Confidencialidad en la transmisión

Contenido

Protocolo PGP

La idea de configurar el cifrado de extremo a extremo mediante PGP (Pretty Good Privacy) y la firma digital de correos electrónicos es una buena manera de garantizar la seguridad y la autenticidad de los mensajes.

Voy a explicar un poco del funcionamiento de PGP y la firma para poder entender que es lo que estamos usando,

PGP crea una clave de sesión secreta (un uso), basada en un número aleatorio para el algoritmo simétrico IDEA que cifra el texto comprimido, la clave de sesión se cifra con la clave pública del receptor y se adjunta al texto cifrado, luego, el conjunto es enviado al receptor.

Para firmar el mensaje se genera un resumen y se crea la firma digital usando la clave privada del remitente (garantiza integridad y no repudio).

Ahora que ya conocemos un poco más sobre lo que vamos a usar voy a realizar un tutorial básico para configurar el cifrado PGP en uno de los clientes de correo electrónico populares, Thunderbird.

Nota importante:
Doy por hecho que todos los participantes en la comunicación tengan claves PGP generadas, si no es así, debes generarlas antes de seguir estos pasos.

Lo primero es instalar GnuPG en **https://gnupg.org** y dirigirnos a la sección de descargas, recordar donde lo hemos guardado porque lo necesitaremos posteriormente.

Configuración de PGP en Thunderbird:

Abre Thunderbird.
Navega a "Herramientas" > "Complementos".
Busca "Enigmail" y haz clic en "Instalar".

Una vez añadido el addon de Enigmail, debemos cerrar y volver a abrir Mozilla Thunderbird. Al volver a ejecutarlo, debemos clicar en la pantalla principal otra vez las tres rallas horizontales y seleccionar “Complementos” y “Enigmail”.

Una vez dentro de las preferencias de Enigmail debemos comprobar en las opciones básicas que encontró la instalación de GnuPG. Si está todo correcto ya estaría todo configurado.

Un detalle importante que nos ofrece Mozilla Thunderbird es poder configurar la cuenta encriptada en otro equipo usando “**Autocrypt**” para eso nos dirigimos a la pestaña de “Configuración de transferencia” y clicamos en “Iniciar la configuración de Autocrypt”. Se nos abrirá una pantalla donde simplemente nos da una explicación de cómo funciona y debemos clicar en siguiente y seguir las instrucciones que nos detalla.

Siguiendo el asistente podremos dar de alta en otro ordenador todo el sistema de correo cifrado.

Si no tienes claves PGP, puedes generarlas:
Navega a "Herramientas" > "Configuración de Enigmail".
Selecciona "Configurar claves" y haz clic en "Nuevo par de claves".

Si ya tienes claves PGP, puedes importarlas:

Navega a "Herramientas" > "Configuración de Enigmail".
Selecciona "Configurar claves" y haz clic en "Importar claves desde un archivo".

Si deseas exportar tus claves:

Navega a "Herramientas" > "Configuración de Enigmail".
Selecciona "Configurar claves" y haz clic en "Exportar claves a un archivo".

Configura Enigmail con tus Claves:

Navega a "Herramientas" > "Configuración de Enigmail".

Selecciona "Configurar Enigmail" y sigue las instrucciones para asociar tus claves.

Asegúrate de seleccionar el servidor de claves PGP que prefieras (por ejemplo, "pgp.mit.edu").

Puedes configurar la opción "Usar servidor de claves HKP" si necesitas utilizar un servidor diferente.

Configuración Adicional:

Puedes personalizar la configuración de Enigmail según tus preferencias. Explora las opciones en "Configuración avanzada" para ajustar detalles como el formato del mensaje cifrado, el almacenamiento de contraseñas, etc.

Enviar un Correo Seguro:

Comienza a redactar un correo en Thunderbird.
Selecciona "OpenPGP" en la barra de menú y elige "Cifrar mensaje" antes de enviar.

Verificar Firma y Descifrar Correos Recibidos:

Cuando recibas un correo cifrado o firmado, Thunderbird te dará opciones para verificar la firma o descifrar el contenido automáticamente.

Consejos Generales:

Asegúrate de compartir tus claves públicas con aquellos con quienes planeas comunicarte de forma segura.
Verificar Firma:

Si recibes un correo firmado, verifica la firma para confirmar la autenticidad del remitente.
Almacenar Claves Privadas de Forma Segura:

Guarda tus claves privadas en un lugar seguro y respáldalas por ejemplo con los métodos de las otras pruebas para mayor seguridad.

Identificación correos maliciosos

Supongamos que una empresa ha recibido un spear fishing.

El "spear phishing" es un tipo específico de ataque de phishing altamente dirigido y personalizado en el que los ciberdelincuentes se enfocan en individuos o grupos concretos en lugar de enviar correos electrónicos genéricos a una amplia audiencia. El objetivo del spear phishing es engañar a las víctimas haciéndoles creer que el correo electrónico es legítimo y proviene de una fuente de confianza.

