



Donostia · Bilbao · Madrid · Pamplona · Almendralejo · Sevilla · Querétaro

PRUEBA EVALUACION CONTINUA

IFCT0109_CEN-SEGURETAT DELS SISTEMES D'INFORMACIÓ

MF0487_3-AUDITORÍA DE SEGURIDAD INFORMÁTICA

NOM:		CALIFICACIÓ
DNI:		
DATA:		

Descarga y completa esta prueba teórica. Una vez que hayas acabado, salva el documento en formato PDF añadiéndole tu nombre y apellidos en el título del mismo y envíalo al correo nunhes@gmail.com.

No olvides cubrir tus datos en el espacio dispuesto a tal efecto en la primera página.

Enunciado del Ejercicio Práctico

Objetivo

El objetivo de este ejercicio es practicar el uso de diversas opciones y técnicas de escaneo de Nmap para realizar una auditoría de seguridad en una red ficticia; familiarizarse con el uso de Nmap en un contexto de auditoría de seguridad y desarrollar habilidades prácticas para identificar y mitigar vulnerabilidades en una red. Los estudiantes deberán **identificar dispositivos, puertos abiertos, servicios, versiones de servicios y posibles vulnerabilidades dentro de la red.**

Escenario

Importante: Guarda capturas de pantalla de todo el proceso para documentar tu ejercicio.

- Recrea una red corporativa con al menos tres máquinas conectadas. Para lo que puedes crear 3 (o más) máquinas virtuales con SO Windows7 que puedes obtener en [este enlace](#).
- Conéctalas a una red NAT con el siguiente rango de direcciones IP 192 . 168 . 1 . 0/24
- Conecta a la red corporativa recién creada una máquina Kali Linux para realizar las operaciones de testing.

Tareas

Importante: Guarda los resultados de cada test en un archivo de texto para documentar tu ejercicio.

1. **Descubrimiento de Host:** Realiza un escaneo para identificar todos los dispositivos activos en la subred 192 . 168 . 1 . 0/24.
2. **Escaneo de Puertos Comunes:** Realiza un escaneo rápido de los puertos más comunes en todos los dispositivos descubiertos.
3. **Escaneo Completo de Puertos:** Realiza un escaneo completo de todos los puertos en uno de los dispositivos identificados en la tarea 1.
4. **Detección de Servicios y Versiones:** Identifica los servicios y versiones que corren en los puertos abiertos de un dispositivo específico.
5. **Detección de Sistemas Operativos:** Intenta determinar el sistema operativo de un dispositivo específico.

Instrucciones

1. Ejecuta cada comando en el orden sugerido, reemplazando 192 . 168 . 1 . x con la dirección IP del dispositivo específico que estás escaneando.
2. Guarda y organiza los resultados de cada escaneo en los archivos correspondientes.
3. Analiza los resultados obtenidos para identificar posibles riesgos de seguridad y realiza un reporte de tus hallazgos.
4. Evalúa las implicaciones de los descubrimientos y sugiere medidas para mitigar las posibles vulnerabilidades que hayas detectado.

Evaluación

Los estudiantes serán evaluados en base a los siguientes criterios:

1. **Precisión:** Correcta ejecución de los comandos y precisión en la identificación de dispositivos y servicios.
2. **Documentación:** Claridad y organización de los resultados almacenados en los archivos de salida.
3. **Análisis:** Calidad del análisis de seguridad y relevancia de las recomendaciones de mitigación.
4. **Comprensión:** Demostración de comprensión de las opciones y técnicas de escaneo de Nmap.

Barcelona 22-Julio-2024