Práctica 3. Servicios avanzados de red: *HTTP y HTTPS*

Roberto Magán Carrión
FR - GII

rmagan@ugr.es

UNIVERSIDAD DE GRANADA

Objetivos

- Introducción a la configuración de un servicio Web (HTTP) con Apache2.
- Servicios web seguros HTTPS con Apache2.

HTTP:
Escenario práctico

Entorno virtualizado

Material de prácticas

Lab37 - Isla - Virtualizado

Descripción

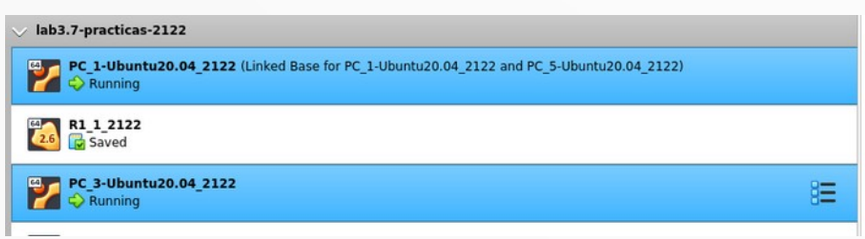
Virtualización de la Isla 1 del laboratorio 3.7 Esta herramienta se pone a disposición de los estudiantes de los grupos A2,B1,B2,C1,C2,D1,D2 para la finalización de las tareas propuestas en el laboratorio o para aquellos estudiantes con algún otro interés en practicar sobre este tipo de escenarios. Con respecto a los primeros, se habilitarán una serie de tareas en Prado para la resolución y entrega de las tareas asociadas a la Práctica 1 que NO SE EVALUARON in situ en el laboratorio 3.7 No se volverá a evaluarán aquellas tareas entregadas en Prado que ya se evaluaron in situ en el laboratorio 3.7

