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 través de líneas 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 pueden 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