Seguridad en Redes
Practica 4.2

David Antuña Rodríguez
Javier Carrión García

1 Configuración de HTTPS

La conexión tiene las siguientes propiedades.

- TLS versión 1.1
- Encriptación: AES_128_CBC
- Autenticación: SHA1
- Intercambio de clave: ECDHE_RSA

El cliente y el servidor realizan el handshake típico, en el último paso el servidor le extiende un ticket de sesión al cliente.

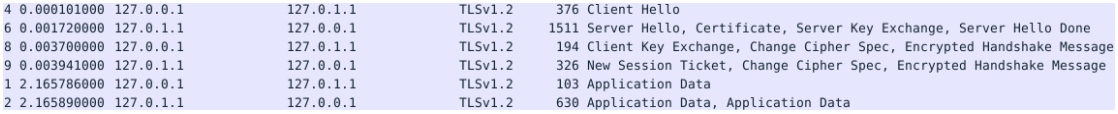

Figure 1.1 : Acuerdo TLS

El handshake es idéntico al anterior salvo que en el saludo del servidor también ha enviado la clave.

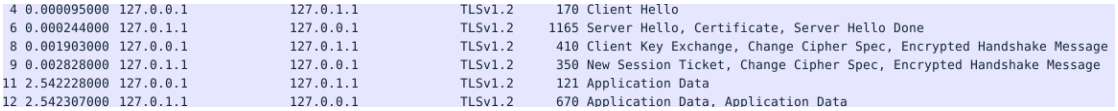

Figure 1.2 : Acuerdo TLS con -cipher

Se emplea el algoritmo que hemos especificado en la orden, el cliente lo envia en el Hello.

Figure 1.3 : Algoritmo elegido

El cliente envia el id de sesión en el saludo, primer mensaje, ahora tan solo se necesitan 3 mensajes para crear la conexión, se elimina el mensaje del servidor que envia el ticket de sesión.

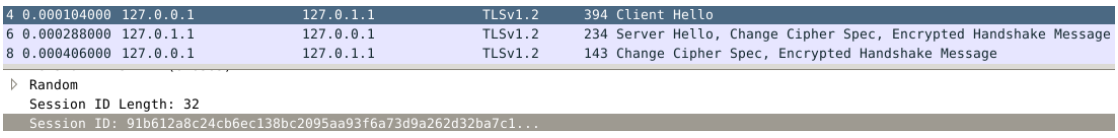

Figure 1.4 : Acuerdo TLS de la sesión almacenada

2 Autenticación del cliente mediante certificado

El handshake ocurre de forma similar pero tras el saludo del servidor el cliente envia su certificado en conjunto con lo que ya enviaba.

4	0.000130000	127.0.0.1	127.0.1.1	TLSv1.2	376	Client Hello
6	0.001157000	127.0.1.1	127.0.0.1	TLSv1.2	2670	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
8	0.005011000	127.0.0.1	127.0.1.1	TLSv1.2	2476	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
9	0.005461000	127.0.1.1	127.0.0.1	TLSv1.2	1334	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
11	6.572064000	127.0.0.1	127.0.1.1	TLSv1.2	112	Application Data
12	6.572159000	127.0.1.1	127.0.0.1	TLSv1.2	630	Application Data, Application Data

Figure 2.1 : Mensajes obtenidos en Wireshark