Práctica 4

Asegurar la granja web

José Manuel Soto Hidalgo
Dpto. Ingeniería de Computadores, Automática y Robótica
Universidad de Granada

jmsoto@ugr.es

Objetivos

- Instalar un certificado SSL para configurar el acceso HTTPS a los servidores web.
- Configurar las reglas del cortafuegos para proteger la granja web

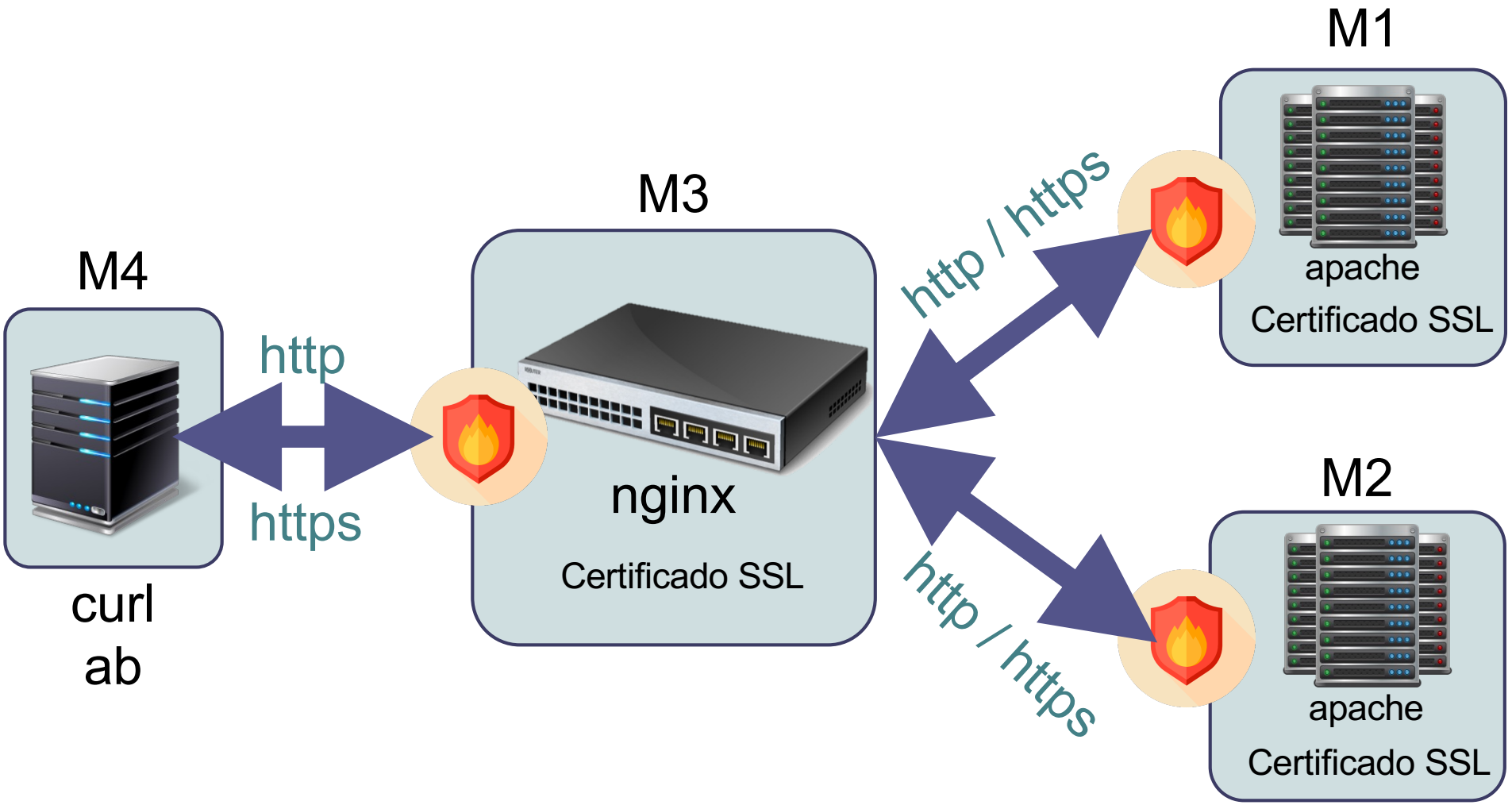
Duración: 3 sesiones

Certificado SSL autofirmado

- Protocolo SSL (Secure Sockets Layer)
  - Autenticación (certificados)
  - Integridad (firmas digitales)
  - Privacidad (encriptación)

- Un certificado SSL sirve para brindar seguridad al visitante de su página web. Es una manera de decirles a sus clientes que el sitio es auténtico, real y confiable para ingresar datos personales
  - Mediante una autoridad de certificación.
  - Crear nuestros propios certificados SSL auto-firmados usando la herramienta openssl.
  - Utilizar certificados del proyecto Certbot (software de Let's Encrypt).

