1. Gravedad del ataque en tres escenarios:

- Confidencialidad comprometida: Si un atacante intercepta mensajes entre Alice y Bob, la información confidencial queda expuesta.
- Integridad en riesgo: Manipular mensajes entre Alice y Bob podría comprometer la integridad de la comunicación.
- Autenticación comprometida: Obtener las claves secretas compartidas permitiría la suplantación de una parte, comprometiendo la autenticación.

2. Episodio 4 de Connected y aplicaciones potenciales de la ley de Bendfor a la criptología:

- Visualización de datos y criptografía: La ley de Bendfor podría aplicarse para analizar patrones en la visualización de datos criptográficos y mejorar la comprensión de la seguridad de los sistemas.
- Análisis de comportamiento criptográfico: Podría utilizarse para identificar comportamientos inusuales o patrones en el cifrado, ayudando a descubrir posibles vulnerabilidades.

3. Modelo OSI:

- El Modelo OSI organiza las funciones de una red en siete capas, desde lo físico hasta la interacción con el usuario.

4. Ataques más conocidos a la capa 3 del modelo OSI:

- ARP poisoning: Manipulación de tablas ARP.
- Ataques de denegación de servicio (DoS): Saturación de recursos para inaccesibilidad.
- Ataques ICMP (ping flood): Sobrecarga del sistema con solicitudes de ping falsas.
- Enrutamiento malicioso: Manipulación de tablas de enrutamiento para desviar tráfico.

5. Conclusiones sobre el protocolo Diffie-Hellman:

- Diffie-Hellman es sólido, pero precauciones adicionales, como autenticación y canales seguros, son necesarias para reforzar la seguridad.