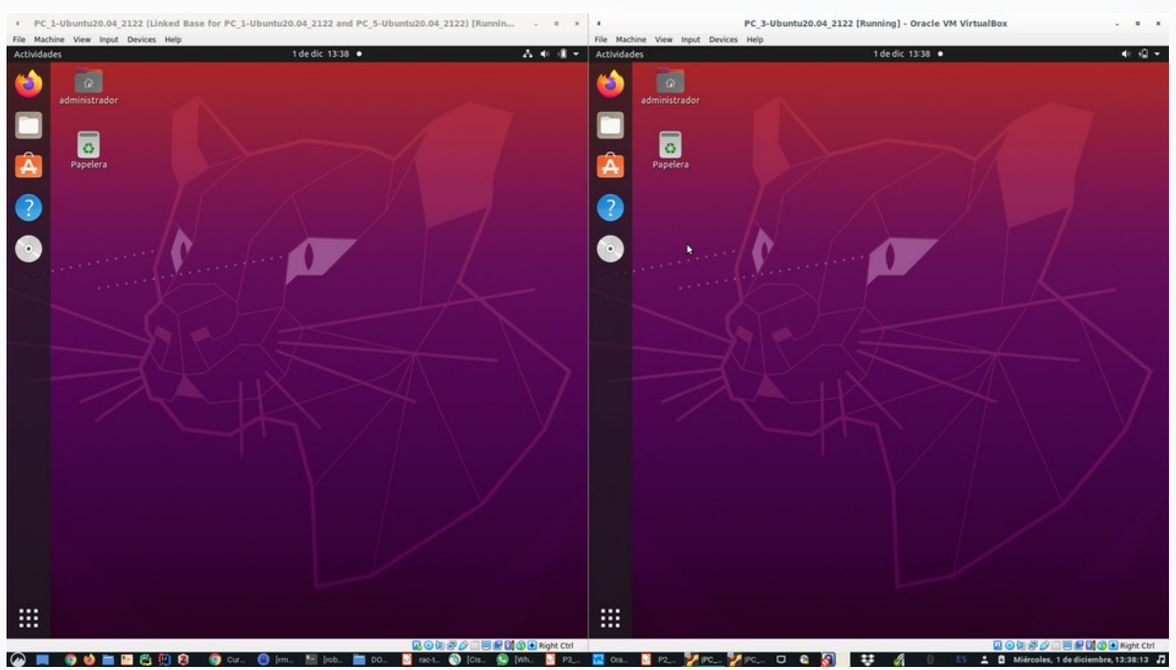
Contenido y configuración

- Elementos: PC1,PC2,PC3 y R11,R12,R13,R14,R15 Los demás elementos se deja como trabajo adicional a los alumnos interesados. Se recomienda echar un vistazo a como están configurados todos los dispositivos a nivel de máquina virtual y en el propio virtualbox así como seguir la instrucciones e indicaciones proporcionas en Seminario 1 de la asignatura.
- Configuración: Todos los PCs, además del direccionamiento e interfaces para su subred de datos y la de gestión, tienen un interfaz NAT deshabilitada (para salir a Internet) así como una interfaz solo anfitrión que da acceso a los PCs virtuales desde la máquina HOST en el rango de direcciones 192.168.59.0/24

NOTA

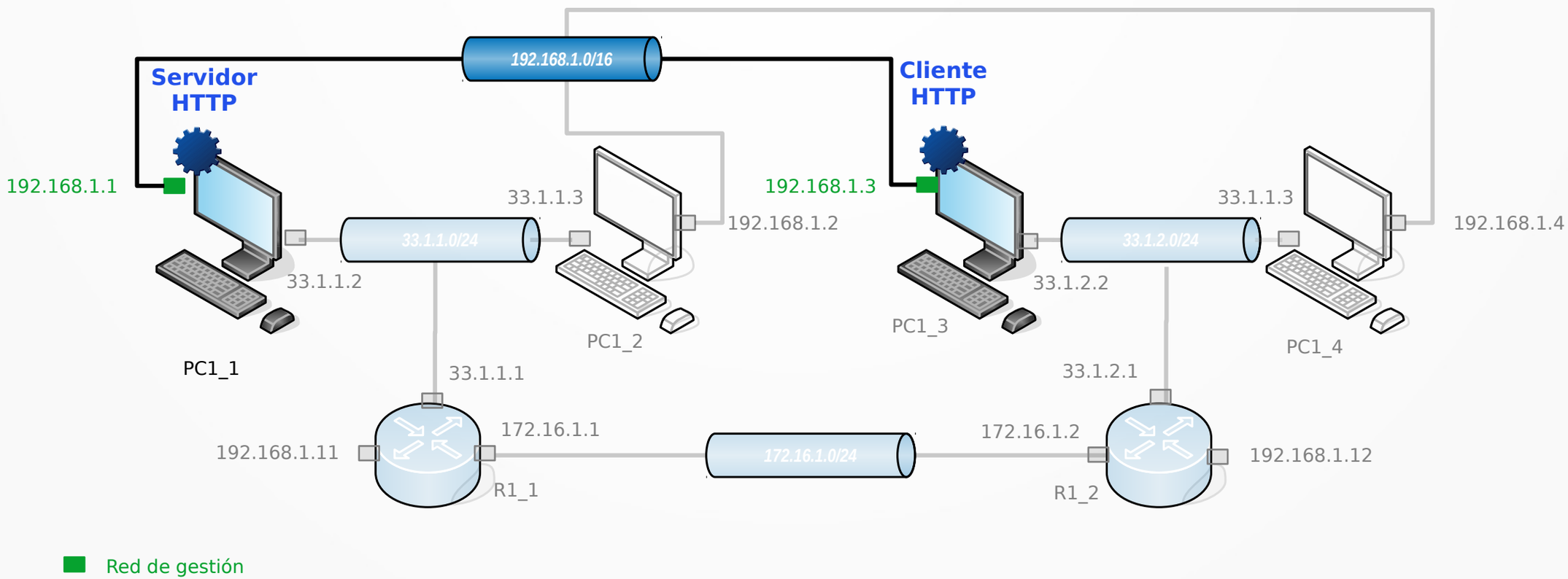
Aquellos alumnos que no pertenezcan a los grupos arriba indicados también pueden utilizar el escenario aunque es decisión del profesor el evaluar los trabajos realizados sobre este entorno virtualizado.