Esquema general de la práctica



Instalar certificado SSL autofirmado

- En **M1** - Generar un certificado SSL autofirmado y configurar apache
  1. Activar módulo SSL de apache y crear directorio para certificados

     - Activar módulo SSL
       - `sudo a2enmod ssl & sudo service apache2 restart`

     - Crear directorio ssl para los certificados
       - `sudo mkdir /etc/apache2/ssl`

Instalar certificado SSL autofirmado

- En **M1** - Generar un certificado SSL autofirmado y configurar apache
  2. Generar certificados (openssl)
     - `sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/swap_usuarioUGR.key -out /etc/apache2/ssl/ swap_usuarioUGR.crt`

       - Datos para configurar el certificado de dominio
         - - Nombre de país: *ES*
         - - Provincia: *Granada*
         - - Localidad: *Granada*
         - - Organización: *SWAP*
         - - Organización sección: *P4*
         - - Nombre: "*usuario_ugr*"
         - - Email: "*email_ugr*"

Instalar certificado SSL autofirmado

- En **M1** - Generar un certificado SSL autofirmado y configurar apache
  3. Configurar apache con ruta de los certificados
     - Configurar archivo default-ssl con los certificados SSL

       `/etc/apache2/sites-available/default-ssl.conf`

       - Agregar la ruta de los certificados en el archivo default-ssl.conf:
         - `SSLEngine on`
         - `SSLCertificateFile /etc/apache2/ssl/swap_usuarioUGR.crt`
         - `SSLCertificateKeyFile /etc/apache2/ssl/swap_usuarioUGR.key`

     - Activar el sitio default-ssl
       - `sudo a2ensite default.ssl`
       - `sudo service apache2 reload`

Instalar certificado SSL autofirmado

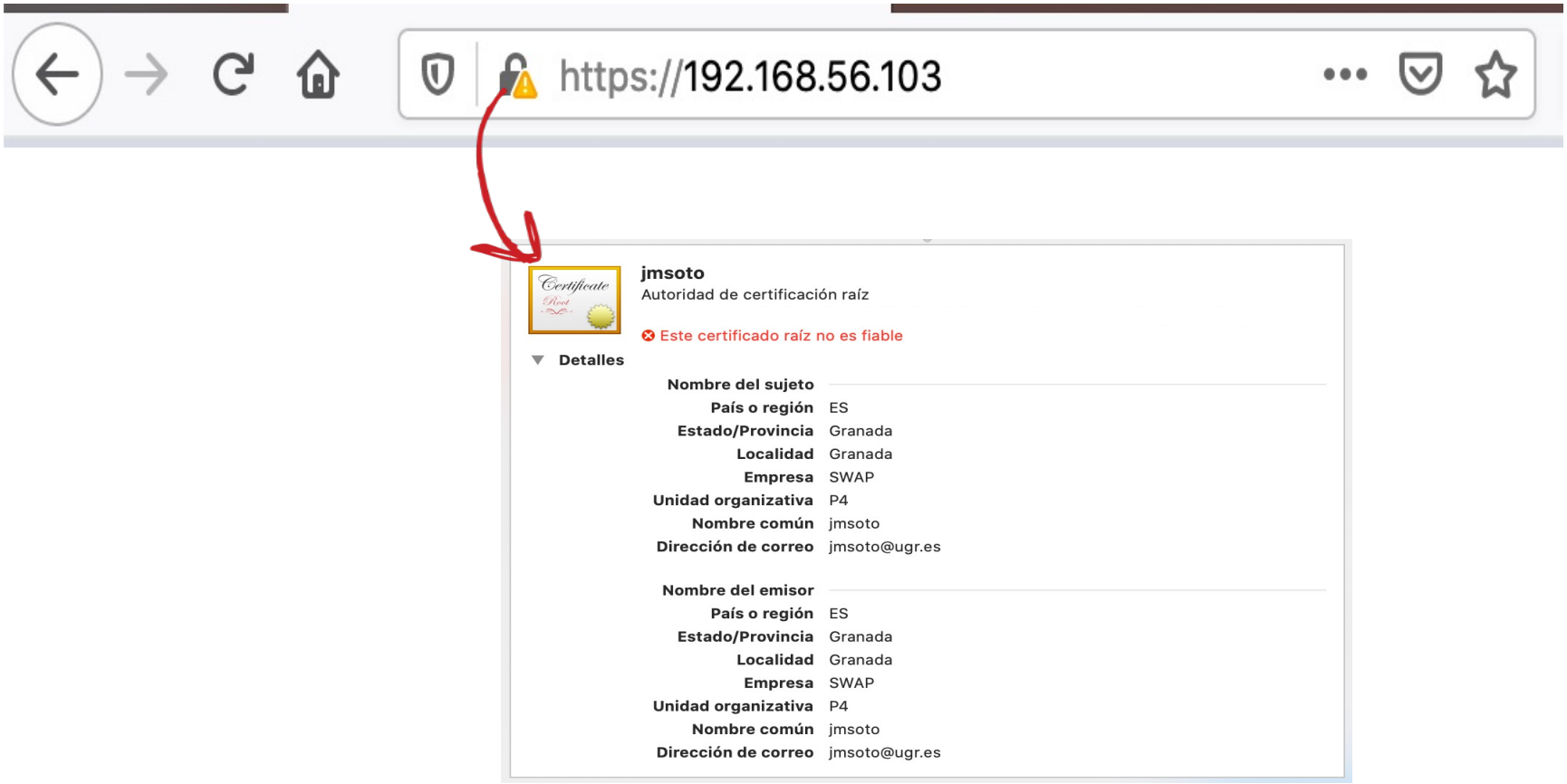
- En **M2** – *NO generar nuevos certificados*
  - Copiar certificados de M1 en M2 en /etc/apache2/ssl
    - `sudo scp swap_usuarioUGR.crt usuario@ipm2:/home/usuario/swap_usuarioUGR.crt`
    - `sudo scp swap_usuarioUGR.key usuario@ipm2:/home/usuario/swap_usuarioUGR.key`
    - `sudo mkdir /etc/apache2/ssl`
    - `sudo mv /home/usuario/apache* /etc/apache2/ssl`
  - Activar módulo SSL
  - Configurar archivo default-ssl con los certificados SSL
  - Activar el sitio default-ssl
  - Reiniciar apache

Instalar certificado SSL autofirmado

- En **M3** – *NO generar nuevos certificados*
  - Copiar certificados de M1 en M3 en /home/usuario
    - `sudo scp swap_usuarioUGR.crt usuario@ipm2:/home/usuario/ssl/swap_usuarioUGR.crt`
    - `sudo scp swap_usuarioUGR.key usuario@ipm2:/home/usuario/ssl/swap_usuarioUGR.key`
  - Configurar balanceador **nginx** con nuevo *server* con los certificados SSL y parámetros correspondientes. Añadimos a los parámetros existentes:
    - `listen 443 ssl;`
    - `ssl on;`
    - `ssl_certificate /home/usuario/ssl/swap_usuarioUGR.crt;`
    - `ssl_certificate_key /home/usuario/ssl/swap_usuarioUGR.key;`

Instalar certificado SSL autofirmado

Ya podemos hacer peticiones por HTTPS al balanceador



Configuración del cortafuegos

Un cortafuegos es un componente esencial que protege la granja web de accesos indebidos.

Actúa como el guardián de la puerta al sistema, permitiendo el tráfico autorizado o denegándolo.

Todos los paquetes TCP/IP han de pasar por el cortafuegos y decidir qué hacer.

- **IPTABLES**

Configuración del cortafuegos - IPTABLES

- Herramienta construida sobre Netfilter, una parte del núcleo Linux que permite interceptar y manipular paquetes de red.
- Se basa en establecer una lista de reglas con las que definir qué acciones hacer con cada paquete en función de la información que incluye.
- Conviene establecer como reglas por defecto la denegación de todo el tráfico y a partir de ahí definir reglas explícitamente.
    - IMPORTANTE: El orden de las reglas

Configuración del cortafuegos - IPTABLES

- Comprobar el estado del cortafuegos
  - `iptables -L -n -v`

- Parar el cortafuegos y eliminar al mismo tiempo todas sus reglas
  - `iptables -F`
  - `iptables -X`
  - `iptables -t nat -F`
  - `iptables -t nat -X`
  - `iptables -t mangle -F`
  - `iptables -t mangle -X`
  - `iptables -P INPUT ACCEPT`
  - `iptables -P OUTPUT ACCEPT`

Configuración del cortafuegos - IPTABLES

- Denegar cualquier tráfico de información
  - `iptables -P INPUT DROP`
  - `iptables -P OUTPUT DROP`
  - `iptables -P FORWARD DROP`
  - `iptables –L –n -v`

- Bloquear el tráfico de entrada
  - `iptables -P INPUT DROP`
  - `iptables -P FORWARD DROP`
  - `iptables -P OUTPUT ACCEPT`
  - `iptables -A INPUT -m state --state NEW,ESTABLISHED -j ACCEPT`
  - `iptables –L –n -v`

Configuración del cortafuegos - IPTABLES

- Abrir el puerto 22 para permitir el acceso por SSH
  - `iptables -A INPUT -p tcp --dport 22 -j ACCEPT`
  - `iptables -A OUTPUT -p udp --sport 22 -j ACCEPT`
- Abrir los puertos HTTP/HTTPS (80 y 443)
  - `iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT`
  - `iptables -A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT`
- Abrir el puerto 53 para permitir el acceso a DNS
  - `iptables -A INPUT -m state --state NEW -p udp --dport 53 -j ACCEPT`
  - `iptables -A INPUT -m state --state NEW -p tcp --dport 53 -j ACCEPT`

Configuración del cortafuegos - IPTABLES

- Manejar IPTABLES mediante el uso de script

```
# (1) se eliminan todas las reglas para hacer la configuración limpia:
iptables -F
iptables -X

# (2) establecer las políticas por defecto (denegar todo el tráfico):
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# (3) permitir cualquier acceso desde localhost (interface lo):
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# (4) permitir la salida del equipo (output) con conexiones nuevas que solicitemos, conexiones establecidas y relacionadas. Permitir la entrada (input) solo de conexiones establecidas y relacionadas:
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

Cuestiones a resolver

- El objetivo de esta práctica es configurar aspectos relativos a la seguridad de la granja web. Se debe añadir usuarioUGR en las distintas configuraciones e ilustrarlo con capturas de pantalla.

- En esta práctica **se llevarán a cabo las siguientes tareas básicas**:
  1. Crear e instalar en la máquina M1 un certificado SSL autofirmado para configurar el acceso HTTPS al servidor. Se debe comprobar que el servidor acepta tanto el tráfico HTTP como el HTTPS.
  2. Copiar al resto de máquinas servidoras (M2) y al balanceador de carga (M3) el certificado autofirmado creado en M1 (archivos .crt y .key) y configurarlas para que acepten tráfico HTTP y HTTPS.
  3. Denegar todo el tráfico entrante a las máquinas M1, M2 y M3 a excepción de tráfico HTTP y HTTPS.
  4. Configurar y documentar las reglas del cortafuegos con IPTABLES a través de un script en cada máquina con las reglas creadas.

NOTA: El correcto funcionamiento de todas las configuraciones debe mostrarse y justificarse documentalmente.

Cuestiones a resolver

- El objetivo de esta práctica es configurar aspectos relativos a la seguridad de la granja web. Se debe añadir usuarioUGR en las distintas configuraciones e ilustrarlo con capturas de pantalla.

- Como **tareas avanzadas**:
  1. Permitir SSH, PING y DNS a las máquinas M1, M2 y M3 así como el tráfico consigo misma (localhost). El resto de servicios y/o peticiones debe denegarse.
  2. Configurar M3 estableciendo reglas de iptables para que sólo M3 sea quien acepte peticiones HTTP y HTTPS mientras que M1 y M2 no acepten peticiones a no ser que sean peticiones provenientes de M3.
  3. Hacer que la configuración del cortafuegos se ejecute al arranque del sistema en todas las máquinas.
  4. **Adicional**: Crear, instalar y configurar un certificado SSL con Cerbot u otro.

NOTA: El correcto funcionamiento de todas las configuraciones debe mostrarse y justificarse documentalmente.

Normas de entrega

- La práctica se realizará de manera individual.
- Se entregará un documento *.pdf* con el desarrollo de la práctica según el guion detallando, en su caso, los aspectos básicos y avanzados realizados. Se deja a libre elección la estructura del documento el cual reflejará el correcto desarrollo de la práctica a modo de diario/tutorial. En el documento de texto a entregar se describirá cómo se han realizado las diferentes configuraciones (así como comandos de terminal a ejecutar en cada momento).
- Para la entrega se habilitará una tarea en PRADO donde se entregará el documento desarrollado siguiendo OBLIGATORIAMENTE el formato **ApellidosNombreP4.pdf**

Evaluación

- La práctica se evaluará mediante el uso de rúbrica específica (accesible por el estudiante en la tarea de entrega) y una defensa final de prácticas.
- Tiene un peso del 20% del total de prácticas
- La detección de prácticas copiadas implicará el suspenso inmediato de todos los implicados en la copia (tanto del autor del original como de quien las copió). OBLIGATORIO ACEPTAR LICENCIA EULA DE TURNITIN
  - Si la memoria supera un 40% de copia Turnitin —> suspenso
    - del 1-10% -> 0
    - del 11-20% -> -1
    - del 20-30% —> -2
    - del 30-40% —> -3
    - 40% —> suspenso
- Las faltas de ortografía se penalizarán con hasta 1 punto de la nota de la práctica.