Resumen 2

Resumen de la charla: Introducción a Nmap y Metasploit

La charla presenta los fundamentos de dos herramientas esenciales en el ámbito de la ciberseguridad ofensiva: **Nmap** y **Metasploit**.

Primero se explica que **Nmap (Network Mapper)** es una herramienta utilizada para el análisis y descubrimiento de redes. Permite identificar hosts activos, puertos abiertos, servicios en ejecución y versiones de software, así como realizar detección de sistemas operativos. También se introduce la sintaxis básica y los tipos de escaneos más utilizados, como el escaneo SYN, el de versiones y el escaneo de scripts NSE.

Posteriormente, se aborda **Metasploit Framework**, una plataforma para pruebas de penetración que incluye herramientas para explotación, post-explotación y generación de payloads. Se explica la estructura de sus módulos (exploits, payloads, auxiliares, post, encoders y nops) y su uso mediante la consola `msfconsole`. La charla ejemplifica cómo aprovechar la información recolectada por Nmap para seleccionar exploits apropiados en Metasploit.

Finalmente, se recalca la importancia de usar estas herramientas de forma ética, solo con permiso, y cómo forman parte esencial del flujo profesional de pentesting: **reconocimiento** → **escaneo** → **explotación** → **post-explotación**.

Preguntas y respuestas

1. ¿Para qué se utiliza principalmente Nmap?

Respuesta: Para descubrir hosts y servicios en una red, así como para identificar puertos abiertos y obtener información de versiones y sistemas operativos.

---

2. ¿Qué es un escaneo SYN en Nmap y por qué es popular?

Respuesta: Es un escaneo “semiabierto” (`-sS`) que envía paquetes SYN sin completar la conexión TCP. Es rápido, sigiloso y consume menos recursos.

---

3. ¿Qué función cumple Metasploit Framework?

Respuesta: Es una plataforma que permite ejecutar pruebas de penetración, desde explotación de vulnerabilidades hasta tareas de post-explotación y generación de payloads.

---

4. ¿Qué relación existe entre Nmap y Metasploit en un pentest?

Respuesta: Nmap proporciona información clave sobre servicios y vulnerabilidades potenciales, que luego Metasploit puede aprovechar para seleccionar y ejecutar exploits adecuados.

---

5. ¿Qué son los módulos en Metasploit?

Respuesta: Son componentes con funciones específicas, como exploits (ataques), payloads (cargas útiles), auxiliares (escaneos y herramientas), y módulos de post-explotación.