Enunciado.pdf

Juandf03

Seguridad de la Información

3º Grado en Ingeniería Informática

Escuela Técnica Superior de Ingeniería Informática
Universidad de Málaga

Curso: 2019-2020

RELACIÓN DE EJERCICIOS:

1. (**8 puntos**) *Negociación en el protocolo TLS*

   El objetivo de esta práctica es analizar, a través de la herramienta Wireshark, el intercambio de datos entre un cliente y un servidor cuando se utiliza el protocolo TLS.

   Para ello, el alumno debe analizar varias tramas correspondientes al acceso a varias páginas web, y responder para cada web a las siguientes preguntas:

   • ¿Cuándo se procede con el handshake y la fase de conexión?
   • ¿Qué versión de TLS se utiliza?
   • En la parte del cliente, ¿en qué trama se puede ver las suites de cifrado que soporta el cliente?
   • ¿Qué suite de cifrado se acepta finalmente para el proceso de conexión?
   • ¿En qué trama se envía el certificado digital del servidor? NOTA: No responder esta pregunta para la web (b)
   • ¿El servidor se autentica al cliente? ¿Y el cliente al servidor?

   Además de la respuesta textual, cada pregunta debe ir acompañada de una captura de pantalla.

   Las tramas que el alumno debe analizar son las siguientes:

   a. (**5 puntos**) Trama MENEAME (https://www.meneame.net)
   b. (**3 puntos**) Trama TLS13_TEST (https://tls13.pinterjann.is/)

1. (**2 puntos**) *TLSv1.3 (RFC 8446)*

   Hemos podido observar que una de las webs mencionadas arriba utiliza TLSv1.3. En TLS v1.3, el proceso de negociación es distinto al seguido en TLSv1.2.

   La tarea del alumno es, utilizando la captura de la trama del apartado 1.b, y utilizando los recursos disponibles online (como la web https://tls13.ulfheim.net), responder a las siguientes preguntas:

   • Explica con tus palabras cual es la principal diferencia entre TLS v1.2 y TLS v1.3 desde el punto de vista del handshake inicial.
   • ¿En qué momento aproximado se envía el certificado digital del servidor?