

## Actividad 10

### Ataques

1. ¿Cómo afecta la disponibilidad un ataque DoS?

Hace que se niegue el acceso a los usuarios a la red

2. ¿Cómo afecta un ataque al ancho de banda?

Inunda la red con solicitudes de tráfico malicioso, lo que consume rápidamente el ancho de banda disponible y hace que la red se vuelva inaccesible

3. ¿Cuál es la importancia de la seguridad física?

Para proteger los datos privados, evitar el robo de estos y el sabotaje a redes LAN y WAN

4. ¿Cómo prevenir un ataque DoS?

Uso de Firewall, Configurar límites de ancho de banda

5. ¿Cómo puede afectar un ataque DDoS?

Satura el ancho de banda, memoria o CPU, haciendo que el servicio se vuelva inaccesible para los usuarios legítimos.

6. ¿Qué es una VPN?

Una conexión segura y encriptada entre un dispositivo y una red privada

7. ¿Cuál es la diferencia entre una VLAN y una VPN?

VLAN segmenta la red física en subredes virtuales, mientras que VPN crea una conexión segura y encriptada entre dos redes privadas

8. ¿Cuáles son los servicios de seguridad que proporciona una VPN?

Autenticación, confidencialidad, integridad y control de acceso

9. ¿Qué es una VPN basada en firewall?

Un mecanismo de transmisión de información que aprovecha los mecanismos de seguridad del firewall incluyendo el acceso a la red interna

10. ¿Con qué protocolo se puede implementar un túnel cifrado?

SSH y SSL/TLS

11. ¿Con qué protocolo se puede generar una VPN?

PPTP, L2F, L2TP e IPsec