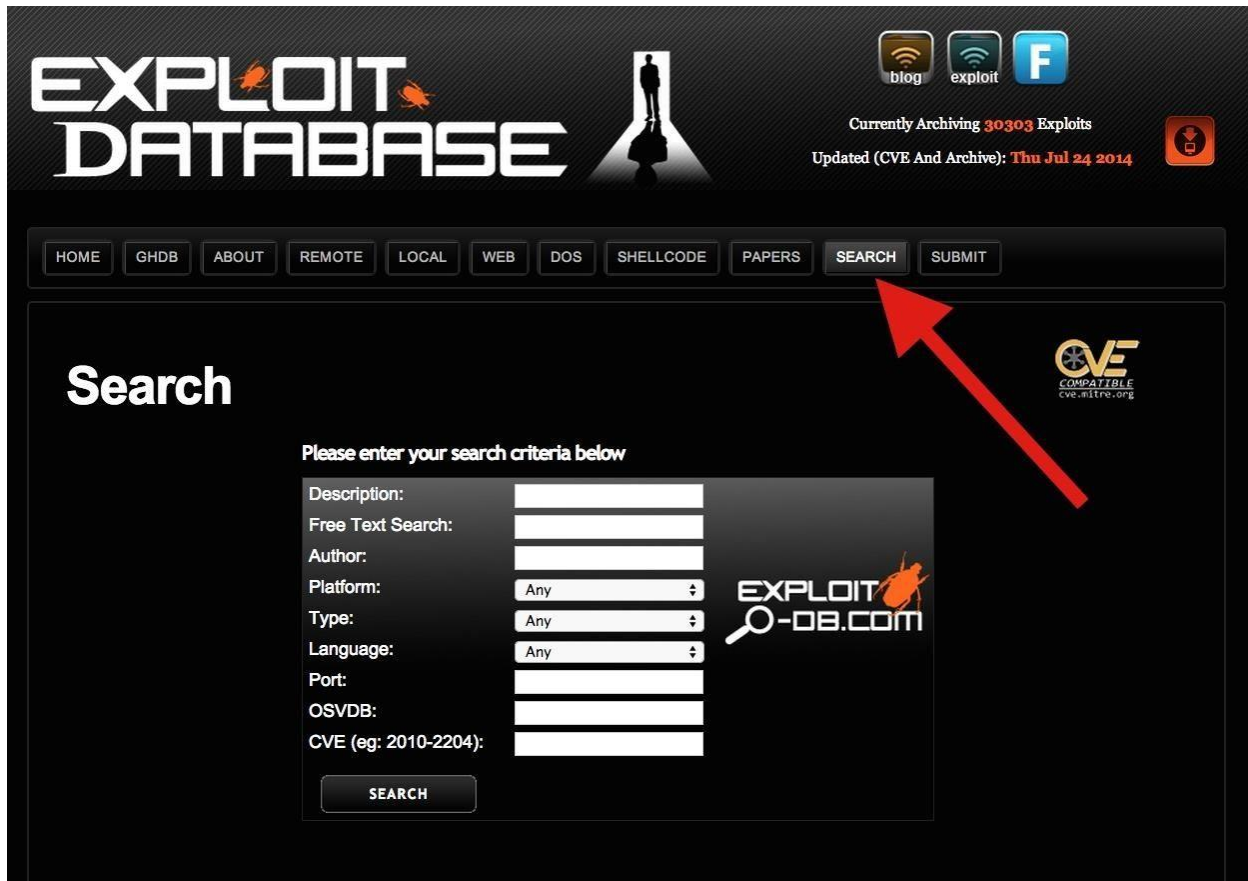


How to Find Exploits Using the Exploit Database in Kali



Author & Credits:

