Laboratorio 6

Deivis J. Castro

LABORATORIO: Configuración de un Servidor Web Seguro

Objetivos del Laboratorio

1. Instalar y Configurar un Servidor Web Funcional con SSL/TLS:

Los participantes instalarán y configurarán un servidor web (Apache o Nginx) en un entorno Linux, asegurándose de que el servidor esté correctamente configurado para manejar conexiones HTTPS utilizando un certificado SSL/TLS válido.

2. Asegurar el Tráfico Web Mediante HTTPS:

Los participantes implementarán una redirección automática de todo el tráfico HTTP a HTTPS en el servidor web, garantizando que todas las comunicaciones entre el servidor y los clientes estén cifradas y protegidas.

3. Verificar la Seguridad de la Conexión Web:

Al finalizar el laboratorio, los participantes comprobarán que el servidor web configurado responde correctamente a las solicitudes HTTPS, y verificarán mediante un navegador web que la conexión es segura.

Prerrequisitos

Conocimientos Básicos de Linux: Familiaridad con comandos básicos de Linux.

Entorno Virtual o Físico de Prueba: Los participantes deben tener acceso a una máquina virtual o física con una distribución de Linux instalada (por ejemplo, Ubuntu o CentOS).

Acceso a Internet: Para la instalación de paquetes y la obtención de certificados SSL.

Materiales Necesarios

Computadora o servidor con una distribución de Linux instalada. • Acceso a Internet para descargar paquetes y herramientas necesarias. • Navegador web para verificar la configuración HTTPS.

1. **INSTALACIÓN VIRTUALBOX**

a. Hyper-V BIOS

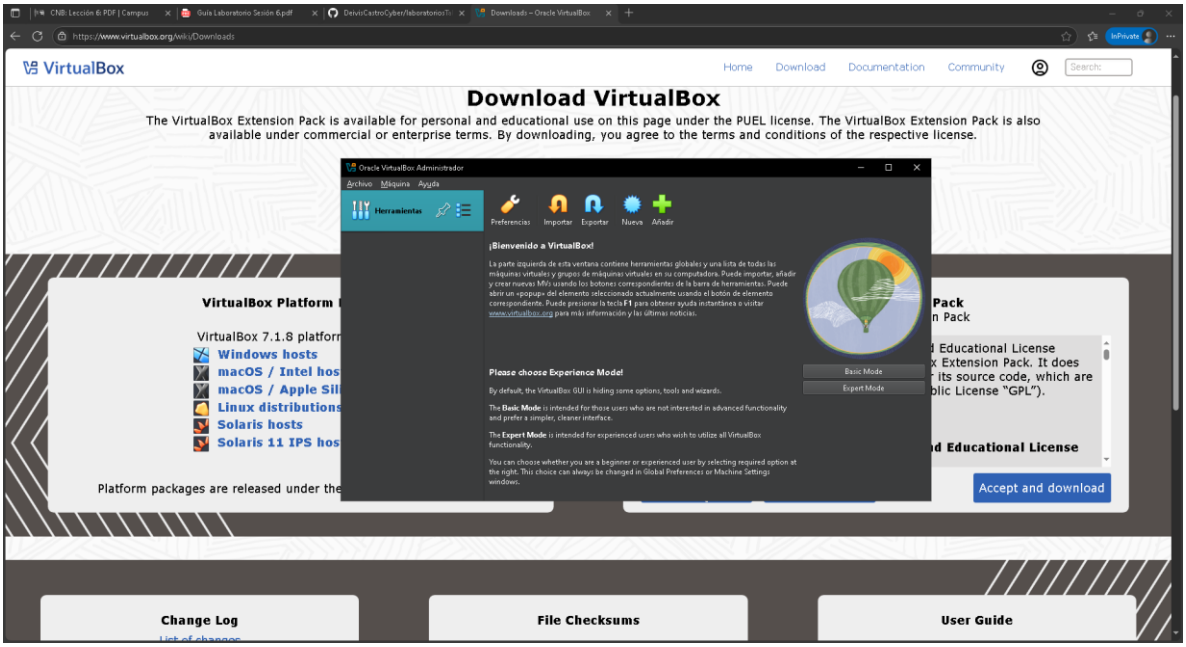
b. Microsoft Visual Redistribuible C++ 2019

