Ejercitación: Conexión a un servidor Ubuntu Server en VirtualBox utilizando Telnet y SSH

Índice

Parte 1: Telnet

Objetivo:

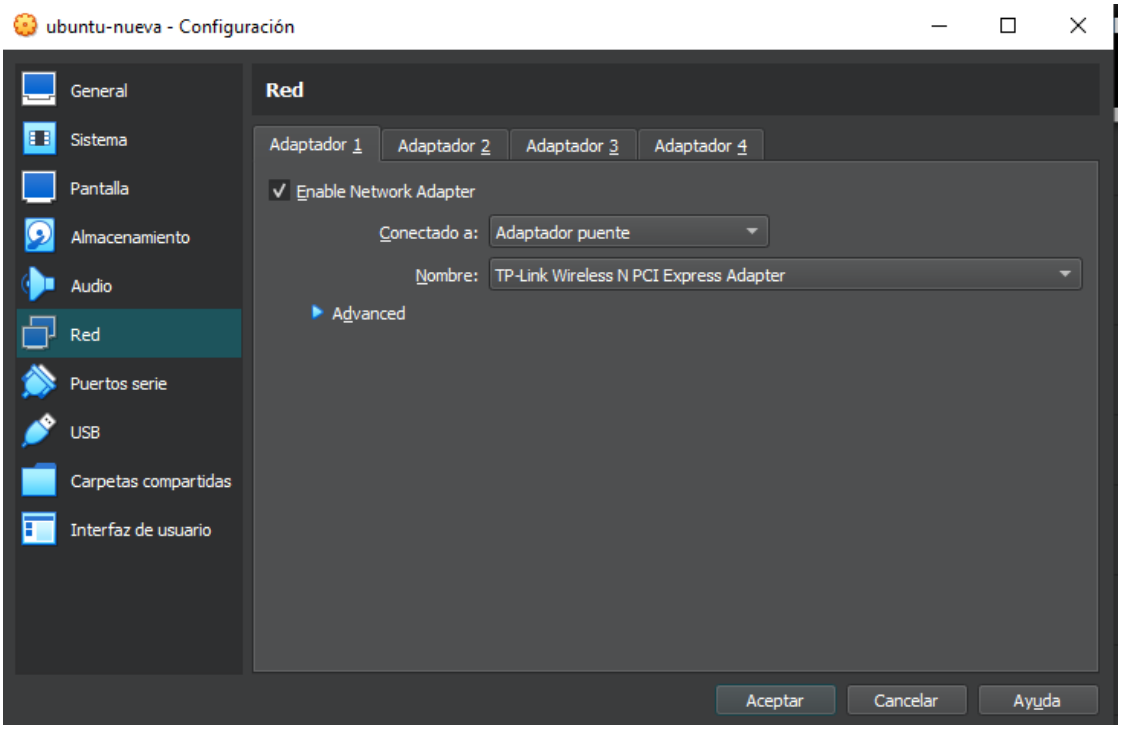
En esta parte de la ejercitación, los estudiantes aprenderán a conectarse a un servidor Ubuntu Server en VirtualBox utilizando el protocolo Telnet. Deberán utilizar un usuario común y el usuario root para establecer la conexión y crear un archivo de texto utilizando el editor nano.

Instrucciones:

Sigue los pasos a continuación para completar la parte 1 de la ejercitación:

1. Configuración del entorno (pasar al paso 2 si ya tienes instalada la MV de intro):
a) Descarga e instala VirtualBox en tu máquina.
b) Descarga una imagen de Ubuntu Server compatible con VirtualBox.
c) Crea una máquina virtual en VirtualBox utilizando la imagen de Ubuntu Server descargada.

2. Configuración de la red:
a) Configura la red de la máquina virtual en modo ***"Adaptador puente"*** para que pueda comunicarse con tu máquina host y otros dispositivos en la red.



3. Acceder como superusuario:

a) Accede como usuario root en tu máquina virtual utilizando uno de los siguientes comandos:

```
sudo su
su root
sudo -i
```

b) Crea una contraseña para el usuario root utilizando el comando:

```
passwd root
```

4. Configuración de Telnet:

a) Instala el servidor Telnet en tu máquina virtual. Abre la terminal y ejecuta el siguiente comando:

```
sudo apt-get install telnetd
```

b) Verifica que el servicio Telnet esté en ejecución. Puedes usar el siguiente comando en la terminal de tu máquina virtual:

```
sudo service openbsd-inetd status
```

o usando el comando:

```
sudo systemctl status inetd
```

Si no está en ejecución, inícialo usando

```
sudo service openbsd-inetd start
```

o usando el comando:

```
sudo systemctl start inetd
```

Aclaración: Si cuando instalas y chequeas el servicio de telnet no sale como activo, ***cambia al usuario root*** y ejecuta los comandos nuevamente (sin el sudo)