Occupytheweb

<https://creator.wonderhowto.com/occupythewebotw/>

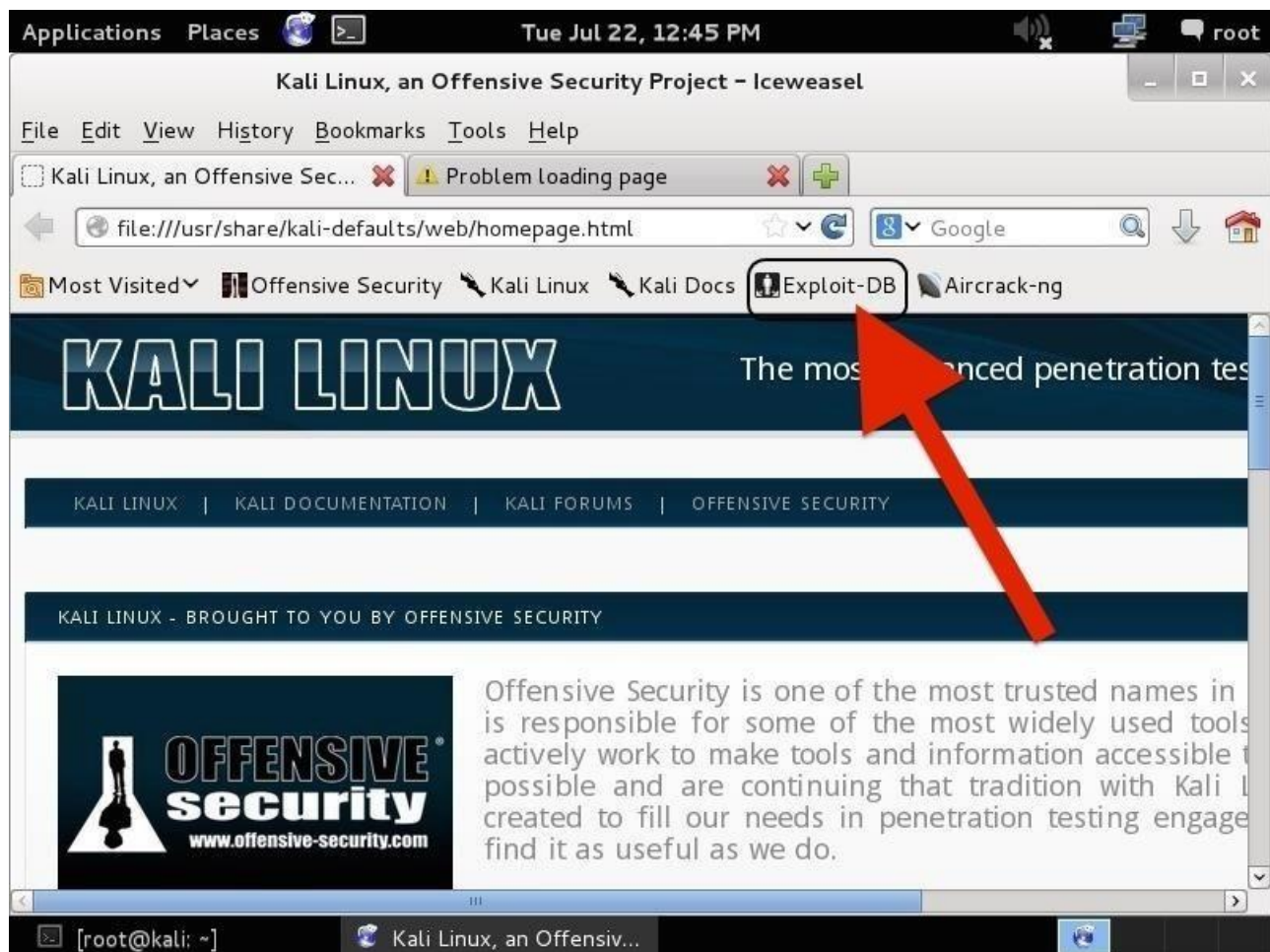
When we are looking for ways to hack a system, we need a specific exploit to take advantage of a certain vulnerability in the operating system, service, or application.

Remember, exploitation is very specific, there is no one silver bullet that will allow you to exploit all systems. You need to find an exploit that will specifically take advantage of a vulnerability in the system that you are attacking. That is where the [Exploit Database](#) can be so incredibly useful.