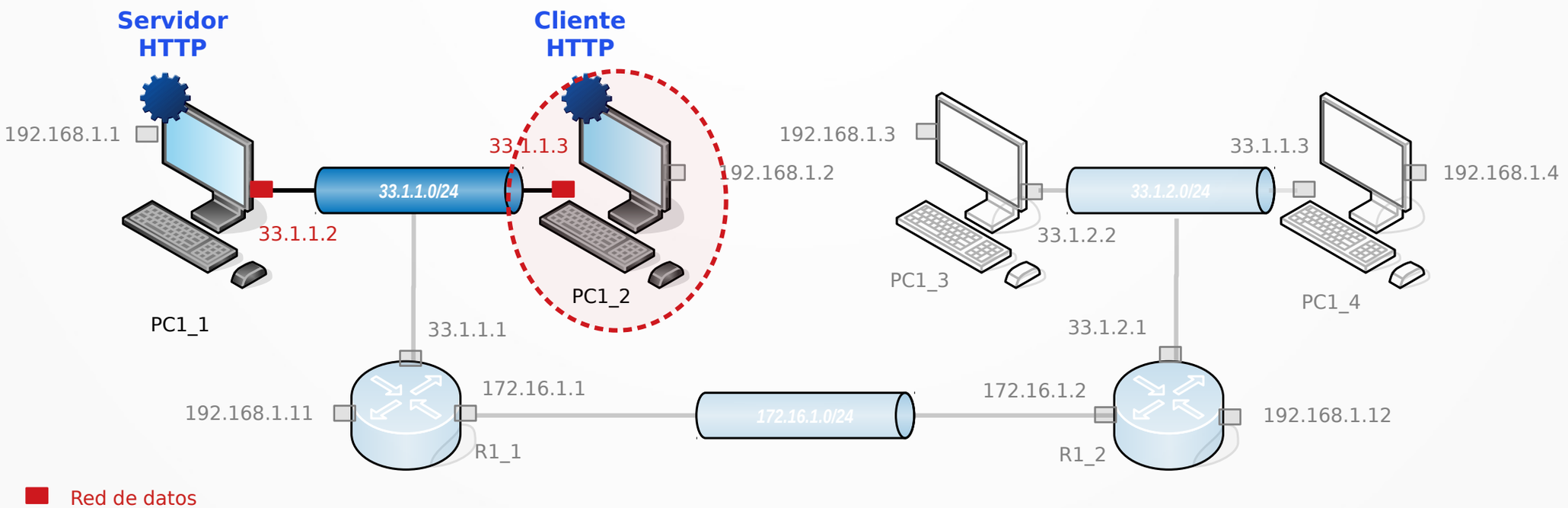
Escenario práctico

Opción 1: *utilizar la red de gestión*



Escenario práctico

Opción 2: *utilizar la red de datos*

