PRÁCTICA 5: PGP y Protocolos

Seguridad en la Información
Curso 2018-2019

Lenguajes y Ciencias de la Computación.
ETSI Informática, Universidad de Málaga

EJERCICIO 1: PGP en Thunderbird

Este ejercicio se centra en el envío de un correo electrónico usando las herramientas de **PGP** y **Thunderbird** [1,2], aunque, el alumno también puede aplicar cualquier otro gestor de correo electrónico con capacidad para interpretar PGP, como pueden ser: Kmail, Pine o Evolution [1].

Concretamente, se pide:

1) **Instalar** Thunderbird (u otro gestor de correo electrónico con capacidad para interpretar PGP).
2) **Configurar** Thunderbird para que gestione una cuenta de correo real, y añadir como complemento el plugin **Enigmail** [3], que permite utilizar GnuPG en el propio gestor de Thunderbird.
3) **Configurar** Enigmail, incluyendo la **generación** de un par de claves públicas (Kpriv, Kpub) del usuario dentro del programa Enigmail.
4) **Enviar un correo electrónico (sólo cifrado, no firmado)** al profesor correspondiente de cada grupo según las indicaciones del campus virtual, indicando:

Subject: **[PGP–SI-2018-2019] Nombre y Apellidos** Body: **Ejercicio 1 con PGP**

Para ello, es necesario importar la clave pública del Profesor/a, que se encuentra disponible en el Campus Virtual.

Es muy importante que se escriba en el subject del email la cabecera indicada anteriormente. De lo contrario, no se considerará como válida la actividad.

EJERCICIO 2: Análisis del protocolo TELNET

En el campus virtual se proporciona una captura de una sesión TELNET entre un cliente (192.168.0.2) y un servidor (192.168.0.1). Esta captura la ha realizado un adversario que se encontraba en la misma red que el cliente, y que busca obtener tanto la información del usuario como los comandos que se han enviado.

La captura de la sesión se ha realizado con el programa **Wireshark** [4]. El alumno también utilizará este programa para analizar la captura de la sesión.

Se pide, por tanto, al alumno que responda a las siguientes preguntas:

1. ¿Qué usuario y contraseña se ha aplicado para acceder al servidor de Telnet 192.168.0.1?
2. ¿Qué sistema operativo se está aplicando en el servidor?
3. ¿Qué comandos ha ejecutado el cliente en el servidor telnet?

En todas las preguntas, es indispensable incluir capturas de pantallas.

EJERCICIO 3: Análisis del protocolo SSH

Tras un ataque de suplantación de identidad, el usuario del ejercicio anterior ha aprendido la lección y ha empezado a utilizar el protocolo SSH. La primera comunicación entre el cliente (192.168.0.13) y el servidor (192.168.0.24) fue capturada por otro adversario, aunque éste no pudo capturar la comunicación del servidor al cliente. Esta captura se encuentra disponible en el campus virtual.

Se pide por tanto al alumno que responda a las siguientes preguntas:

1. ¿A partir de qué paquete comienza a cifrarse el tráfico de red?
2. ¿A qué nivel se aplica el cifrado del protocolo SSH? Es decir, ¿se aplica el cifrado a los protocolos de red (IP, TCP, etc.), a las capas superiores, o a ambos?
3. ¿Es posible ver alguna información sobre credenciales de seguridad como puede ser el usuario y la contraseña?

INFORMACIÓN COMPLEMENTARIA

Instalar Thunderbird y PGP

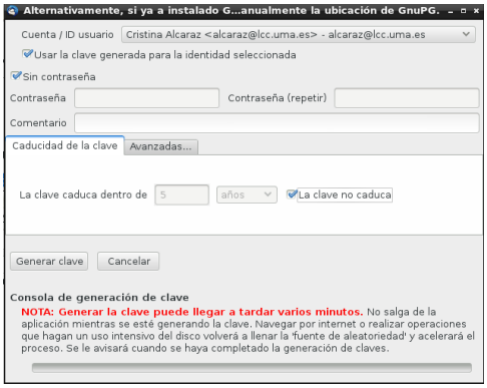
En las distribuciones Linux, existen varias formas de instalar *Thunderbird*:

a. Fedora 19: **yum install thunderbird**.
   i. Las versiones superiores de Fedora requieren usar **dnf install thunderbird**.
b. Kali Linux o Ubuntu: **apt-get install thunderbird**.

Con respecto a Windows, puede descargarse el programa de instalación desde la página de Thunderbird [2].

La herramienta *GPG*, necesaria para hacer funcionar la extensión *Enigmail*, viene instalada por defecto en las distribuciones Linux. Sin embargo, en Windows es necesario descargar e instalar el programa GnuPG [5].

Instalación y uso de Enigmail



Para instalar y configurar *Enigmail*, se aconseja seguir las instrucciones del manual de usuario, disponibles en [6].

Es también fundamental generar el par de claves públicas (Kpriv, Kpub) sin contraseña o sin la palabra de paso, de lo contrario, puede que se produzcan problemas posteriores para generar firmas o descifrar texto cifrado.

Wireshark

Respecto al uso de la herramienta *Wireshark*, se aconseja consulta tanto la guía de usuario de Wireshark [7] como la guía del INCIBE [8].

TELNET Y SSH

Los principales RFC referentes a los protocolos *TELNET* y *SSH* son los siguientes:

- *TELNET*: RFC 854, 855-861
- *SSH*: RFC 4251, 4252-4256

Referencias:

[1] https://fedoraproject.org/wiki/Using_GPG
[2] https://www.thunderbird.net/es-ES/
[3] https://enigmail.net/index.php/en/
[4] https://www.wireshark.org/
[5] https://www.gnupg.org/
[6] https://www.enigmail.net/index.php/en/user-manual
[7] https://www.wireshark.org/docs/wsug_html_chunked/
[8]https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf