Nombre: Lissette Quebrada L.

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.

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.

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.

Desarrollo:

Telnet:

- Ventajas y desventajas de utilizar el protocolo Telnet:

  Ventajas:
  1. Simplicidad: Telnet es un protocolo simple y fácil de usar, lo que facilita su implementación y configuración.
  2. Compatibilidad: Telnet es compatible con una amplia gama de sistemas operativos y dispositivos de red, lo que permite acceder a ellos de forma remota.

Desventajas:

1. Falta de seguridad: Telnet transmite datos en texto plano, lo que significa que no proporciona ningún cifrado para proteger la confidencialidad de la información transmitida. Esto hace que sea vulnerable al espionaje y a los ataques de interceptación.
2. Ausencia de autenticación robusta: Telnet carece de mecanismos de autenticación sólidos, lo que significa que es más fácil para un atacante suplantar la identidad y obtener acceso no autorizado a sistemas remotos.

SSH:

- Ventajas y desventajas de utilizar el protocolo SSH:

  Ventajas:

  1. Seguridad: SSH proporciona una capa de seguridad adicional al cifrar todos los datos transmitidos, lo que garantiza la confidencialidad y la integridad de la información. También admite autenticación sólida, como claves públicas y autenticación de dos factores.
  2. Acceso remoto seguro: SSH permite establecer conexiones seguras y cifradas a través de redes no confiables, como Internet, lo que lo hace ideal para acceder a sistemas de forma remota de manera segura.

  Desventajas:

  1. Configuración inicial más compleja: En comparación con Telnet, la configuración inicial de SSH puede ser más compleja, especialmente al generar y gestionar claves de cifrado. Esto puede requerir un conocimiento técnico más avanzado.
  2. Mayor uso de recursos: SSH utiliza técnicas criptográficas más pesadas que Telnet, lo que puede requerir más recursos computacionales en términos de capacidad de procesamiento y ancho de banda.

Diferencias entre SSH y Telnet:

- Principales diferencias entre SSH y Telnet:

  1. Seguridad: SSH utiliza cifrado para proteger la confidencialidad y la integridad de los datos transmitidos, mientras que Telnet envía información en texto plano, lo que la hace vulnerable a ataques de interceptación.
  2. Autenticación: SSH admite autenticación sólida, como claves públicas y autenticación de dos factores, mientras que Telnet carece de mecanismos de autenticación robustos.
  3. Funcionalidades adicionales: SSH ofrece funcionalidades adicionales, como la capacidad de transferir archivos de forma segura (SFTP) y ejecutar comandos remotos de forma segura, que Telnet no proporciona. SSH también permite el reenvío seguro de puertos (port forwarding) para acceder a servicios en redes remotas de manera segura.