EDB is a project of [Offensive Security](#), the same folks who developed [BackTrack](#) and [Kali Linux](#), which includes exploits categorized by platform, type, language, port, etc. to help you find the exploit that will work in your particular circumstance. Then, if you feel it will work on your target, you can simply copy and paste it into Kali for your attack.

Step 1 Fire up Kali & Open a Browser

Let's start by firing up Kali and opening a browser, such as Iceweasel, the default browser in Kali (EDB can be reached from any browser, in any operating system). If we use the default browser in Kali, we can see that there is a built-in shortcut to the "Exploit-DB" in the browser shortcut bar, as seen below.



When we click on it, it takes us to the Exploit Database, as seen below.

The screenshot shows the homepage of the Exploit Database. At the top, the logo "EXPLOIT DATABASE" is displayed in a stylized font. To the right, there are social media icons for "blog", "exploit", and "F". Below these, it says "Currently Archiving 30280 Exploits" and "Updated (CVE And Archive): Tue Jul 22 2014". A navigation menu includes links for HOME, GHDB, ABOUT, REMOTE, LOCAL, WEB, DOS, SHELLCODE, PAPERS, SEARCH, and SUBMIT. A banner for "Advanced malware detection" from Cisco is visible. The main heading is "The Exploit Database", followed by a description: "The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database." Below this, there are two sections: "Remote Exploits" and "Local Exploits", each with a table of entries.

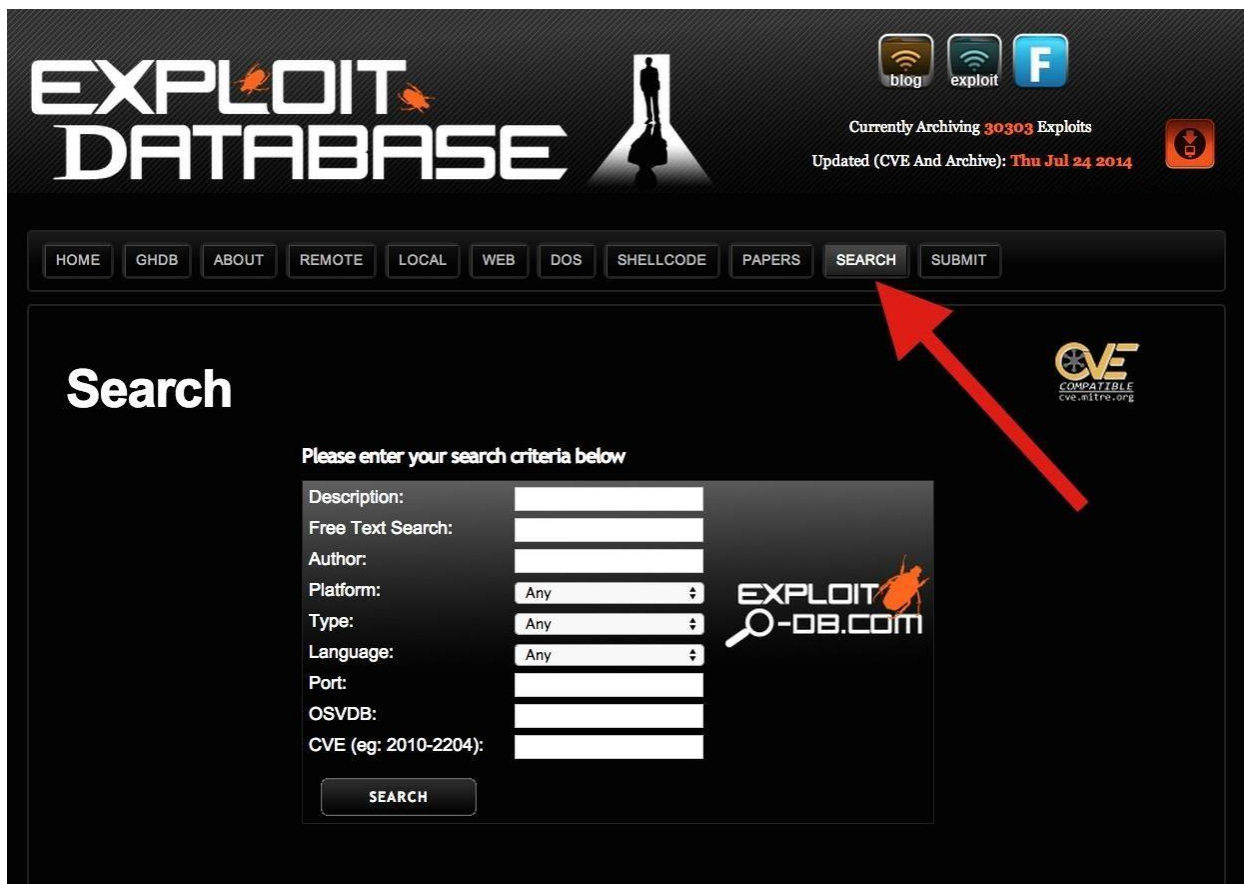
Date	D	A	V	Description	Plat.	Author
2014-07-14	↓	📄	✓	Kolibri WebServer 2.0 - GET Request SEH Exploit	windows	Revin Hadi Saputr.
2014-07-10	↓	📄	🔒	OpenVAS Manager 4.0 - Authentication Bypass Vulnerability PoC	linux	EccE
2014-07-21	↓	-	✓	IBM GCM16/32 1.20.0.22575 - Multiple Vulnerabilities	php	Alejandro Alvarez.
2014-07-16	↓	-	🔒	Boat Browser 8.0 and 8.0.1 - Remote Code Execution Vulnerability	android	c00tlass
2014-07-14	↓	-	✓	D-Link info.cgi POST Request Buffer Overflow	hardware	metasploit
2014-07-14	↓	-	✓	D-Link HNAP Request Remote Buffer Overflow	hardware	metasploit
2014-07-14	↓	-	✓	D-Link Unauthenticated UPnP M-SEARCH Multicast Command Injection	hardware	metasploit

