

SearchSploit
v4.0.1

OFFENSIVE[®]
security

EXPLOIT 
DATABASE

Last Updated: 24-Sept-2018



SearchSploit – The Manual

Table of Contents

- What is SearchSploit?
- How to Install SearchSploit
 - Kali Linux
 - Linux
 - Apple OS X/macOS
 - Windows
 - Git
- Keeping SearchSploit Up-to-Date
- Using SearchSploit
 - Basic Search
 - Title Searching
 - Removing Unwanted Results
 - Piping Output *(Alternative Method of Removing Unwanted Results)*
 - Colour Output
 - Copy To Clipboard
 - Copy To Folder
 - Exploit-DB Online
- Filing a Bug Report
- EDB Partners



What is SearchSploit?

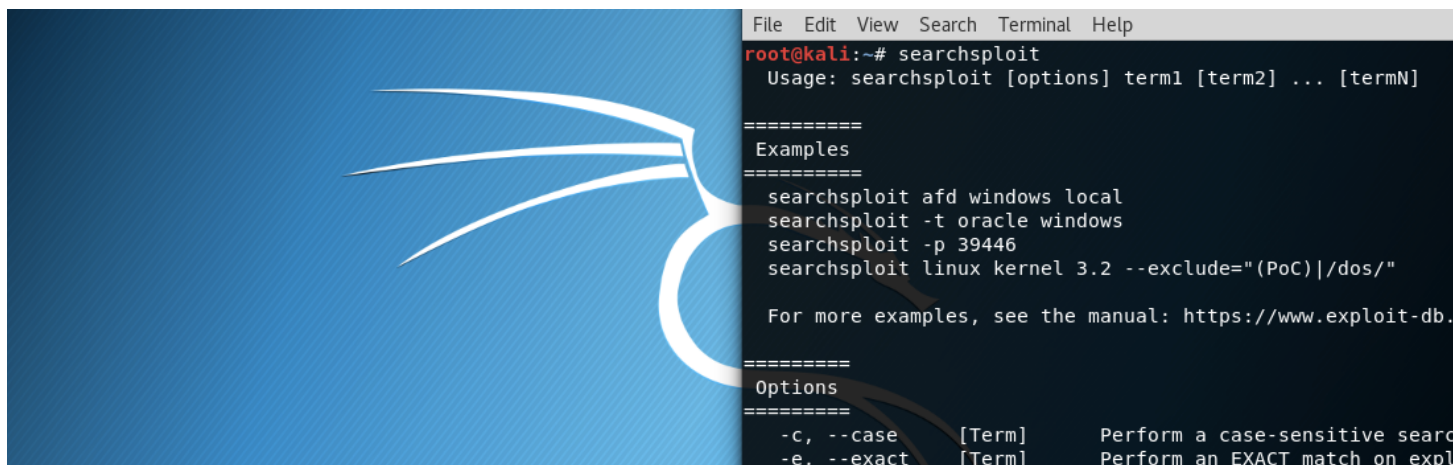
Included in our Exploit Database repository on GitHub is "searchsploit", a command line search tool for **Exploit-DB** that also allows you to take a copy of Exploit Database with you, everywhere you go. **SearchSploit** gives you the power to perform detailed off-line searches through your locally checked-out copy of the repository. This capability is particularly useful for security assessments on segregated or air-gapped networks without Internet access.

Many exploits contain links to binary files that are not included in the standard repository but can be found in our Exploit Database Binary Exploits repository instead. If you anticipate you will be without Internet access on an assessment, ensure you check out both repositories for the most complete set of data.

This guide is for version 4 of SearchSploit.