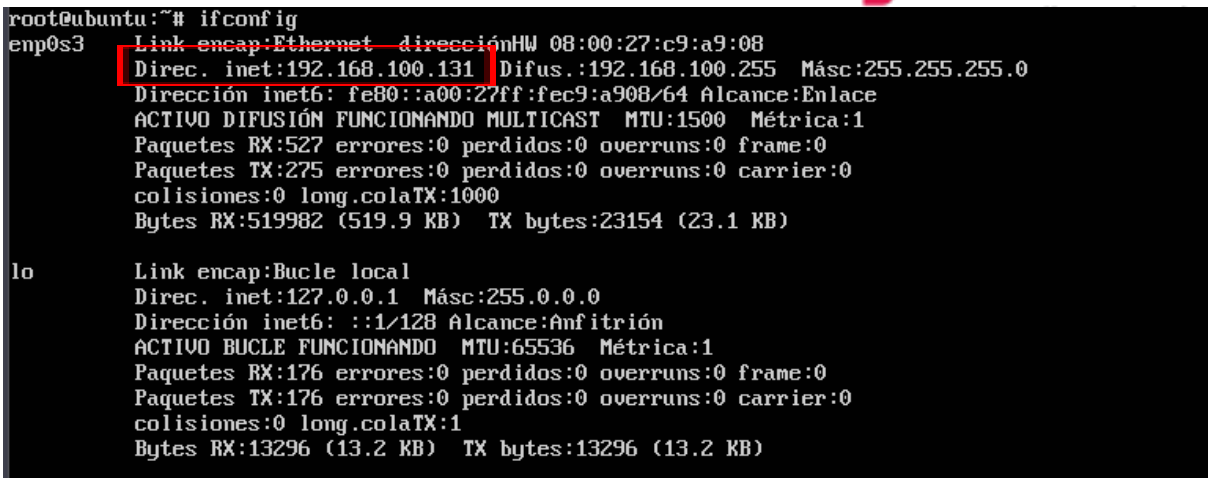
5. Conexión Telnet:

a) En la terminal de tu máquina host (si estas en Windows puedes utilizar la terminal cmd), utiliza el siguiente comando para conectarte a la máquina virtual utilizando Telnet:

```
telnet <dirección_IP>
```

Reemplaza **<dirección_IP>** con la dirección IP de la máquina virtual.

Recuerda que la dirección IP de tu máquina virtual la puedes obtener realizando el comando ifconfig en tu máquina virtual:



b) Ingresa desde la máquina host a tu VM:

Podes hacerlo con tu usuario (o root) cuando se solicite.

c) Ingresa la contraseña correspondiente cuando se solicite.

d) Una vez conectado, crea un archivo de texto utilizando el editor nano con el siguiente comando:

```
nano archivo.txt
```

e) Escribe "Hola, me conecté por Telnet" en el archivo.

f) Guarda el archivo y cierra el editor nano.

g) Verifica que el archivo se haya creado correctamente.

¡Felicidades! Has completado la parte 1 de la ejercitación de conexión a un servidor Ubuntu Server en VirtualBox utilizando el protocolo Telnet. Ahora puedes practicar y explorar diferentes configuraciones y comandos en tu máquina virtual utilizando Telnet.

Parte 2: SSH

Objetivo:

En esta parte de la ejercitación, los estudiantes aprenderán a conectarse a un servidor Ubuntu Server en VirtualBox utilizando el protocolo SSH. Deberán utilizar un usuario común y el usuario root para establecer la conexión y crear un archivo de texto utilizando el editor nano.

Instrucciones:

Sigue los pasos a continuación para

completar la parte 2 de la ejercitación:

1. Configuración del entorno:
a) Descarga e instala VirtualBox en tu máquina.
b) Descarga una imagen de Ubuntu Server compatible con VirtualBox.
c) Crea una máquina virtual en VirtualBox utilizando la imagen de Ubuntu Server descargada.

2. Configuración de la red:
a) Configura la red de la máquina virtual en modo "Adaptador puente" para que pueda comunicarse con tu máquina host y otros dispositivos en la red.

3. Configuración de SSH:
a) Asegúrate de que el servidor SSH esté instalado en tu máquina virtual. Durante la instalación de Ubuntu Server, se te ofrecerá la opción de instalar OpenSSH Server. Asegúrate de seleccionar esa opción.
Puedes chequear si el paquete de OpenSSH server está instalado utilizando el comando:

```
dpkg -l openssh-server
```

Si el paquete está instalado, verás un resultado como este:

```
ii  openssh-server   1:7.9p1-10ubuntu0.1  amd64  secure shell
(SSH) server, for secure access from remote machines
```

Si el paquete no está instalado, puedes instalarlo utilizando el gestor de paquetes:

```
sudo apt-get install openssh-server
```

b) Verifica que el servicio SSH esté en ejecución. Puedes usar el siguiente comando en la terminal de tu máquina virtual:

```
sudo service ssh status
```

