Escaneo de vulnerabilidades II

Práctica N°5 II

Se hará uso de:

- **Nmap/Zenmap**
- **Laboratorio Metasploitable2**

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

Nota: Recordad que esta fase es intrusiva y si lo hacéis sin permiso, estaréis incurriendo en un delito.

1. Realizaremos un **ping sweep** para comprobar, primero la dirección IP de nuestro objetivo, y segundo la conexión entre nuestra máquina y la del objetivo.

2. Debes de escanear vulnerabilidades también con **nmap** contra **Metasploitable2**, ¿ves algo interesante?

3. Crea una política de análisis completa con **zenmap**.

4. Ejecuta la política de análisis que has creado contra la máquina Metasploitable2.

5. Configura en **Nessus** una política de análisis de vulnerabilidades centrado exclusivamente en el análisis de aplicaciones web. Realiza un escaneo contra la web de **Metasploitable2**.

6. Realiza con **OWASP-ZAP** un análisis rápido de la web de **Metasploitable2**. ¿Ha sacado lo mismo que Nessus?