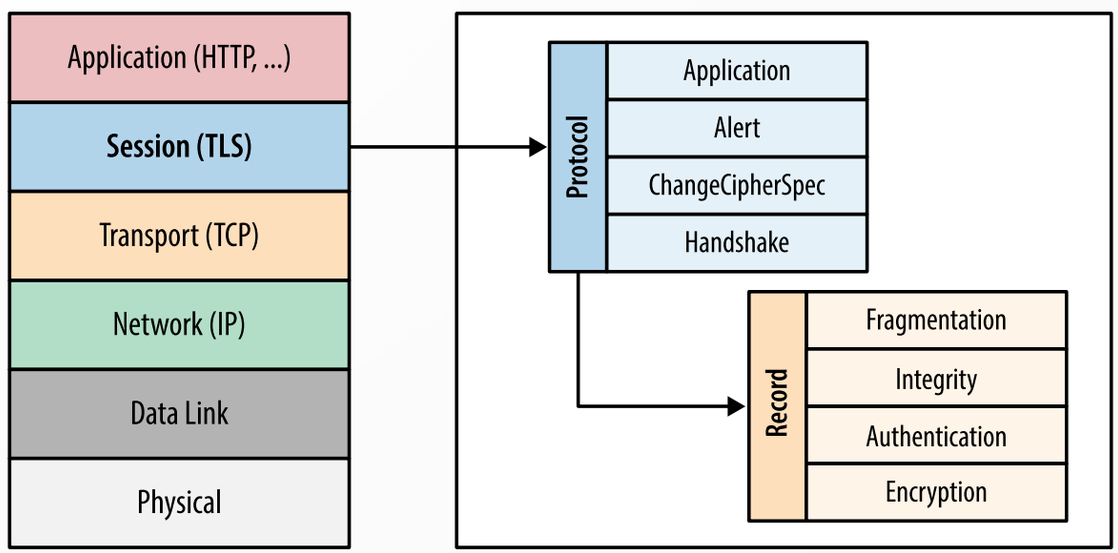


HTTPS: http-over-tls

1. TLS

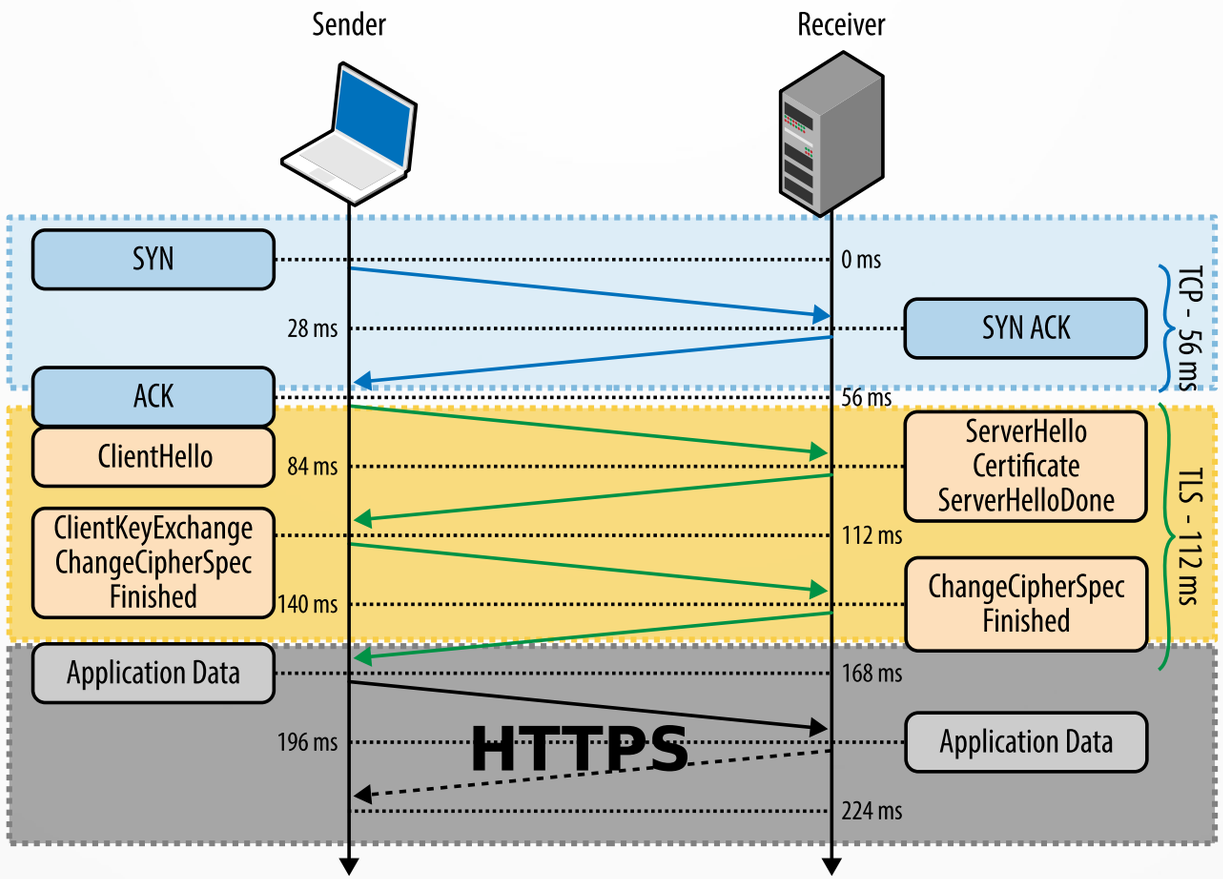
TLS (Transport Layer Protocol)