c. Python -- Core Win32api

pip install pywin32

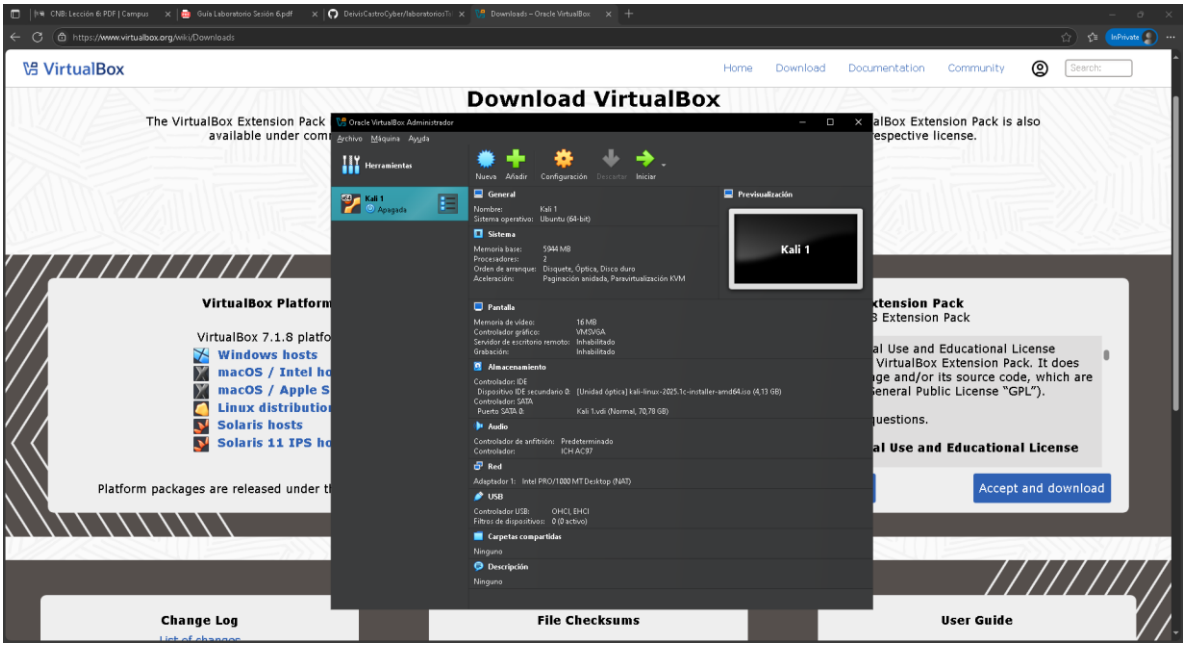
python –m pip install pywin32

VIRTUAL BOX INSTALADO

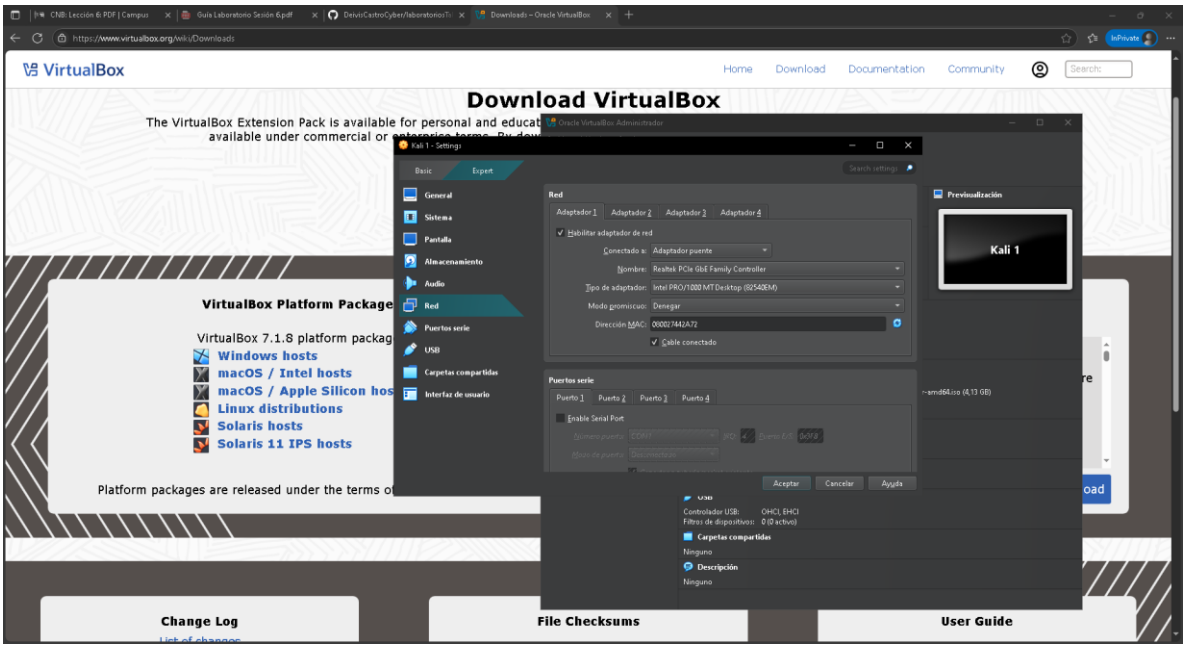


2. INSTALACION KALILINUX

a. Crear nueva máquina en Virtual Box con la ISO de Kaliinux



b. Configurar en la opción de RED de la nueva máquina la selección del adaptador puente en vez de la opción NAT.



Parte 1: Preparación del Entorno

Paso 1: Actualización del Sistema

• Comando:

bash

Copiar código

sudo apt update && sudo apt upgrade –y

• Descripción: Los participantes actualizan su sistema operativo Linux para asegurar que todos los paquetes estén al día.

Paso 2: Instalación del Servidor Web

Elección del Servidor Web:

Los participantes pueden elegir entre Apache o Nginx.

Para Apache:

• Comando:

bash

Copiar código

sudo apt install apache2 -y

• Verificación:

Accede al servidor a través de un navegador con

http://[tu_dominio_o_ip] para verificar que Apache está funcionando correctamente.

VERIFICAR APHACHE HABILITADO Y ACTIVO

Sudo systemctl enable httpd

Sudo systemctl start httpd

Sudo systmctl status apache2

Para Nginx: •

Comando: bash

Copiar código

sudo apt install nginx -y

• Verificación: Accede al servidor a

través de un navegador con http://[tu_dominio_o_ip] para verificar que Nginx está funcionando correctamente.

Parte 2: Configuración de HTTPS en el Servidor Web

Paso 3: Generación de una Solicitud de Firma de Certificado (CSR)

Comando:

bash Copiar código openssl req -new -newkey rsa:2048 -nodes -keyout [tu_dominio].key -out [tu_dominio].csr

Descripción: Los participantes generan una clave privada y una CSR para solicitar un certificado SSL. Paso 4: Obtención del Certificado SSL

Opción 1:

Let's Encrypt (Certificado Gratuito)

Comando para Apache:

bash

Copiar código

sudo apt install certbot python3-certbot-apache -y sudo certbot --apache

o Comando para Nginx:

bash

Copiar código sudo apt install certbot python3-certbot-nginx -y sudo certbot --nginx

o Descripción:

Utiliza Certbot para solicitar y obtener un certificado SSL gratuito de Let's Encrypt.

Opción 2: Certificado Comercial

Descripción: Alternativamente, los participantes pueden utilizar la CSR generada para solicitar un certificado SSL de pago y luego instalarlo manualmente.

