Explotación de vulnerabilidades

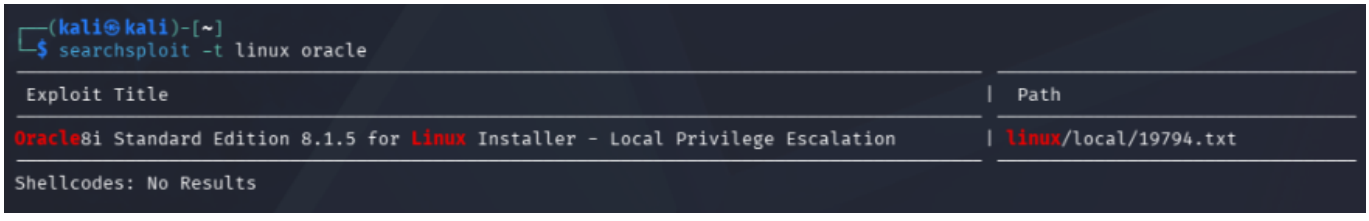
SearchSpolit

Es una herramienta de búsqueda para Exploit-DB que permite llevar una copia de Exploit DataBase, útil cuando no se tiene acceso a internet. Se puede instalar con los siguientes comandos:

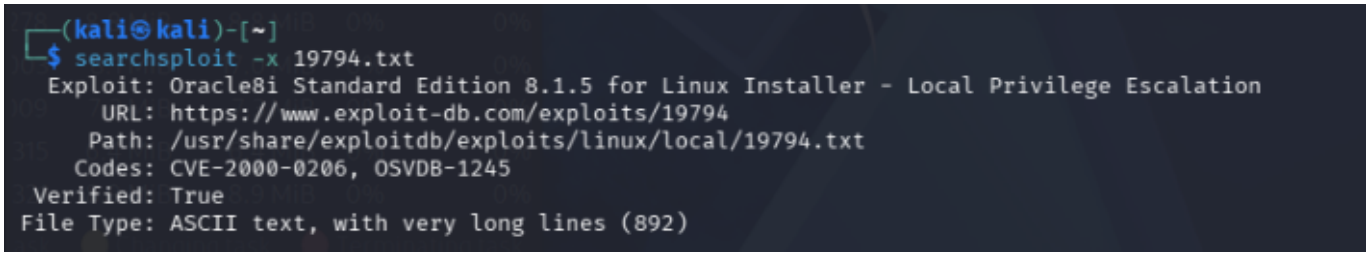
```
sudo apt install exploitbd
```

Nos permite realizar búsquedas por distintos campos, devolviendo un título autoexplicativo y la ruta al exploit.

Si queremos realizar una búsqueda por título se usa el flag -t:



Se puede realizar un visionado básico con el flag -x:



Los exploits identificados pueden guardarse con el flag m en el sistema.

Metasploit

Es un proyecto open source que permite desarrollar y ejecutar exploits contra una máquina objetivo. Se compone de diversos módulos que permiten realizar distintas acciones de pentesting. Metasploit contiene los siguientes módulos:

- AUXILIARY: Permite obtener información sobre un objetivo para identificar posibles vulnerabilidades que lo afecten. Útil para establecer una estrategia de ataque.
- EXPLOIT: Programas que explotan vulnerabilidades en un software determinado. Utilizado para ganar acceso a un sistema.
- PAYLOAD: Programas que acompañan el expoil para realizar funciones específicas en el sistema operativo coprometido. Hay varios tipos:
    - Singles: Payload autónomos que realizan una tarea concreate en el sistema victima:
        - Creación de usuario
        - Crear Shell directa
        - Crear Shell reversa
        - Ejecución de un comando.
    - Stagers: Se encargan de crear conexión entre el cliente y la victima, se usan como apoyo para descargar payload de tipo Staged
    - Staged: Son descargados t ehecutados por los payload Stagers, se usan para realizar tareas en el equipo victima.
- Encoders: Código de cifrado para evasión de antivirus y seguridad perimetral
- Nops: Utilizados por las paylaods para ajecutar en memoria, evitanq ue el procesador interrumpa la carga de este.
- Post: Utilizado para la post-explotación