Cuaderno de Trabajo - Taller de Nmap en Windows

# Introducción

Este cuaderno de trabajo está diseñado para acompañar el taller de Nmap en Windows. Incluye actividades prácticas, comandos sugeridos y espacio para registrar observaciones y resultados.

# Actividad 1: Mapeo de la red local

Objetivo: Identificar todos los dispositivos activos en la red local.

Comando sugerido:

nmap -sn 192.168.1.0/24

Espacio para observaciones:

# Actividad 2: Análisis de servicios

Objetivo: Detectar servicios y versiones en un host específico.

Comando sugerido:

nmap -sV 192.168.1.X

Espacio para observaciones:

# Actividad 3: Evaluación de vulnerabilidades

Objetivo: Identificar posibles vulnerabilidades usando scripts NSE.

Comando sugerido:

nmap --script vuln 192.168.1.X

Espacio para observaciones:

# Actividad 4: Simulación de roles

Objetivo: Comprender el uso ético de Nmap mediante una dinámica de roles.

Instrucciones: Dividir al grupo en 'auditores' y 'administradores de red'. Realizar un debate sobre los límites éticos y legales del escaneo de redes.

Espacio para reflexiones:

# Evaluación Individual

Responde las siguientes preguntas:

1. ¿Qué comando usarías para escanear todos los dispositivos de tu red local?

2. ¿Qué información proporciona el parámetro -sV?

3. ¿Qué precauciones éticas deben tomarse al usar Nmap?

4. ¿Qué diferencias hay entre un escaneo básico y uno agresivo?

5. ¿Qué utilidad tienen los scripts NSE en un análisis de seguridad?