Protocolo SSL

En este laboratorio, investigaremos el protocolo SSL y en concreto en los Registros SSL enviados a través de una conexión TCP.

## Sesión SSL

En esta práctica utilizaremos el archivo de traza ssl-ethereal-trace-1.

Es importante tener en cuenta que una trama Ethernet puede contener uno o más registros SSL. (esto es muy diferente de HTTP, para el cual cada trama Ethenet contiene o un mensaje HTTP completo o una porción del mensaje HTTP.) Además, un registro SSL puede no encajar en un frame necesitándose varios frames para enviar el registro.

Responda a las siguientes preguntas:

1. Para cada una de las primeras 8 tramas Ethernet, especifique la fuente de la trama (cliente o servidor), determine el número de registros SSL que se incluyen en el frame, y enumere los tipos de registros SSL que se incluyen en el frame.

2. Cada uno de los registros SSL comienza con los mismos tres campos (con posiblemente diferentes valores). Uno de estos campos es "tipo de contenido" y tiene una longitud de un byte. Listar los tres campos y sus longitudes.

## ClientHello Record

3. Expanda el registro de ClientHello. (si su rastreo contiene múltiples ClientHello, expanda el frame que contiene el primero.) ¿Cuál es el valor del tipo de contenido?

4. ¿El registro de ClientHello contiene un nonce ("desafío")? Si es así, ¿Cuál es el valor del desafío en notación hexadecimal?

5. ¿El registro de ClientHello anuncia los cifrados qué soporta? Si es así, en el primer conjunto listado, ¿cuáles son el algoritmo de clave pública, el algoritmo de clave simétrica y el algoritmo hash?

## ServerHello Record

6. Localice el registro ServerHello SSL. ¿Este registro especifica un cifrado elegido? ¿Cuáles son los algoritmos elegidos?

7. ¿Este registro incluye un “nonce”? Si es así, ¿cuál es su longitud?

8 - ¿Incluye el registro un ID de sesión?

9. ¿Este registro contiene el certificado, o está el certificado incluido un registro aparte? ¿El certificado encaja en una sola trama Ethernet?

Client Key Exchange Record:

10. Localice el registro de intercambio de claves del cliente. ¿Este registro contiene un pre-master secreto? ¿El secreto está encriptado? ¿Si es así, cómo? ¿Cuál es la longitud del secreto cifrado?

Change Cipher Spec Record (sent by client) and Encrypted Handshake Record:

11. Localice y muestre el Change Cipher Spec Record enviados por el cliente y por el servidor indicando la diferencia entre uno y otro

Application Data

12. Respecto del cifrado de datos identifique si losregistros que contienen los datos de la aplicación incluyen un MAC (Message Authentication Code).