Note, The name of this utility is Search**Sploit** and as its name indicates, it will search for all exploits and shellcode. It will not include any results for Google Hacking Database, but it can include Papers if configured (*correctly!*).





```
File Edit View Search Terminal Help
root@kali:~# searchsploit
Usage: searchsploit [options] term1 [term2] ... [termN]

=====
Examples
=====
searchsploit afd windows local
searchsploit -t oracle windows
searchsploit -p 39446
searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"

For more examples, see the manual: https://www.exploit-db.com/

=====
Options
=====
-c, --case [Term]      Perform a case-sensitive search
-e, --exact [Term]    Perform an EXACT match on exploit
```

How to Install SearchSploit

Linux

Kali Linux:

If you are using the standard GNOME build of Kali Linux, the “**exploitdb**” package is already included by default! However, if you are using the Kali Light variant or your own custom-built ISO, you can install the package manually as follows:

```
root@kali:~# apt update && apt -y install exploitdb
```

You may wish to install some other related packages, "exploitdb-paperes" and "exploitdb-bin-splits".



How to Install SearchSploit

Linux

If you are not using Kali Linux, the exploitdb package may not be available through the package manager in which case, you can continue by following the 'git' section below.

Apple OS X/macOS

If you have homebrew (*package, formula*) installed, running the following will get you setup:

```
user@MacBook:~$ brew update && brew install exploitdb
```

Alternatively, if you do not have brew installed, you can still continue by following the 'git' section below.

Windows

At this time, there is no easy or straightforward way to use searchsploit... Sorry, not sorry.

The best alternative we can suggest would be to use Kali Linux in a virtual machine, docker or Windows Subsystem for Linux.

Kali Linux Virtual Machine Images:

<https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/>

Kali Linux Docker Image:

<https://www.kali.org/news/official-kali-linux-docker-images/>

Kali on the Windows Subsystem for Linux:

<https://www.kali.org/tutorials/kali-on-the-windows-subsystem-for-linux/>



How to Install SearchSploit

GIT

On *nix systems, all you really need is either "CoreUtils" or "utilities" (e.g. *bash*, *sed*, *grep*, *awk*, etc.), as well as "git". These are installed by default on many different Linux distributions, including OS X/macOS.

You can easily check out the git repository by running the following:

```
$ git clone https://github.com/offensive-security/exploitdb.git /opt/exploitdb
```

An optional step that will make using **SearchSploit** easier is to include it into your **\$PATH**.

Example: In the following output, you can see that the directory "/usr/local/bin" is included in the \$PATH environment variable:

```
$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
$
```

With this in mind, you can then create a symbolic link in the "/usr/local/bin" directory that points to searchsploit, allowing you to run it without providing the full path:

```
$ ln -sf /opt/exploit-database/searchsploit /usr/local/bin/searchsploit
$
```

The last stage is to copy the resource file and edit it to match your system environment so it points to the correct directories:

```
$ cp -n /opt/exploit-database/.searchsploit_rc ~/
$
$ vim ~/.searchsploit_rc
```



Each section in the resource file (`.searchsploit_rc`), is split into sections (such as "Exploits", "Shellcodes", "Papers").

- **files_array** - A Comma-Separated Value file (`files_*.CSV`) that contains all the data that relates to that section (such as: *EDB-ID, Title, Author, Date Published, etc*).
- **path_array** - This points to the directory where all the files are located. ****This is often the only value that needs altering****.
- **name_array** - The value name to display in SearchSploit for that section.
- **git_array** - The remote git location to use to update the local copy.
- **package_array** - The package name to use when there is a package manager available (such as *apt or brew*).

If you want to include Exploit-DB Papers, you can check out the git repository. Afterwards, edit searchsploit's resource file so paper's path_array points to the same directory you just checked out.



Keeping SearchSploit Up-to-Date

If you are using Kali Linux, you can expect the exploitdb package to be updated weekly. If you are using homebrew or Git, you can expect daily updates (*at 05:05 UTC*).

Regardless of how you installed **SearchSploit**, all you need to do in order to update it is run the following:

```
$ searchsploit -u
```

If you are using the Kali Linux package and haven't updated since before 20 September 2016, you will first need to update the package in the traditional manner:

```
root@kali:~# apt update && apt -y full-upgrade
```

Please note, we do not recommend you use GitHub's ".zip" or the legacy "archive.tar.bz2" packages to update.