Paso 5: Configuración del Servidor Web para HTTPS Para Apache: • Comando:

bash Copiar código

sudo nano /etc/apache2/sites-available/default-ssl.conf

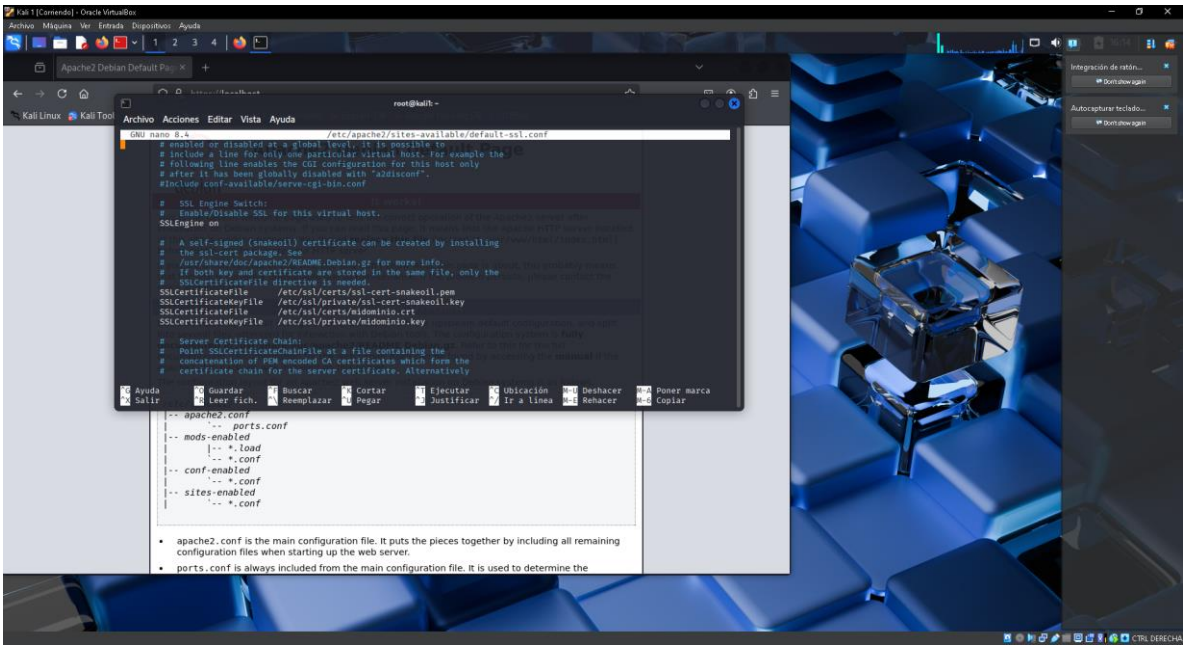
• Configuración: Configura las rutas del certificado en el archivo default- ssl.conf:

plaintext Copiar código

SSLEngine on SSLCertificateFile /etc/ssl/certs/[tu_dominio].crt

SSLCertificateKeyFile /etc/ssl/private/[tu_dominio].key

SSLCertificateChainFile /etc/ssl/certs/[ca_bundle].crt



• Habilitación y Reinicio:

bash Copiar

código sudo a2enmod

ssl sudo a2ensite default-ssl.conf

sudo systemctl restart apache2

Para Nginx:

• Comando:

bash Copiar código sudo nano /etc/nginx/sites-available/default

• Configuración: Configura las rutas del certificado en el archivo de configuración:

plaintext

Copiar código server { listen 443 ssl; server_name your_domain_or_ip;

ssl_certificate /etc/ssl/certs/[tu_dominio].crt; ssl_certificate_key /etc/ssl/private/[tu_dominio].key;

root /var/www/html; index index.html; }

• Habilitación y Reinicio:

Bash

Copiar código sudo systemctl restart nginx

Parte 3: Redirección de HTTP a HTTPS

Paso 6: Configuración de la Redirección Para Apache: • Comando:

bash Copiar código sudo nano /etc/apache2/sites-available/000-default.conf

• Configuración: Añade la redirección:

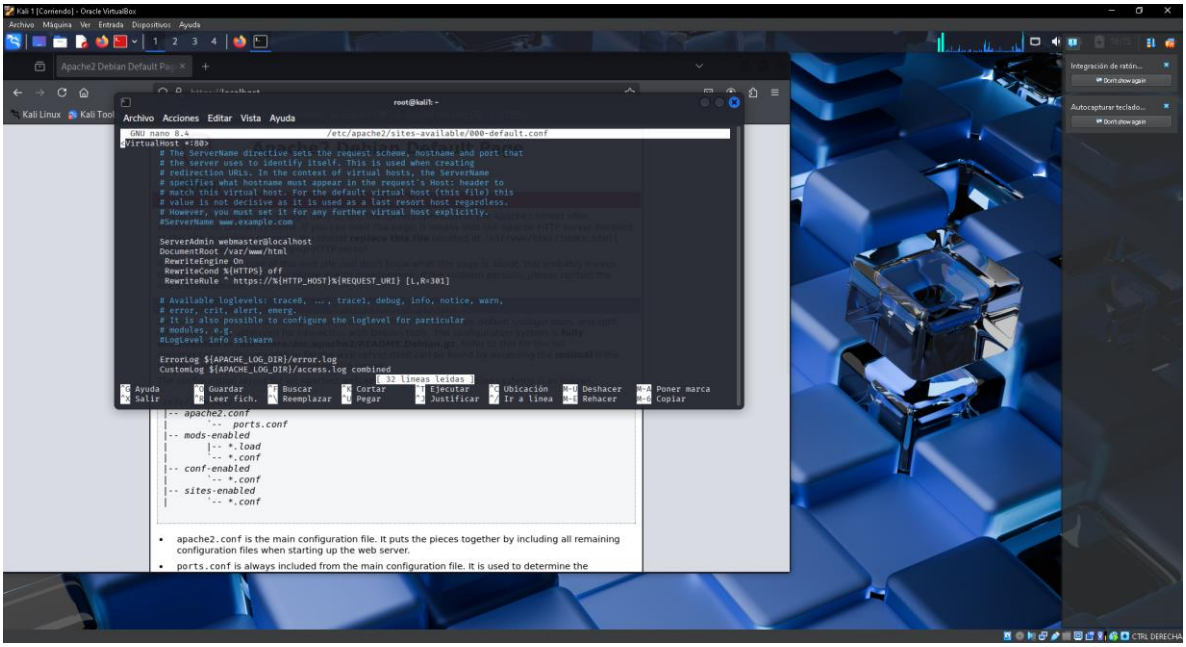
plaintext

Copiar código

RewriteEngine On

RewriteCond %{HTTPS} off

RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]



Habilitación y Reinicio:

bash Copiar código

Sudo a2enmod

sudo systemctl restart apache2

Para Nginx:

• Comando:

bash

Copiar código

sudo nano /etc/nginx/sites-available/default

Configuración: Añade la redirección:

plaintext

Copiar código

server { listen 80; server_name your_domain_or_ip; return 301 https://$host$request_uri; }

• Habilitación y Reinicio:

bash Copiar código sudo systemctl restart nginx Parte 4: Verificación

Paso 7: Verificación de la Conexión Segura

• Acción: Los participantes acceden al servidor web desde un navegador utilizando https://[tu_dominio_o_ip].

• Verificación: Comprueba que la conexión es segura y que el tráfico HTTP es redirigido correctamente a HTTPS.

Parte 5: Documentación y Presentación Paso 8: Documentación del Proceso

• Acción: Cada grupo documenta los pasos seguidos durante el laboratorio, incluyendo cualquier problema encontrado y cómo fue resuelto. • Entrega: Los participantes preparan un informe final y lo presentan al instructor para su revisión.