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:

Telnet te permite conectarte y controlar dispositivos de forma remota, es simple solamente necesita de una conexión a Internet y un cliente Telnet para acceder a otros sistemas.

Desventajas:

Telnet transmite datos en texto plano, lo que significa que cualquier persona que pueda interceptar la conexión podría leer la información confidencial, como contraseñas o datos privados.
Telnet carece de transferencia de archivos.
Telnet no está diseñado para ser eficiente en redes lentas o con alto tráfico, lo que puede resultar en una experiencia de usuario lenta.
Telnet puede ser problemática en materia de estabilidad, ya que una interrupción en la conexión puede llevar a la pérdida de datos o conexiones interrumpidas.

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 utilizar tu servidor remoto de github conectado con tu computadora principal a través de una máquina virtual sin la necesidad de utilizar un token. Permite trabajar en tu computadora y sincronizar los archivos que se crean en la computadora principal con la máquina virtual.

Desventaja:

En resumen, aunque podrías teóricamente acceder a GitHub a través de una conexión Telnet desde una máquina virtual sin un token de acceso, esta práctica no es segura y no se recomienda en entornos reales de producción.

Telnet no está optimizado para redes de alta velocidad o con tráfico intenso. Por lo tanto la comunicación es bastante lenta.

SSH:

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

Ventajas:

SSH proporciona un nivel de seguridad superior al cifrar la conexión entre tu dispositivo y el servidor remoto.
SSH te permite acceder y administrar dispositivos de forma remota de manera confiable. Es capaz de transferir archivos de manera segura.

Desventajas:

Configurar SSH puede requerir algunos pasos adicionales en comparación con otros protocolos más simples. Es necesario generar y gestionar pares de claves SSH, lo cual puede resultar un poco más complejo.
Aunque SSH es seguro, si utilizas contraseñas débiles, podrías estar expuesto a ataques de fuerza bruta.

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:

SSH ofrece diferentes métodos de autenticación, incluyendo el uso de claves públicas y privadas. Esto permite una autenticación más segura y sin necesidad de transmitir contraseñas a través de la red.
No es tan difícil como se dice su configuración.

Desventajas:

Las conexiones SSH pueden interrumpirse debido a problemas de red o tiempo de espera. Esto puede resultar en una desconexión del acceso remoto y requerir una nueva conexión. Si no se guardan las sesiones o no se utilizan herramientas para gestionar las reconexiones, esto puede ser una molestia.

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

Seguridad: SSH proporciona un alto nivel de seguridad al cifrar toda la comunicación entre el cliente y el servidor, lo que protege los datos transmitidos, incluyendo contraseñas y

comandos. En cambio, Telnet transmite los datos en texto plano, lo que significa que cualquier persona que pueda interceptar la conexión puede leer la información confidencial.

Autenticación: SSH ofrece métodos de autenticación más seguros, como el uso de claves públicas y privadas, lo que elimina la necesidad de transmitir contraseñas a través de la red. Telnet, en cambio, utiliza autenticación basada en contraseñas, lo que lo hace más vulnerable a ataques de fuerza bruta y suplantación de identidad.

Funcionalidad: SSH tiene una funcionalidad más amplia que Telnet. Además de acceder a la línea de comandos remota, SSH también permite transferir archivos de forma segura y ejecutar aplicaciones gráficas a través de la reenvío de X11. Telnet, por otro lado, se centra principalmente en el acceso remoto a la línea de comandos.

Puertos: SSH utiliza el puerto 22 de forma predeterminada para las conexiones, mientras que Telnet utiliza el puerto 23. Esto puede ser relevante cuando se consideran restricciones de firewall y configuraciones de red que podrían afectar la conectividad.