Servidores Web de Altas Prestaciones. Práctica 4

Asegurar la granja web.

Ricardo Ruiz Fernández de Alba

30/05/2023

Índice

Introducción

Un certificado SSL garantiza la seguridad de un sitio web y transmite confianza a los visitantes al afirmar que el sitio es auténtico y confiable para ingresar datos personales. El protocolo SSL es una capa de seguridad que se sitúa sobre TCP/IP y proporciona comunicación segura entre el cliente y el servidor. Ofrece autenticación mediante certificados, integridad mediante firmas digitales y privacidad a través de encriptación.

La versión actual, SSLv3, se considera insegura, y el nuevo estándar es TLS (Transport Layer Security). Hay diferentes formas de obtener un certificado SSL e instalarlo en un servidor web para utilizar el protocolo HTTPS:

- Autoridad de certificación
- **Certificados auto-firmados**
- Certbot (antes Let's Encrypt)

Tareas

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.

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

Tarea 1. Certificado SSL

En la siguiente tarea, generaremos e instalaremos un certificado autofirmado:

Para generar un certificado SSL autofirmado en Ubuntu Server solo debemos activar el módulo SSL de Apache, generar los certificados e indicarle la ruta a los certificados en la configuración. Así pues, como root ejecutaremos en la máquina M1:

Referencias