Universidad de La Laguna

Práctica de Laboratorio #12. Pentesting con Metasploit

En esta práctica vamos a realizar un ejercicio de lo que se conoce como **Pentesting** o test de penetración en sistemas informáticos. Se propone realizar un estudio de la herramienta Metasploit para la detección de vulnerabilidades en sistemas y servicios instalados en una red corporativa.

Ejercicios

1. Instalar una máquina virtual de Kali Linux. Esta distribución basada en Debian contiene software específico para la realización de tests de penetración. Entre ellos **Metasploit**. Por defecto, esta distro no configura la red ni arranca ningún servicio. Debemos hacerlo a mano (o configurarlo adecuadamente).
2. Como guía de trabajo, podemos utilizar el tutorial Metasploit Unleashed. Realizar una primera lectura para comprender las bases del Pentesting.
3. Preparar Kali para usar metasploit:
    - Instalar una base Debian desde una plantilla del IaaS-ULL.
    - Añadir los repositorios de Kali Linux.
    - Instalar uno de los metapaquetes de Kali Linux que contenga Metasploit. Por ejemplo, kali-linux-top10.
4. Instalar en otra máquina virtual un sistema vulnerable. Podemos utilizar Metasploitable 2 o Metasploitable 3. Tiene una guía para ejecutar Metasploitable2 en VirtualBox. En el IaaS-ULL disponen de plantillas para clonar estas imágenes.
5. Como guía pueden seguir el tutorial de Metasploit Unleashed, intentar averiguar cuantas y cuales son las vulnerabilidades del sistema vulnerable instalado.

Escribir un informe con los trabajos realizados y las vunerabilidades detectadas. El informe debe incluir una Memoria de Autorización del propietario del sistema analizado.