lo que proporciona un equilibrio adecuado entre seguridad y rendimiento.

2. RSA (Rivest-Shamir-Adleman):

RSA es uno de los algoritmos de cifrado asimétrico más utilizados, fundamental para la seguridad en comunicaciones electrónicas y autenticación de datos. Desarrollado en 1977, RSA se basa en la dificultad de factorizar grandes números primos. El algoritmo utiliza un par de claves: una clave pública para cifrar datos y una clave privada para descifrarlos.

3. SHA-256 (Secure Hash Algorithm 256-bit):

SHA-256 es parte de la familia SHA-2 y genera un valor de hash de 256 bits a partir de una entrada de cualquier tamaño. Es resistente a colisiones y preimágenes, lo que lo hace adecuado para aplicaciones que requieren alta integridad de los datos, como la verificación de integridad de archivos y la protección de contraseñas. SHA-256 divide la entrada en bloques de 512 bits y realiza una serie de operaciones matemáticas complejas para producir un hash único.

ESTÁNDARES DE CIFRADO

1. SSL (Secure Sockets Layer):

SSL es un protocolo de seguridad desarrollado por Netscape en la década de 1990 para proteger las comunicaciones en internet. Utiliza técnicas de cifrado para asegurar que los datos transferidos entre un cliente y un servidor estén protegidos contra interceptación y manipulación. Aunque SSL ha sido en gran medida reemplazado por TLS, sigue siendo relevante en la historia de la seguridad en internet.

2. TLS (Transport Layer Security):

TLS es el sucesor de SSL y es el estándar actual para asegurar comunicaciones en internet. Introducido en 1999, TLS ha pasado por múltiples actualizaciones para abordar vulnerabilidades y mejorar la seguridad. TLS 1.3, la versión más reciente, reduce la latencia y elimina características criptográficas obsoletas. TLS proporciona confidencialidad, integridad y autenticación en las comunicaciones, siendo esencial para HTTPS, VPNs, correos electrónicos seguros y otras aplicaciones de red.

PROTOCOLOS DE SEGURIDAD

1. HTTPS (HyperText Transfer Protocol Secure):

HTTPS es la versión segura de HTTP, usada para asegurar la transferencia de datos en la web. Emplea protocolos como TLS o SSL para cifrar la información intercambiada entre el navegador del usuario y el servidor web. HTTPS no solo protege la confidencialidad de los datos, sino que también autentica la identidad del servidor, asegurando a los usuarios que se están conectando a un sitio web legítimo. Los navegadores muestran un candado en la barra de direcciones para indicar que la conexión es segura

2. SFTP (Secure File Transfer Protocol):

SFTP es un protocolo de transferencia de archivos que añade una capa de seguridad adicional sobre FTP mediante el uso de SSH. A diferencia de FTP, que transmite datos en texto plano, SFTP cifra tanto los datos como los comandos de transferencia, protegiendo la información de accesos no autorizados. SFTP no solo asegura la transferencia de archivos, sino que también permite la ejecución de comandos para gestionar archivos de manera remota, como listar directorios y cambiar permisos. Es ampliamente utilizado en entornos empresariales para la transferencia segura de archivos confidenciales.

3. SSH (Secure Shell):

SSH es un protocolo de red que proporciona acceso remoto seguro a sistemas a través de una red no segura. Cifra toda la comunicación entre el cliente y el servidor, protegiendo información sensible como credenciales y comandos ejecutados. SSH se utiliza principalmente para administración remota de servidores y dispositivos, permitiendo a los administradores realizar tareas de gestión de forma segura. Además de acceso remoto, SSH soporta la transferencia segura de archivos a través de protocolos como SCP y SFTP. SSH usa

autenticación basada en contraseñas o claves públicas/privadas, aumentando la seguridad y flexibilidad en la autenticación.

CONCLUSION

En esta investigación, hemos examinado tres protocolos esenciales para la seguridad en internet: HTTPS, SFTP y SSH. HTTPS, al cifrar la comunicación entre el navegador y el servidor web, asegura que la información sensible como contraseñas y datos financieros esté protegida contra espionaje y alteración. SFTP, por su parte, mejora significativamente la seguridad en la transferencia de archivos al cifrar tanto los datos como los comandos, lo que es crucial para la protección de información sensible en entornos empresariales. SSH proporciona acceso remoto seguro y permite la transferencia de archivos y ejecución de comandos de manera protegida, garantizando la confidencialidad de las comunicaciones y la integridad de los datos. El conocimiento y la implementación adecuada de estos protocolos son fundamentales para mantener la seguridad y confianza en las plataformas digitales y en la infraestructura de red moderna, especialmente ante el aumento de amenazas cibernéticas y ataques sofisticados. La aplicación efectiva de HTTPS, SFTP y SSH contribuye a una mejor protección de los datos y a una navegación y administración de sistemas más seguras.

BIBLIOGRAFIA

Comprender los tipos de criptografía: Simétrica, Asimétrica, Hash y más... | Geekflare

Criptografía: Algoritmos de clave simétrico y asimétrico explicados (redeszone.net)

https://justcryptography.com/funcionamiento-de-los-algoritmos-asimetricos-y-la-firma-digital/

Cifrado RSA frente a AES: Una mirada más cercana a la defensa digital (ssldragon.com)

¿Qué es el cifrado AES y cómo funciona? | Ciberseguridad

¿Qué es el cifrado AES y cómo funciona? | Ciberseguridad

What's the difference between SHA and AES encryption? - Stack Overflow

https://www.bing.com/search?q=SSL+TLS&qs=n&form=QBRE&sp=-1&lq=0&pq=ssl+tls&sc=0-7&sk=&cvid=F63750174B74424D9C8A05FB8EE384EE&ghsh=0&ghacc=0&ghpl=

TLS vs SSL: ¿Cuál es la diferencia? ¿Cuál debería usar? (kinsta.com)

¿Qué son los protocolos de seguridad HTTPS, SFTP, SSH y SMTPS? - Seguridad informática I (sybcodex.com)

https://www.bing.com/search?q=HTTPS+SFTP+SSH&qs=n&form=QBRE&sp=-1&lq=0&pq=https+sftp+ssh&sc=16-14&sk=&cvid=5B46D7AA15BF43059C7B50CA58C7801B&ghsh=0&ghacc=0&ghpl=

SSH y SFTP diferencias | GoAnywhere MFT