Using SearchSploit

Help Screen

By using `"-h"`, you can see all the features and options that are available to you:

```
root@kali:~# searchsploit -h
Usage: searchsploit [options] term1 [term2] ... [termN]

=====
Examples
=====
searchsploit afd windows local
searchsploit -t oracle windows
searchsploit -p 39446
searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"
searchsploit linux reverse password

For more examples, see the manual: https://www.exploit-db.com/searchsploit/

=====
Options
=====
-c, --case [Term]      Perform a case-sensitive search (Default is inSEnsITiVe).
-e, --exact [Term]    Perform an EXACT match on exploit title (Default is AND) [Implies "-t"].
-h, --help            Show this help screen.
-j, --json [Term]     Show result in JSON format.
-m, --mirror [EDB-ID] Mirror (aka copies) an exploit to the current working directory.
-o, --overflow [Term] Exploit titles are allowed to overflow their columns.
-p, --path [EDB-ID]   Show the full path to an exploit (and also copies the path to the clipboard
if possible).
-t, --title [Term]    Search JUST the exploit title (Default is title AND the file's path).
-u, --update          Check for and install any exploitdb package updates (deb or git).
-w, --www [Term]     Show URLs to Exploit-DB.com rather than the local path.
-x, --examine [EDB-ID] Examine (aka opens) the exploit using $PAGER.
    --colour          Disable colour highlighting in search results.
    --id              Display the EDB-ID value rather than local path.
    --nmap [file.xml] Checks all results in Nmap's XML output with service version (e.g.: nmap -
sV -oX file.xml).

    Use "-v" (verbose) to try even more combinations
    --exclude="term"  Remove values from results. By using "|" to separated you can chain multiple
values.

    e.g. --exclude="term1|term2|term3".

=====
Notes
=====
* You can use any number of search terms.
* Search terms are not case-sensitive (by default), and ordering is irrelevant.
* Use '-c' if you wish to reduce results by case-sensitive searching.
* And/Or '-e' if you wish to filter results by using an exact match.
* Use '-t' to exclude the file's path to filter the search results.
* Remove false positives (especially when searching using numbers - i.e. versions).
* When updating or displaying help, search terms will be ignored.

root@kali:~#
```



Basic Search

Simply add any number of search terms you wish to look for:

```
root@kali:~# searchsploit afd windows local
```

Exploit Title	Path (/usr/share/exploitdb/)
Microsoft Windows (x86) - 'afd.sys' Local Privilege Escalation (MS11-046)	exploits/windows_x86/local/40564.c
Microsoft Windows - 'AfdJoinLeaf' Local Privilege Escalation (MS11-080) (Metasploit)	exploits/windows/local/21844.rb
Microsoft Windows - 'afd.sys' Local Kernel (PoC) (MS11-046)	exploits/windows/dos/18755.c
Microsoft Windows 7 (x64) - 'afd.sys' Dangling Pointer Privilege Escalation (MS11-080)	exploits/windows_x86-64/local/39525.py
Microsoft Windows 7 (x86) - 'afd.sys' Dangling Pointer Privilege Escalation (MS11-080)	exploits/windows_x86/local/39446.py
Microsoft Windows XP - 'afd.sys' Local Kernel Denial of Service	exploits/windows/dos/17133.c
Microsoft Windows XP/2003 - 'afd.sys' Local Privilege Escalation (K-plugin) (MS08-067)	exploits/windows/local/6757.txt
Microsoft Windows XP/2003 - 'afd.sys' Local Privilege Escalation (MS11-080)	exploits/windows/local/18176.py

```
Shellcodes: No Result
root@kali:~#
```

Note, **SearchSploit** uses an **AND** operator, **not** an **OR** operator. The more terms that are used, the more results will be filtered out.

Pro Tip: Do not use abbreviations.

- Example: SQLi -> SQL Injection

Pro Tip: If you are not receiving the expected results, try searching more broadly by using more general terms.

