Manual del programa corrector de prácticas C3P0

Práctica 3 - Protocolo SSL

Oscar Delgado

Este documento describe el uso y características principales del corrector de la práctica 3, en la que es necesario trabajar con el protocolo SSL, añadiendo seguridad a las comunicaciones del servidor y cliente IRC creados en la práctica 1 y 2, respectivamente.

1 Uso básico

El corrector C3P0 es una aplicación nativa para Linux, que debe ejecutarse desde la línea de comandos. Para ello basta abrir una terminal del sistema y ejecutar el comando *c3po*. Para solicitar ayuda, y obtener un listado de todas las funcionalidades del programa, se debe utilizar el siguiente comando:

```
# c3po --help
```

Aunque la mayoría de las funcionalidades deberían ser autoexplicativas, en las siguientes secciones se analizarán como mayor detalle las más significativas.

Otra opción muy útil, que utilizarás a menudo en el desarrollo de la práctica, es `--verbose`, que muestra una traza de ejecución detallada de cada prueba realizada, y de la respuesta devuelta por el servidor. Esta opción puede añadirse a cualquier otra.

1.1 Servidor y puerto

Estas opciones, señalizadas con `--servidor <IP servidor>` y `--puerto <puerto servidor>`, respectivamente, sirven para indicar al corrector una dirección IP y puerto específicos sobre los que lanzar las pruebas. Por defecto, si no se indica lo contrario con estos valores, el corrector se ejecuta contra la dirección IP `127.0.0.1`, o `localhost`, y puerto `6667`.

1.2 Lista de pruebas

Con la opción `--lista-tests` el corrector muestra una lista completa de las pruebas disponibles, junto con su número de identificación, `num`, y una pequeña explicación de cada una:

```
# c3po --lista-tests
```

Si se desea mayor información sobre una prueba específica, puede utilizarse la opción `-info-test <num>`. Por ejemplo, para obtener una explicación detallada de la prueba 1, denominada `TestComandoJoin`, basta con ejecutar:

```
# c3po --info-test 1
```

1.3 Selección y lanzamiento de pruebas

Una vez informados sobre las distintas pruebas existentes, y su número de identificación, se debe utilizar la opción `--tests <rango>` para seleccionarlas y ejecutarlas. El parámetro `rango` funciona como habitualmente: es posible seleccionar valores discretos, separados por comas, rangos, separando los extremos por guiones, y, finalmente, combinar ambas opciones. Algunos ejemplos de selección son los siguientes:

```
c3po --tests 1,3,5     - Ejecuta las pruebas 1, 3 y 5
c3po --tests 1-5         - Ejecuta todas las pruebas entre 1 y 5
c3po --tests 1,3,5-8   - Ejecuta las pruebas 1, 3, 5, 6, 7 y 8
```

La siguente sección amplia la información sobre cada tipo de prueba.

2 Descripción de las pruebas

2.1 Prueba 0: Fichero de autores

Para que la bateria de pruebas pueda ejecutarse correctamente, el corrector necesita leer algunos datos del fichero de autores (`'autores.txt'`), que se ha descrito ya en el manual del corrector de la primera práctica, pero que se reproduce a continuación:

```
G-CCCC-NN-P1
NIA#Apellido1 Apellido2, Nombre
...
NIA#Apellido1 Apellido2, Nombre
```

donde *CCCC* es el número de la clase de prácticas y *NN* es el número del grupo **siempre con dos dígitos**.

2.2 Prueba 1: Certificados digitales

El objeto de esta prueba es comprobar que los certificados digitales han sido creados correctamente. Para ello, éstos deben encontrarse dentro de un directorio llamado `certs`, y, en un alarde de originalidad, denominarse `ca.pem`, `cliente.pem` y `servidor.pem` para la CA, cliente y servidor, respectivamente.

Por otro lado, el atributo *Common Name* del certificado de la CA debe ser *Redes2 CA*, *G-CCCC-NN-P1-client* para el del cliente, y *G-CCCC-NN-P1-server* para el del servidor. Así, para una pareja que asista a la clase 2363 y sea la número 8, el *Common Name* de los certificados de cliente y servidor debe ser *G-2363-08-P3-client* y *G-2363-08-P3-server*, respectivamente.

2.3 Prueba 2: Cliente-servidor ECHO

En esta prueba será necesario implementar una arquitectura básica de cliente/servidor en la que probar más fácilmente las funciones desarrolladas para el protocolo SSL.

Básicamente debe cumplir los siguientes requisitos :

- Aceptar cualquier entrada por la entrada estándar y enviarla a través del túnel SSL. El servidor debe limitarse a devolver de nuevo al cliente tal cual, sin modificar, lo que reciba. El cliente debe escribir, a su vez, por la salida estándar estos datos provenientes del servidor. Tanto cliente como servidor NO deben hacer nada más, como aceptar parámetros por la línea de comandos. Así, se deben poder invocar sin ningún parámetro adicional.

- Devolver códigos de retorno adecuados al resultado del intento de conexión: 0, si todo fue bien, -1, si hubo algún error.
- El cliente debe finalizar su ejecución cuando reciba el comando '**exit**'. Antes debe enviar al servidor el mismo comando, que también provocará su finalización ordenada.

Para que la prueba se pueda ejecutar correctamente, los binarios deben estar localizados en el directorio `echo` y denominarse `cliente_echo` y `servidor_echo`, respectivamente.

2.4 Pruebas 3 y 4: SSL

Por último, esta test comprueba el funcionamiento del cliente y servidor IRC de la práctica 1 utilizando SSL para proteger sus comunicaciones.

Para superar la prueba, se deben cumplir los siguientes requisitos :

- **Cliente**
  - Los binarios del cliente y servidor IRC deben encontrarse dentro de un directorio denominado `cliente_servidor`, y llamarse `cliente_IRC` y `servidor_IRC`, respectivamente.
  - El cliente IRC debe aceptar como parámetro de la línea de comandos la bandera `--ssldata` *`cadena`*. Con ella, NO debe lanzar el interfaz gráfico, sino únicamente establecer una conexión segura con el servidor IRC y enviar inmediatamente *cadena*.
  - El cliente IRC debe aceptar como parámetro de la línea de comandos la bandera `--port` *`puerto`*. Con ella, la conexión debe realizarse al puerto indicado en lugar del 6667 habitual.
- **Servidor**
  - El servidor IRC debe aceptar la conexión segura y esperar comandos IRC habituales, aunque no se probará funcionalidad más allá del registro inicial del usuario.
  - Debe aceptar, asimismo, como parámetro de la línea de comandos la bandera `--port` *`puerto`*. Con ella, el servidor debe escuchar en el puerto indicado en lugar del 6667 habitual.

2.5 Resumen y evaluación

Las pruebas, y algunas restricciones de formato y nombres de ejectuables y directorios, junto con sus puntuaciones, se resumen en la siguiente tabla:

Certificados	certs	ca.pem, cliente.pem, servidor.pem	2 ptos.
Cliente/servidor echo	echo	cliente_echo, servidor_echo	2,5 ptos.
Cliente/servidor IRC	cliente_servidor	cliente_IRC, servidor_IRC	1,25 + 1,25 ptos.

Formato del fichero de la práctica

El nombre de este fichero debe ser **G-CCCC-NN-P3.tar.gz**, donde *CCCC* es el número de la clase de prácticas y *NN* es el número del grupo **siempre con dos dígitos**.

Para el resto de cuestiones, se aplican las mismas normas descritas en el manual del corrector de la práctica 1.