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

Índice

[**Parte 1: Telnet 1**](#_ay8uvpz6f6ev)

[**Objetivo: 1**](#_v9uuma84so7i)

[**Instrucciones: 2**](#_vbkmbvjuyfcw)

[**Parte 2: SSH 3**](#_i7f0rv45qpmn)

[**Objetivo: 3**](#_vyyr53gz8ecq)

[**Instrucciones: 3**](#_e4m8tlbynehm)

[**Parte 3: Preguntas sobre Telnet, SSH y diferencias entre ambos 4**](#_4z8kowp1wiaq)

[**Instrucciones: 4**](#_43mrfeutqeyz)

# **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):**

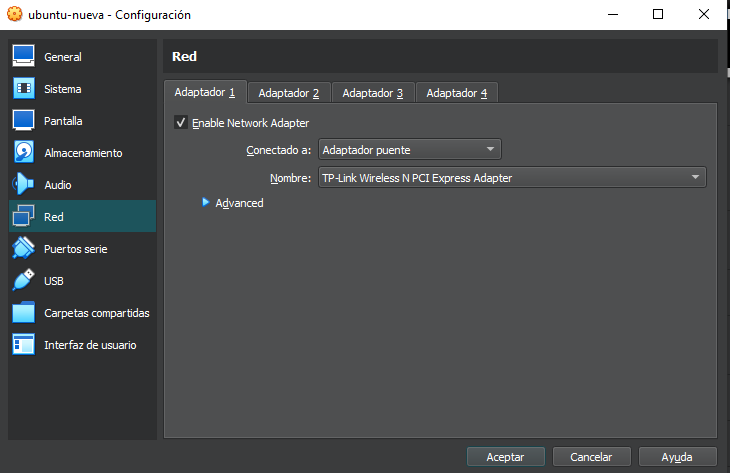
a) Descarga e instala VirtualBox en tu máquina.

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)

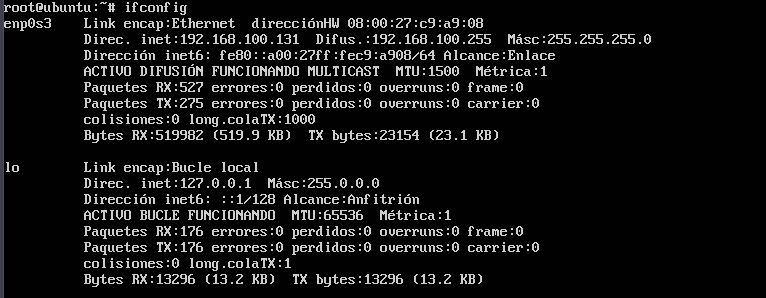
**5. Conexión Telnet:**

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?

* Ventajas:
  + Admite autenticación de usuario
  + es muy útil para enviar y recibir información
  + no se utilizan técnicas de cifrado de datos
* Desventajas:
  + no cifra los datos enviados
  + solo se muestra texto y números no muestra gráficos ni colores

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.

* ventajas:
  + permite acceder y controlar dispositivos de forma remota desde cualquier lugar
  + es un protocolo muy estándar ya que es compatible con casi cualquier sistema operativo
  + es un protocolo simple y fácil de usar
* Desventajas:
  + funciones limitadas ya que permite su uso solo a traves de lineas de comandos
  + los datos que se transmiten no van cifrados lo que genera una falta de seguridad ya que los datos pueden ser vulnerables contra ataques.

SSH:

a) Pregunta: ¿Cuáles son las ventajas y desventajas de utilizar el protocolo SSH?

* Ventajas:
  + no requiere de licencia para uso no comercial
  + ofrece múltiples servicios a través de una misma conexión
  + proporciona un cifrado sólido de datos
* Desventajas:
  + no protege a los usuarios de ataques realizados a través de otros protocolos
  + las transacciones salientes sin restricciones puede generar vulnerabilidades de seguridad

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.

* Ventajas:
  + la principal ventaja es su seguridad ya que protege todo a través de contraseña
  + utiliza varios métodos de autenticación sólida.
  + permite acceso remoto a través de la línea de comandos, sino que también admite la ejecución de aplicaciones gráficas
* Desventajas
  + maneja una configuración más compleja que telnet.
  + mayor consumo de recursos debido al cifrado de extremo a extremo y a las funciones de seguridad adicionales
  + depende de la conectividad de red ya que con una red lenta o inestable puede afectar la experiencia de uso.

Diferencias entre SSH y Telnet:

a) Pregunta: ¿Cuáles son las principales diferencias entre SSH y Telnet?

* La diferencia más notable entre SSH y Telnet radica en la seguridad. SSH proporciona una comunicación cifrada de extremo a extremo, lo que significa que todos los datos transmitidos están encriptados y protegidos contra la intercepción y la suplantación de identidad. En cambio, Telnet transmite los datos en texto plano, lo que los hace vulnerables a los ataques de captura y visualización.
* SSH ofrece una variedad de métodos de autenticación seguros, como el uso de claves criptográficas asimétricas o autenticación de contraseña. Estos métodos ayudan a garantizar la identidad del usuario y evitar el acceso no autorizado. Por otro lado, Telnet carece de una autenticación sólida y puede permitir el acceso sin restricciones a los sistemas remotos.
* SSH es más versátil en cuanto a funcionalidad en comparación con Telnet. Además de proporcionar acceso remoto a través de la línea de comandos, SSH admite la ejecución de aplicaciones gráficas y la transferencia segura de archivos (mediante el uso de SFTP o SCP). Telnet, en cambio, se limita principalmente a la emulación de terminal y el acceso a la línea de comandos
* Aunque Telnet ha sido ampliamente utilizado en el pasado, su uso ha disminuido debido a sus limitaciones de seguridad. Por otro lado, SSH se ha convertido en el estándar de facto para el acceso remoto seguro y la administración de sistemas

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.

* Seguridad y cifrado de datos:
  + SSH proporciona una comunicación segura y cifrada de extremo a extremo mientras que Telnet transmite los datos en texto plano, sin cifrar
  + Todos los datos transmitidos a través de SSH están encriptados y metoos sólidos de autenticación mientras que Telnet carece de las medidas de seguridad proporcionadas por SSH, lo que lo hace más vulnerable a ataques.
  + Telnet no proporciona ninguna medida de seguridad para proteger la confidencialidad de los datos transmitidos mientras que SSH asegura que los datos permanezcan confidenciales y protegidos contra la intercepción no autorizada.
* características funcionales:
  + SSH admite la ejecución de aplicaciones gráficas y la transferencia segura de archivos mediante SFTP (SSH File Transfer Protocol) o SCP (Secure Copy). mientras que Telnet se limita principalmente a la emulación de terminal y el acceso a la línea de comandos
  + SSH proporciona una funcionalidad más amplia y versátil para diferentes necesidades de conexión remota mientras que Telnet es un poco más limitado
  + SSH admite el reenvío de puertos, lo que permite redirigir el tráfico de red a través de una conexión SSH segura mientras que Telnet no ofrece soporte nativo para el reenvío de puertos ni para la ejecución de aplicaciones gráficas