THE BRIDGE

BOOTCAMP
Ciberseguridad en formato online

EJERCICIOS NESSUS

Prerrequisitos

Para realizar este ejercicio debemos contar con nuestra máquina **Kali** y la máquina **Metasploitable**. De nuevo las estableceremos en la misma red y con conexión a Internet en ambas máquinas, para ello las pondremos en **Red Nat** dentro de la misma máscara de subred.

En esta ocasión una empresa nos ha contratado para realizar una auditoría a una nueva máquina que van a implementar dentro de su red interna, para ello quieren comprobar sus vulnerabilidades. Para poder llevar a cabo el análisis debemos utilizar la herramienta Nessus.

En el contrato firmado para la realización del ejercicio de Pentesting nos han incluido la cláusula de realizar un primer escaneo en **caja negra**; y después en **caja blanca**, para así comparar los resultados.

Las credenciales que nos han otorgado son:

- **User: vagrant**
- **Pass: vagrant**

Ejercicio 1 – Nessus en Caja Negra

1. Realizar un análisis de vulnerabilidades sobre la máquina Metasploitable en modo Black Box:
    - Tipo: Basic Network Scan
    - Sin credenciales
2. Exportar informe PDF:
    - Ejecutivo: Complete List of Vulnerabilities by Host
    - Técnico: Detailed Vulnerabilities by Host.

Ejercicio 2 – Nessus en Caja Blanca

1. Realizar un análisis de vulnerabilidades sobre la máquina Metasploitable en modo Black Box:
    - Tipo: Basic Network Scan
    - Con credenciales
2. Exportar informe PDF:
    - Ejecutivo: Complete List of Vulnerabilities by Host
    - Técnico: Detailed Vulnerabilities by Host.

Ejercicio 3 – Análisis

1. Complete una tabla parecida al cuadro de abajo según los hallazgos de cada análisis.

CVSS	Black Box	White Box
Critical		
High		
Medium		
Low		
Info		


THE
BRIDGE