



VÍDEO intypedia009es

LECCIÓN 9: INTRODUCCIÓN AL PROTOCOLO SSL

EJERCICIOS

AUTOR: Dr. Alfonso Muñoz Muñoz

Dr. Ingeniero de Telecomunicación. Universidad Politécnica de Madrid
R&D Security Researcher. T>SIC Group – UPM

EJERCICIO 1

El protocolo SSL garantiza:

- a) confidencialidad e integridad de los datos
- b) autenticidad
- c) ataques Man in the middle
- d) confidencialidad, integridad y autenticidad

EJERCICIO 2

SSL y TLS se diferencian en:

- a) el nivel físico en el que se utiliza cada protocolo
- b) el volumen de datos que pueden proteger
- c) TLS mejora SSL en la protección a diversos ataques
- d) son idénticos

EJERCICIO 3

El protocolo SSL handshake protocol permite:

- a) definir la forma de encapsular los datos transmitidos entre cliente y servidor
- b) configura las claves para un cifrado tipo one time pad
- c) permite negociar los parámetros de seguridad necesarios para establecer una comunicación segura entre cliente y servidor
- d) que los clientes web no usen algoritmos de cifrado vulnerables

EJERCICIO 4

SSL/TLS Record Protocol permite:

- a) el intercambio de claves de sesión para el cifrado de una comunicación
- b) definir la forma de encapsular los datos transmitidos entre cliente y servidor
- c) almacenar las claves de sesión empleadas para garantizar la integridad de los datos enviados
- d) al protocolo SSL handshake utilizar claves RSA de 1024 bits

EJERCICIO 5

El protocolo SSL/TLS protege de los ataques MiTM en el acceso a la banca online:

- a) siempre y cuando un cliente web tenga la garantía que el certificado digital recibido del servidor web es "válido"
- b) independientemente de la naturaleza del certificado que identifica al servidor
- c) SSL no protege de los ataques MiTM
- d) siempre que un usuario introduzca la url del banco en un buscador web para confirmar que es la url correcta

RESPUESTAS

1. d
2. c
3. c
4. b
5. a

Madrid, España, julio de 2011

<http://www.intypedia.com>

<http://twitter.com/intypedia>