- Example: Kernel 2.6.25 -> Kernel 2.6 // Kernel 2.x

```
root@kali:~# searchsploit kernel 2.6
```

Exploit Title	Path (/usr/share/exploitdb/)
Authentium SafeCentral 2.6 - 'shdrv.sys' Local Kernel Ring0 SYSTEM	exploits/windows/local/11232.c
DESlock+ < 3.2.6 - 'DLMFDISK.sys's Local Kernel Ring0 SYSTEM	exploits/windows/local/5144.c
DESlock+ < 3.2.6 - 'DLMFENC.sys' Local Kernel Ring0 link list zero (PoC)	exploits/windows/dos/5142.c
DESlock+ < 3.2.6 - 'LIST' Local Kernel Memory Leak	exploits/windows/local/5141.c
DESlock+ < 3.2.6 - Local Kernel Ring0 link list zero SYSTEM	exploits/windows/local/5143.c
Google Android Kernel 2.6 - Local Denial of Service Crash (PoC)	exploits/android/dos/23248.txt
Linux Kernel 2.2.25/2.4.24/2.6.2 - 'mremap()' Local Privilege Escalation	exploits/linux/local/160.c
Linux Kernel 2.2.25/2.4.24/2.6.2 - 'mremap()' Validator	exploits/linux/local/154.c
Linux Kernel 2.2.x/2.3.x/2.4.x/2.5.x/2.6.x - ELF Core Dump Local Buffer Overflow (PoC)	exploits/linux/dos/25647.sh
Linux Kernel 2.4.1 < 2.4.37 / 2.6.1 < 2.6.32-rc5 - 'pipe.c' Local Privilege Escalation (3)	exploits/linux/local/9844.py
Linux Kernel 2.4.22-28/2.6.9 - 'igmp.c' Local Denial of Service	exploits/linux/dos/686.c
Linux Kernel 2.4.23/2.6.0 - 'do_mremap()' Bound Checking Privilege Escalation	exploits/linux/local/145.c



Title Searching

By default, searchsploit will check BOTH the title of the exploit as well as the path. Depending on the search criteria, this may bring up false positives (*especially when searching for terms that match platforms and version numbers*). Searches can be restricted to the titles by using the **"-t"** option:

```
root@kali:~# searchsploit -t oracle windows
-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
Oracle 10g (Windows x86) - 'PROCESS_DUP_HANDLE' Local Privilege Escalatio | exploits/windows_x86/local/3451.c
Oracle 9i XDB (Windows x86) - FTP PASS Overflow (Metasploit) | exploits/windows_x86/remote/16731.rb
Oracle 9i XDB (Windows x86) - FTP UNLOCK Overflow (Metasploit) | exploits/windows_x86/remote/16714.rb
Oracle 9i XDB (Windows x86) - HTTP PASS Overflow (Metasploit) | exploits/windows_x86/remote/16809.rb
Oracle MySQL (Windows) - FILE Privilege Abuse (Metasploit) | exploits/windows/remote/35777.rb
Oracle MySQL (Windows) - MOF Execution (Metasploit) | exploits/windows/remote/23179.rb
Oracle MySQL for Microsoft Windows - Payload Execution (Metasploit) | exploits/windows/remote/16957.rb
Oracle VM VirtualBox 5.0.32 r112930 (x64) - Windows Process COM Injection | exploits/windows_x86-64/local/41908.txt
Oracle VirtualBox Guest Additions 5.1.18 - Unprivileged Windows User-Mode | exploits/multiple/dos/41932.cpp
-----
Shellcodes: No Result
root@kali:~#
root@kali:~# searchsploit oracle windows | wc -l
94
root@kali:~#
```

If we did not use "-t", we would have 87 (7 lines are in the heading/footer) results, rather than 9.



