

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

- Telnet es un protocolo simple y fácil de usar, lo que facilita la conexión y el acceso remoto a la máquina virtual. Se puede instalar fácilmente usando los comandos adecuados.
- Telnet es ampliamente compatible y está disponible en la mayoría de los sistemas operativos y plataformas.
- Telnet se puede conectar desde cualquier terminal que se tenga en el dispositivo por ejemplo git bash y powershell.

Desventajas:

- Una de las principales desventajas de Telnet es que es un protocolo no seguro.
- En cualquier momento se puede perder la conexión entre el dispositivo local y el dispositivo remoto.

- Telnet es vulnerable a ataques como el "sniffing" de red, donde los atacantes pueden interceptar y capturar paquetes de datos enviados a través de la red.

SSH:

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

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:

- SSH es una herramienta versátil que permite realizar diversas tareas de acceso remoto, como ejecutar comandos en una máquina remota.
- SSH tiene la capacidad de ejecutar comandos remotos, transferir archivos de forma segura, redireccionar puertos y crear túneles seguros.
- Una de las principales ventajas de SSH es su enfoque en la seguridad. SSH utiliza métodos de cifrado y autenticaciones fuertes para proteger las comunicaciones remotas.

Desventajas:

- Aunque SSH es altamente seguro, su configuración inicial puede ser un poco compleja para usuarios no familiarizados con él.
- Tanto el cliente como el servidor deben tener software SSH instalado y configurado adecuadamente para utilizar SSH como protocolo de acceso remoto.

Diferencias entre SSH y Telnet:

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

Instrucciones: Responde la pregunta destacando al menos tres diferencias clave entre SSH y Telnet en términos de seguridad, cifrado de datos y características funcionales.

Diferencias:

- Seguridad: SSH se enfoca en la seguridad y proporciona un medio de comunicación seguro usando mensajes cifrados, mientras que telnet carece de medidas de seguridad integradas en el acceso remoto.
- Cifrado de datos: Telnet no cuenta con cifrado de datos, lo que significa que la información viaja en texto plano de una conexión a otra, mientras que SSH cuenta con un cifrado para los datos que se transmiten entre el cliente y el servidor.
- Características funcionales: Telnet se centra en ofrecer un acceso remoto básico a través de una interfaz de línea de comandos, esto es útil en caso de realizar acciones sencillas. Por otro lado, SSH ofrece una amplia gama de características funcionales para la conexión remota.