Conceptos de Seguridad en Redes

Spoofing

El **spoofing** se refiere a una técnica común utilizada por los actores de amenazas para **hacerse pasar por una fuente de confianza** con el fin de engañar, manipular o robar a su objetivo. Esta táctica explota el principio fundamental de la confianza, ya sea engañando a un sistema o a las personas para que crean que el atacante es algo que no es.

Funciona falsificando datos para parecer una fuente confiable o familiar. Por ejemplo, un atacante puede falsificar la dirección "de" en un correo electrónico, disfrazar su número de teléfono para que coincida con el de un banco, o alterar paquetes de datos en una red para que parezcan provenir de un dispositivo seguro.

Existen diversos tipos de spoofing, incluyendo:

- **Spoofing de Correo Electrónico:** Falsificación de la dirección del remitente.
- **Spoofing de IP:** Falsificación de la dirección de origen de los paquetes de datos, común en ataques de denegación de servicio.
- **Spoofing de DNS:** Redirección de usuarios a sitios web falsos.
- **Spoofing de ARP:** Envío de mensajes ARP falsificados para interceptar o manipular el tráfico de red local.

Fuente: Trend Micro. *Spoofing: qué es, tipos y cómo evitarlo.* [https://www.trendmicro.com/es_es/what-is/social-engineering/spoofing.html]

Denegación de servicio (DoS)

Un ataque de **Denegación de Servicio (DoS)** es un intento malicioso de sobrecargar de tráfico una propiedad web o un servicio para interrumpir su funcionamiento normal. El objetivo es hacer que una máquina o dispositivo no esté disponible para los usuarios a los que va dirigido.

El ataque funciona al sobrecargar o inundar una máquina objetivo con solicitudes hasta que el tráfico normal es incapaz de ser procesado, lo que provoca una denegación de servicio.

La principal diferencia entre los tipos de ataque es la fuente:

- **DoS:** Se caracteriza por utilizar una **única máquina** para lanzar el ataque.
- **DDoS (Denegación de Servicio Distribuido):** Es un tipo de ataque DoS que proviene de **muchas fuentes distribuidas**, a menudo en forma de una *botnet* (una red de ordenadores comprometidos).

Fuente: Cloudflare. *¿Qué es un ataque de denegación de servicio (DoS)?*. [https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/]

Man in the middle (MITM)

Un ataque de **Man in the middle (MITM)**, o ataque de hombre en el medio, es un tipo de ciberataque en el que un atacante se inserta secretamente entre dos entidades en un canal de comunicación para **robar o alterar datos**.

El atacante intercepta el mensaje sin el conocimiento de ninguna de las partes. El objetivo es explotar protocolos débiles basados en la web o la red para desviar el tráfico legítimo y robar información sensible, como credenciales de inicio de sesión o información financiera.

El proceso básico de un ataque MITM es:

1. La persona A envía un mensaje a la persona B.
2. El atacante de MITM intercepta el mensaje sin que A o B lo sepan.
3. El atacante puede leer, cambiar el contenido del mensaje o eliminarlo por completo, y luego reenviarlo a la persona B (o no reenviarlo).

Fuente: Fortinet. *Ataque de hombre en el medio: Tipos y ejemplos*. [https://www.fortinet.com/lat/resources/cyberglossary/man-in-the-middle-attack]