UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola d'Enginyeria de Telecomunicació
i Aeroespacial de Castelldefels

Nombre y Apellidos: _____

Seguretat en Xarxes. AD2

Ejercicio 1 (4.5 puntos)

Utilizando la Autoridad de Certificación y el OCSP responder que ya tienes creados:

1. Emite un certificado válido para un servidor https y configura el servidor para que use dicho certificado. El campo Common Name (CN) del certificado debe ser AD2server_tu_nombre.

Si no lo has hecho previamente, guarda tu AC como autoridad de confianza en el navegador y conéctate al servidor https (asegúrate de que el OCSP responder esté funcionando)

2. Sube un pantallazo de la ventana de tu navegador en la que se vea claramente el certificado del servidor que has creado.

Emite un certificado para un cliente TLS, con common name AD2client_tu_nombre. Instala dicho certificado en el navegador con su correspondiente clave privada(.p12 container). Conéctate de nuevo al servidor https desde el navegador.

3. Sube un pantallazo que muestre la identificación del usuario que pide el navegador (isolicitando que escojas un certificado).

Revoca el certificado del cliente con tu AC.

4. Conéctate de nuevo al servidor https y comprueba que no se puede establecer la conexión. Sube un pantallazo en el que se vea que se ha realizado una consulta al servidor OCSP y su respuesta.

5. Sube el fichero index.txt de tu AC.

Ejercicio 2 (3.5 puntos)

Implementa un ataque ARP poisoning, y, a continuación, un MITM TLS cuando la víctima se conecta a https://www.instagram.com. Usa tu apellido como username y 2023 como password.

Sube un pantallazo que muestre las credenciales de la víctima interceptadas por mitmproxy.

Ejercicio 3 (2 puntos)

Usando las 2 MVs, se pide configurar un Local Port Forwarding, usando el puerto local 3000 que redirija las conexiones https al servidor www.google.com a través de un túnel ssh.

Se pide subir a Atenea:

- Un pantallazo con el comando ssh utilizado, y con la URL que usáis en el navegador para redireccionar la conexión TLS a través del túnel SSH.
- Un pantallazo de wireshark, en el que se vea que la sesión TLS con el servidor se establece desde el servidor SSH.