- Protocolo que ofrece a capas de aplicación:
  - i Confidencialidad
  - ii Autenticación
  - iii Integridad
- Protocolos del protocolo
  - i **Handshake**
  - ii Application
  - iii Alert
  - iv Change Cipher Spec
  - v **Record**



1. TLS

TLS handshake



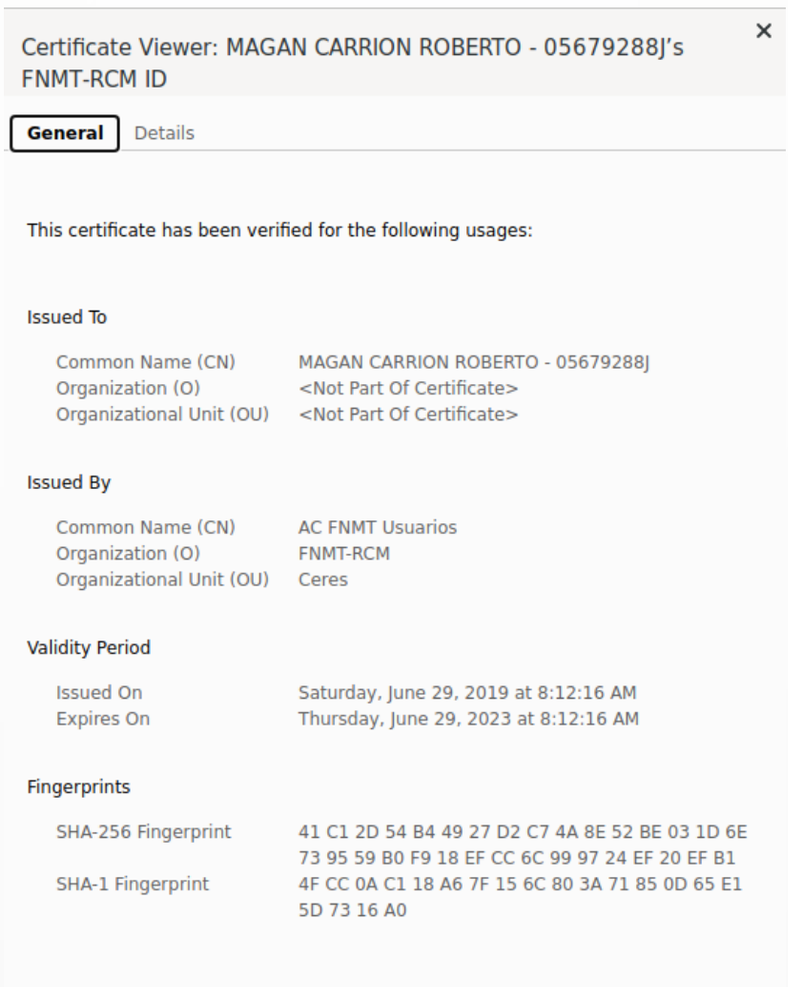
TCP Three-way handshake

Material criptgráfico, autenticación, intercambio de certificados, generación de claves de cifrado, etc.

Peticiones y respuestas de la capa de aplicación sobre una canal seguro.

1. TLS

Autenticación y certificados: X.509



Escenario práctico

Opción 1: *utilizar la red de gestión*