Si no está en ejecución, inícialo usando

```
sudo service ssh start
```

4. Conexión SSH:

a) En la terminal de tu máquina host, utiliza el siguiente comando para conectarte a la máquina virtual como usuario común a través de SSH:

```
ssh usuario@<dirección_IP>
```

Reemplaza **<dirección_IP>** con la dirección IP de la máquina virtual.

b) Ingresa la contraseña del usuario común cuando se solicite.

c) Una vez conectado, crea un archivo de texto utilizando el editor nano con el siguiente comando: `nano archivo.txt`.

d) Escribe "Hola, me conecté por SSH" en el archivo.

e) Guarda el archivo y cierra el editor nano.

f) Verifica que el archivo se haya creado correctamente.

¡Felicidades! Has completado la parte 2 de la ejercitación de conexión a un servidor Ubuntu Server en VirtualBox utilizando el protocolo SSH. Ahora puedes practicar y explorar diferentes configuraciones y comandos en tu máquina virtual utilizando SSH.

Parte 3: Preguntas sobre Telnet, SSH y diferencias entre ambos

Instrucciones:

Con tu grupo reflexiona sobre las siguientes preguntas relacionadas con los protocolos Telnet, SSH y las diferencias entre ellos:

Telnet:
a) Pregunta: ¿Cuáles son las ventajas y desventajas de utilizar el protocolo Telnet?
b) Instrucciones: Responde la pregunta en base a tu conocimiento y experiencia. Menciona al menos dos ventajas y dos desventajas de utilizar Telnet como protocolo de acceso remoto.

Respuesta
Ventajas:

- Telnet es relativamente fácil de implementar y usar, lo que lo convierte en una opción sencilla para establecer conexiones remotas.

- La mayoría de los sistemas operativos y dispositivos de red son compatibles con Telnet, lo que permite la comunicación entre diferentes plataformas.

Desventajas

- Telnet carece de un mecanismo de autenticación robusto. Aunque requiere un nombre de usuario y contraseña para iniciar sesión, esta información se envía sin cifrar, lo que facilita el robo de credenciales.

- Telnet carece de muchas funcionalidades avanzadas presentes en protocolos más modernos, como SSH. No permite el reenvío de puertos, túneles seguros, transferencia de archivos u otras características que son útiles en entornos de red más complejos.

SSH:
a) Pregunta: ¿Cuáles son las ventajas y desventajas de utilizar el protocolo SSH?
b) Instrucciones: Responde la pregunta en base a tu conocimiento y experiencia. Menciona al menos dos ventajas y dos desventajas de utilizar SSH como protocolo de acceso remoto.

Respuesta:
Ventajas

- El aspecto más destacado de SSH es su enfoque en la seguridad. Todos los datos transmitidos a través de una conexión SSH están cifrados, lo que garantiza la confidencialidad de la información.

- SSH utiliza un puerto específico (por defecto, el puerto 22) para establecer conexiones, lo que facilita su administración en los firewalls y mejora la seguridad al bloquear el acceso no autorizado a otros puertos.

Desventajas

- Debido a que SSH utiliza técnicas de cifrado para asegurar la comunicación, puede generar una carga computacional adicional en los dispositivos implicados. Esto puede ser un factor a considerar en sistemas con recursos limitados o en conexiones de alta velocidad que requieren un rendimiento máximo.

- Configurar correctamente SSH en los dispositivos y establecer los parámetros de seguridad puede requerir ciertos conocimientos técnicos. Esto puede ser un inconveniente para usuarios menos experimentados.

Diferencias entre SSH y Telnet:
a) Pregunta: ¿Cuáles son las principales diferencias entre SSH y Telnet?
b) Instrucciones: Responde la pregunta destacando al menos tres diferencias clave entre SSH y Telnet en términos de seguridad, cifrado de datos y características funcionales.

Respuesta:

- La diferencia más significativa entre SSH y Telnet es la seguridad. SSH proporciona un alto nivel de seguridad al cifrar todos los datos transmitidos entre el cliente y el servidor, lo que protege la confidencialidad de la información. Por otro lado, Telnet no cifra los datos, lo que significa que se transmiten en texto plano y son susceptibles a la interceptación por parte de personas no autorizadas.
- SSH ofrece métodos de autenticación más seguros y robustos, como el uso de claves públicas, autenticación de dos factores y contraseñas encriptadas. Telnet, por otro lado, se basa principalmente en el uso de nombres de usuario y contraseñas para la autenticación, que se transmiten en texto plano, lo que los hace más vulnerables a ataques de interceptación y robo de credenciales.
- SSH ofrece funcionalidades avanzadas, como el reenvío de puertos (port forwarding), la ejecución de comandos remotos, la transferencia segura de archivos (SFTP) y el acceso a través de túneles seguros. Telnet carece de estas funcionalidades y, por lo tanto, tiene un conjunto más limitado de capacidades.