Actividad 11. Ataque de denegación de servicio

En seguridad informática, un **ataque de denegación de servicio**, llamado también ataque **DoS** (**Denial of Service**), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.

La gama de ataques varía ampliamente, desde inundar un servidor con millones de solicitudes para reducir su rendimiento, abrumarlo con una cantidad sustancial de datos no válidos, hasta enviar solicitudes con una dirección IP ilegítima.

En los siguientes artículos se habla sobre los **ataques de denegación de servicio**:

- ¿Qué es un ataque de denegación de servicio (DoS)?
- ¿Qué son los ataques DoS y DDoS?
- Qué es un ataque DDoS y cómo puede afectarte
- ¿Qué es un ataque DDoS (denegación de servicio distribuido)?
- ¿Qué es un ataque DDoS?

En los siguientes artículos se habla de **cómo prevenir los ataques Dos y DDos**:

- Medidas de prevención contra ataques de denegación de servicio
- ¿Cómo prevenir los ataques de denegación de servicio?
- Ataques DDoS: ¿qué son y qué puedo hacer para proteger mi empresa?

Se pide:

1. Explica que es un ataque de denegación de servicio, sus tipos y como se pueden evitar.
2. Realiza varios ataques de denegación de servicio sobre las máquinas metasploitable2 y metasploitable 3 (Windows y Linux).
3. Explica cómo se puede proteger un sistema de un ataque de denegación de servicio.