EJERCICIOS METASPLOIT II

Prerrequisitos

- Kali Linux
- Metasploitable2

Ejercicio 1 - Metasploit

- Crear un workspace de trabajo llamado "metasploitable2".
- Cambiar al workspace de trabajo recién creado.
- Realizar las siguientes operaciones en el workspace, comprobando las entradas en la base de datos del Workspace (comandos hosts, services, vulns, notes, creds...).
    - 1.Realizar un escaneo de puertos contra la máquina utilizando db_nmap.

Ejercicio 2 - Metasploit

- Explotar los backdoors de las versiones instaladas de Vsftpd y UnrealIRCd.

Ejercicio 3 - Metasploit

- Realizar un ataque de fuerza bruta con los módulos auxiliares correspondientes para conseguir las credenciales de acceso de PostgreSQL y explotarlo para conseguir acceso a la máquina.
- NOTA: Utilizar los diccionarios disponibles en Kali en la ruta /usr/share/wordlists/metasploit/ y tened en cuenta en las opciones que tanto usuario como contraseña pueden estar en blanco.

Ejercicio 4 - Metasploit

- Realizar un ataque de fuerza bruta con los módulos auxiliares correspondientes para conseguir las credenciales de acceso de FTP y VNC Server.
- NOTA: Utilizar los diccionarios disponibles en Kali en la ruta /usr/share/wordlists/metasploit/ y tened en cuenta en las opciones que tanto usuario como contraseña pueden estar en blanco.