Este ataque se caracteriza por la personalización, puesto que se adapta a la víctima. Los atacantes investigan a la persona o entidad a la que se dirigen y personalizan los mensajes para que parezcan auténticos. Para ello los atacantes por ejemplo suplantan la identidad de alguien conocido por la víctima, como un compañero de trabajo, así que usan formación pública, como nombres, cargos y eventos recientes, para hacerlo parecer real. Es por este tipo de ataques que los correos electrónicos pueden contener enlaces o archivos adjuntos maliciosos diseñados para robar información confidencial o propagar malware. Este tipo de correos pueden incluir amenazas o presiones para que la víctima realice una acción específica, como proporcionar información confidencial o transferir dinero.

Para protegerse contra el spear phishing, es importante:

- Mantener una alta conciencia de seguridad y escepticismo al recibir correos electrónicos, incluso si parecen provenir de fuentes conocidas.
- Verificar la identidad del remitente antes de realizar cualquier acción solicitada en el correo.
- No abrir enlaces o archivos adjuntos en correos electrónicos sospechosos.
- Usar soluciones de seguridad, como software antivirus y sistemas de detección de phishing.
- Educar a los empleados sobre las amenazas de spear phishing y la importancia de la seguridad cibernética.

En las siguientes líneas se proporciona un pequeño tutorial sobre qué tendría que tenerse en cuenta para determinar, usando tanto el contenido como las cabeceras del correo, la falsedad o no del mismo, además de un pequeño tutorial sobre el proceso para comprobar la falsedad o no de los posibles links que se incluyen en los correos y sobre el proceso forense digital para determinar si los ficheros adjuntos que se añaden a los correos pueden resultar maliciosos para el negocio o no.

Sobre la verificación de correo electrónico, debemos tener en cuenta que las cabeceras de los correos nos proporciona información sobre el emisor como su **IP y la ruta que sigue,** debemos comprobar también el nombre de los remitentes pues hay veces que usan un **nombre existente** que puede parecer real pero la dirección desde la que se envía es falsa. Los ataques de fishing suelen contener **errores de ortografía** por lo que deberíamos estar pendientes a este tipo de faltas. No podemos olvidar que lo que se pretende con este tipo de ataque es obtener información confidencial por lo que **NO debemos aceptar solicitudes inusuales** y aún menos si implican envío de dinero o clicks en enlaces. Respecto a la verificación de enlaces podemos comprobar la dirección real de este (no solo el texto visible) pausándonos encima del link y comprobar si proviene de una **fuente fiable**. Como se ha visto en otras consultorías es revelante asegurar la **conexión segura** de ese sitio web (SSL). El conjunto de estas señales forma lo que se llama Phishing Indicators y nos resulta útil para cumplir nuestro objetivo de determinar si el correo es malicioso y estamos siendo atacados.

A este proceso se recoge en lo que denominamos **análisis forense digital** en el siguiente párrafo se muestran los pasos a seguir para realizarlo de forma efectiva.

Primero lo que debemos definir es el alcance de nuestro análisis, ¿qué incidentes vamos a tratar?¿qué estamos investigando?, lo segundo sería la preparación y recopilación de evidencias, esto incluye asegurarse de que la escena del incidente se mantenga intacta y segura, identificación y registro de información sobre el sistema o dispositivos involucrados, sería conveniente realizar una copia de seguridad de los datos relevantes y la

recopilación de registros de eventos, registros del sistema, archivos, registros de red ....

Con los datos recogidos deberá llevarse a cabo un análisis para comprender el incidente, este análisis usará como parámetros de medida los datos mencionados en el párrafo anterior sobre si los correos son maliciosos. En este paso podemos usar herramientas forenses para el análisis de la información recibida, algunas de ellas serían:

- Autopsy
- CAINE
- Digital Forensics Framework
- Volatilidad
- Redline
- COFEE
- Wireshark
- DumpZilla

Más información sobre estas herramientas y análisis forense en el siguiente enlace https://ciberseguridad.com/servicios/analisis-forense/software/

Al finalizar el análisis deberíamos conocer el alcance del daño ocasionado si esque hubiéramos sido atacados.

A continuación se muestra de forma esquemática los pasos seguidos durante todo el proceso:

¿Correo malicioso? Comprobaciones:

- Cabeceras (IP+ ruta)
- Nombre emisor
- Errores ortográficos
- Solicitudes inusuales
- Enlaces falsos (dir mensaje, fuente fiable)
- Conexión segura

Proceso análisis forense digital:

- Alcance
- Recopilación evidencias
- Copia seguridad
- Dispositivos involucrados
- Conclusión (¿malicioso o no?, daño ocasionado)