

Explotación de vulnerabilidades

SearchSploit

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 exploitdb
```

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

```
(kali@kali)-[~]
└─$ searchsploit linux oracle
```

Exploit Title	Path
Oracle (oidldapd connect) - Local Command Line Overflow	linux/local/183.c
Oracle 8 - File Access	linux/local/19142.sh
Oracle 8 - oratclsh Suid	linux/local/19125.txt
Oracle 8.x - cmctl Buffer Overflow	linux/local/20411.c
Oracle 8i - TNS Listener Local Command Parameter Buffer Overflow	linux/local/21362.c
Oracle 9i/10g - 'utl_file' FileSystem Access	linux/remote/2959.sql
Oracle Application Server 4.0.8.2 - ndwfn4.so Buffer Overflow	linux/dos/20747.txt
Oracle Automated Service Manager 1.3 - Installation Privilege Escalation	linux/local/24458.txt
Oracle Business Intelligence Enterprise Edition 5.5.0.0.0 / 12.2.1.3.0 / 12.2.1.4.0 - '...	linux/webapps/48964.txt
Oracle Database Server 9.0.x - Oracle Binary Local Buffer Overflow	linux/local/23258.c
Oracle Database Vault - 'ptrace(2)' Local Privilege Escalation	linux/local/7177.c
Oracle Glassfish OSE 4.1 - Path Traversal (Metasploit)	linux/webapps/45198.rb
Oracle Internet Directory 2.0.6 - oidldap	linux/local/20312.c
Oracle MySQL / MariaDB - Insecure Salt Generation Security Bypass	linux/remote/38109.pl
Oracle MySQL 5.1.48 - 'HANDLER' Interface Denial of Service	linux/dos/34520.txt
Oracle MySQL < 5.1.49 - 'DDL' Statements Denial of Service	linux/dos/34522.txt
Oracle MySQL < 5.1.49 - Malformed 'BINLOG' Arguments Denial of Service	linux/dos/34521.txt
Oracle Siebel CRM 19.0 - Persistent Cross-Site Scripting	linux/webapps/47132.txt
Oracle VM Server Virtual Server Agent - Command Injection (Metasploit)	linux/remote/16915.rb
Oracle VM VirtualBox - Cooperating VMs can Escape from Shared Folder	linux/local/41597.txt
Oracle VM VirtualBox 4.1 - Local Denial of Service	linux_x86-64/dos/21224.c
Oracle VM VirtualBox 5.1.14 r112924 - Unprivileged Host User to Host Kernel Privilege E	linux/local/41907.c
Oracle VM VirtualBox < 5.0.32 / < 5.1.14 - Local Privilege Escalation	linux/local/41196.txt
Oracle WebCenter FatWire Content Server < 7 - Improper Access Control	linux/webapps/44757.txt
Oracle8i Standard Edition 8.1.5 for Linux Installer - Local Privilege Escalation	linux/local/19794.txt

```
Shellcodes: No Results
```

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

```
(kali@kali)-[~]
└─$ searchsploit -t linux oracle
```

Exploit Title	Path
Oracle8i Standard Edition 8.1.5 for Linux Installer - Local Privilege Escalation	linux/local/19794.txt

```
Shellcodes: No Results
```

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

```
(kali@kali)-[~]
└─$ searchsploit -x 19794.txt
```

```
Exploit: Oracle8i Standard Edition 8.1.5 for Linux Installer - Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/19794
Path: /usr/share/exploitdb/exploits/linux/local/19794.txt
Codes: CVE-2000-0206, OSVDB-1245
Verified: True
File Type: ASCII text, with very long lines (892)
```

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 exploit para realizar funciones específicas en el sistema operativo comprometido. Hay varios tipos:
 - **Singles:** Payload autónomos que realizan una tarea concreta en el sistema víctima:
 - Creación de usuario
 - Crear Shell directa
 - Crear Shell reversa
 - Ejecución de un comando.
 - **Stagers:** Se encargan de crear conexión entre el cliente y la víctima, se usan como apoyo para descargar payload de tipo Staged
 - **Staged:** Son descargados y ejecutados por los payload Stagers, se usan para realizar tareas en el equipo víctima.
- **Encoders:** Código de cifrado para evasión de antivirus y seguridad perimetral
- **Nops:** Utilizados por los payloads para ejecutar en memoria, evitan que el procesador interrumpa la carga de este.
- **Post:** Utilizado para la post-explotación

From:

<https://knoppia.net/> - **Knoppia**

Permanent link:

https://knoppia.net/doku.php?id=master_cs:int:tm4v2

Last update: **2026/05/18 16:18**

