Escaneo

Práctica N°4

Las correcciones de las prácticas se deben de remitir a cphe@thesecuritysentinel.es

1. Usaremos la máquina virtual como laboratorio para esta práctica, debes de configurarla en modo NAT e identificar las direcciones **IP activas** (deberían ser la de Kali Linux y Metasploitable2 y las internas de VMWare).

2. Realizaremos un **ping** para comprobar la conexión entre nuestra máquina y Metasploitable2.

3. Realizaremos un **escaneo completo de puertos** que vaya por rangos de 10000 en 10000, además debe de obtenerse el tipo de servicio, versión y sistema operativo de la máquina **Metasploitable2**.

4. Realizar un escaneo "sigiloso" (-sS) del mismo objetivo, pero en esta ocasión no debes de comprobar ni el tipo de servicio, ni su versión ni el sistema operativo. ¿Cuál ha sido más rápido, el anterior análisis o éste? **Razona el motivo**.

5. Usar zenmap y hacer el escaneo más completo (**Slow comprehensive scan**), no os preocupéis si el análisis lleva más tiempo, porque tarda en realizarse un poco.