Nombre: Alejandro Asenjo

Módulo 4: sistemas seguros de acceso y transmisión de datos

Fecha: 23 de junio de 2014

Certificados Digitales (PGP) a través de Thunderbird

En Windows para ver los certificados instalados es certmgr.msc. No se recomienda un certificado que esté vigente más de 3 años.

En España la Certificación es de la Fábrica de Moneda y Timbre.

Se recomienda esta informados a través de la página web de Red Temática de Criptografía y Seguridad de la Información (CriptoRED).

El protocolo utilizado para cifrar mensajes se llama PGP (Pretty Good Privacy). Para poder utilizar PGP desde Thunderbird, hay que instalar:

- **GnuPG**: (GNU Privacy Guard): Una implementación libre de PGP
- **Enigmail**: Un complemento de Thunderbird.

Una vez instalados, se procedió a la creación de la llave PGP, utilizando OpenPGP de Thunderbird.

Redactamos el mensaje y en la solapa de OpenPGP, seleccionamos “Attach My Public Key” para enviar la clave pública al destinatario.

El “destinatario” al recibir la clave pública, debe abrir el correo y en el adjunto está la “clave pública” con la extensión “.asc”, a continuación la importa.

Una vez recibida el correo electrónico firmado digitalmente o cifrado se peidrá que introduzca la contraseña secreta para descifrar el mensaje.

Si la clave se viera “comprometida” (es decir, alguien ha tenido acceso al archivo que contiene la clave privada), se debe revocar el conjunto de llaves lo antes posible y crear un nuevo par.

Más información: https://support.mozilla.org/es/kb/firma-digital-y-cifrado-de-mensajes

Armitage (herramienta de Kali Linux)

Es la interfaz gráfica de metasploit.

Maltego (herramienta de Kali Linux)

Ataca el dominio y se puede ver su crecimiento y los emails que involucra dicho dominio.

MD5

Es uno de los algoritmos de reducción criptográficos.

Se realiza una instalación del XAMPP y se ejecuta el MySQL donde podemos comprobar cambiando el parámetro a MD5 como funciona el algoritmo de encriptación