Removing Unwanted Results

We can remove unwanted results by using the "--exclude="" option. We are also able to remove multiple terms by separating the value with a "|" (*pipe*). This can be demonstrated by the following:

```
root@kali:~# searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"
```

Exploit Title	Path (/usr/share/exploitdb/)
Linux Kernel 2.6.39 < 3.2.2 (Gentoo / Ubuntu x86/x64) - 'Mempodipper' Local P	exploits/linux/local/18411.c
Linux Kernel 2.6.39 < 3.2.2 (x86/x64) - 'Mempodipper' Local Privilege Escalat	exploits/linux/local/35161.c
Linux Kernel 3.2.0-23/3.5.0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf_swe	exploits/linux_x86-64/local/33589.c
Linux Kernel 3.2.x - 'uname()' System Call Local Information Disclosure	exploits/linux/local/37937.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X86_X32=y' Local	exploits/linux_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG_X86_X32' Arbitrary Write (exploits/linux/local/31346.c
Linux Kernel < 3.2.0-23 (Ubuntu 12.04 x64) - 'ptrace/sysret' Local Privilege	exploits/linux_x86-64/local/34134.c

```
Shellcodes: No Result
root@kali:~#
root@kali:~# searchsploit linux kernel 3.2 | wc -l
19
root@kali:~#
```

By doing this, we slim the results down to 7 rather than 12 (7 lines are for the heading/footer)!

Pro Tip: By doing: "searchsploit linux kernel --exclude="(PoC)|/dos/" | grep '3.2' ", you'll get even "cleaner" output (sorted based on version without any heading/footers).



Piping Output (*Alternative Method of Removing Unwanted Results*)

The output from searchsploit can be piped into any other program, which is especially useful when outputting the results in JSON format (*using the "-j" option*). With this, it is possible to remove any unwanted exploits by using grep. In the following example, we use grep to filter out any "Denial of Service (DoS)" results.

```
root@kali:~# searchsploit XnView | grep -v '/dos/'
```

Exploit Title	Path (/usr/share/exploitdb/)
XnView 1.90.3 - '.xpm' Local Buffer Overflow	exploits/windows/local/3777.c
XnView 1.92.1 - 'FontName' Slideshow Buffer Overflow	exploits/windows/local/5346.pl
XnView 1.92.1 - Command-Line Arguments Buffer Overflow	exploits/windows/remote/31405.c
XnView 1.93.6 - '.taac' Local Buffer Overflow	exploits/windows/local/5951.c
XnView 1.97.4 - '.MBM' File Remote Heap Buffer Overflow	exploits/windows/remote/34143.txt

```
root@kali:~#  
root@kali:~# searchsploit XnView | wc -l  
24  
root@kali:~#
```

By piping the search results into grep, we managed to filter the results down to 5 rather than 17 (7 lines are in the heading/footer)!

Pro Tip: We recommend using "/dos/" with grep rather than "dos" so the filter is applied to the path, rather than the title. Although denial of service entries may not include "dos" in their title, they will nevertheless have "dos" in the path. Removing results based on the path will also ensure you don't inadvertently filter out results that legitimately contain "dos" in their title (*i.e.: EDB-ID #24623*).



Colour Output

By default, searchsploit highlights the search terms in the results when they are displayed to the user. This works by inserting invisible characters into the output before and after the colour changes.

Now, if you were to pipe the output (*for example, into grep*) and try to match a phrase of both highlighted and non-highlighted text in the output, it would not be successful. This can be solved by using the "--colour" option (*--color works as well*).

```
root@kali:~# searchsploit wordpress mail list

-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
WordPress Plugin Mailing List - Arbitrary File Download | exploits/php/webapps/18276.txt
WordPress Plugin Mailing List 1.3.2 - Remote File Inclusion | exploits/php/webapps/17866.txt
WordPress Plugin WP-phpList 2.10.2 - 'unsubscribeemail' Cross-Site Scripting | exploits/php/webapps/33365.txt
-----
Shellcodes: No Result
root@kali:~#
root@kali:~# searchsploit wordpress mail list | grep "Mailing List 1.3.2"
root@kali:~#
root@kali:~# searchsploit wordpress mail list --colour | grep "Mailing List 1.3.2"
WordPress Plugin Mailing List 1.3.2 - Remote File Inclusion | exploits/php/webapps/17866.txt
root@kali:~#
```



Copy To Clipboard

So now that we have found the exploit we are looking for, there are various ways to access it quickly.

