

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.

4 0.000101000	127.0.0.1	127.0.1.1	TLSv1.2	376 Client Hello
6 0.001720000	127.0.1.1	127.0.0.1	TLSv1.2	1511 Server Hello, Certificate, Server Key Exchange, Server Hello Done
8 0.003700000	127.0.0.1	127.0.1.1	TLSv1.2	194 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9 0.003941000	127.0.1.1	127.0.0.1	TLSv1.2	326 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1 2.165786000	127.0.0.1	127.0.1.1	TLSv1.2	103 Application Data
2 2.165890000	127.0.1.1	127.0.0.1	TLSv1.2	630 Application Data, Application Data

Figure 1.1 : Acuerdo TLS

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

4 0.000095000	127.0.0.1	127.0.1.1	TLSv1.2	170 Client Hello
6 0.000244000	127.0.1.1	127.0.0.1	TLSv1.2	1165 Server Hello, Certificate, Server Hello Done
8 0.001903000	127.0.0.1	127.0.1.1	TLSv1.2	410 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9 0.002828000	127.0.1.1	127.0.0.1	TLSv1.2	350 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
11 2.542228000	127.0.0.1	127.0.1.1	TLSv1.2	121 Application Data
12 2.542307000	127.0.1.1	127.0.0.1	TLSv1.2	670 Application Data, Application Data

Figure 1.2 : Acuerdo TLS con -cipher

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

▽ Cipher Suites (2 suites)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Figure 1.3 : Algoritmo elegido

El cliente envía 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 envía el ticket de sesión.

4 0.000104000	127.0.0.1	127.0.1.1	TLSv1.2	394 Client Hello
6 0.000288000	127.0.1.1	127.0.0.1	TLSv1.2	234 Server Hello, Change Cipher Spec, Encrypted Handshake Message
8 0.000406000	127.0.0.1	127.0.1.1	TLSv1.2	143 Change Cipher Spec, Encrypted Handshake Message

▷ Random

Session ID Length: 32

Session ID: 91b612a8c24cb6ec138bc2095aa93f6a73d9a262d32ba7c1...

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