By using **"-p"**, we are able to get some more information about the exploit, as well as copy the complete path to the exploit onto the clipboard:

```
root@kali:~# searchsploit 39446
-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
Microsoft Windows 7 (x86) - 'afd.sys' Dangling Pointer Privilege Escalation (| exploits/windows_x86/local/39446.py
-----
Shellcodes: No Result
root@kali:~#
root@kali:~# searchsploit -p 39446

Exploit: Microsoft Windows 7 (x86) - 'afd.sys' Dangling Pointer Privilege Escalation (MS14-040)
URL: https://www.exploit-db.com/exploits/39446/
Path: /usr/share/exploitdb/exploits/windows_x86/local/39446.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied EDB-ID #39446's path to the clipboard.
root@kali:~#
root@kali:~# /usr/share/exploitdb/exploits/windows_x86/local/39446.py
```



Copy To Folder

We recommend that you do not alter the exploits in your local copy of the database. Instead, make a copy of ones that are of interest and use them from a working directory. By using the **"-m"** option, we are able to select as many exploits we like to be copied into the same folder that we are currently in:

```
root@kali:~# searchsploit MS14-040
-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
Microsoft Windows 7 (x64) - 'afd.sys' Dangling Pointer Privilege Escalatio| exploits/windows_x86-64/local/39525.py
Microsoft Windows 7 (x86) - 'afd.sys' Dangling Pointer Privilege Escalatio| exploits/windows_x86/local/39446.py
-----
Shellcodes: No Result
root@kali:~#
root@kali:~# searchsploit -m 39446 win_x86-64/local/39525.py

  Exploit: Microsoft Windows 7 (x86) - 'afd.sys' Dangling Pointer Privilege Escalation (MS14-040)
    URL: https://www.exploit-db.com/exploits/39446/
    Path: /usr/share/exploitdb/exploits/windows_x86/local/39446.py
  File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /root/39446.py

  Exploit: Microsoft Windows 7 (x64) - 'afd.sys' Dangling Pointer Privilege Escalation (MS14-040)
    URL: https://www.exploit-db.com/exploits/39525/
    Path: /usr/share/exploitdb/exploits/windows_x86-64/local/39525.py
  File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /root/39525.py

root@kali:~#
```

You do not have to give the exact EDB-ID value (such as "39446"); SearchSploit is able to automatically extract it from a path given to it (such as "39525").



Exploit-DB Online

The Exploit Database repository is the main core of Exploit-DB, making **SearchSploit** efficient and easy to use. However, some of the exploit metadata (*such as screenshots, setup files, tags, and vulnerability mappings*) are not included. To access them, you will need to check the website.

You can quickly generate the links to exploits of interest by using the "-w" option:

```
root@kali:~# searchsploit WarFTP 1.65 -w
-----
Exploit Title | URL
-----
WarFTP 1.65 (Windows 2000 SP4) - 'USER' Remote Buffer Overflow (Perl) | https://www.exploit-db.com/exploits/3482/
WarFTP 1.65 (Windows 2000 SP4) - 'USER' Remote Buffer Overflow (Pytho | https://www.exploit-db.com/exploits/3474/
WarFTP 1.65 - 'USER' Remote Buffer Overflow | https://www.exploit-db.com/exploits/3570/
-----
Shellcodes: No Result
root@kali:~#
```

Filling a Bug Report

If you have any issues or questions, please search (*then open!*) an issue on the GitHub repository (<https://github.com/offensive-security/exploitdb/issues?q=is%3Aissue>).

EDB Partners

If you have a commercial requirement for more data than is publicly available, an extended version of **SearchSploit** is available exclusively to [EDB Partners](#).

Updated instructions for this document can be found at:

<https://www.exploit-db.com/searchsploit/>