Date	D	A	V	Description	Plat.	Author
2014-07-19	↓	-	🔒	Microsoft XP SP3 MQAC.sys - Arbitrary Write Privilege Escalation	windows	KoreLogic
2014-07-21	↓	-	🔒	Microsoft XP SP3 - BthPan.sys Arbitrary Write Privilege Escalation	windows	KoreLogic
2014-07-21	↓	-	🔒	Linux Kernel ptrace/sysret - Local Privilege Escalation	lin_amd64	Vitaly Nikolenko

If you are not using Iceweasel and its built-in shortcut, you can navigate to Exploit-DB by typing www.exploit-db.com in the URL bar.

Step 2 Search the Exploit Database

If we look at the top menu bar in the Exploit Database website, second from the right is a menu item called "Search". When we click on it, it enables us to search the database of exploits and returns a search function screen similar to the screenshot below.



Let's use this search function to find some recent Windows exploits (we are always looking for new Windows exploits, aren't we?). In the search function window, we can enter any of the following information;

- Description
- Free Text Search
- Author
- Platform (this is the operating system)
- Type
- Language
- Port
- OSVDB (the [Open Source Vulnerability Database](#))
- CVE ([Common Vulnerability and Exploits](#))

The last two fields can be used if you are specifically looking for an exploit that takes advantage of a known, numbered vulnerability in either of those databases.

In the Platform field, enter "Windows", in the Type field, enter "remote", and in the Free Text Search box, enter "Office". When we do so, the Exploit Database returns a list and a

link to all of the exploits that meet those criteria. Of course, you can put in whatever criteria you are searching for. I am only using these as an example.

Search

<< prev 1 2 >> next

Date	D	A	V	Description	Plat.	Author
2014-03-22	↓	-	✓	Internet Explorer - TextRange Use-After-Free (MS14-012)	windows	metasploit
2013-12-03	↓	-	✓	Microsoft Tagged Image File Format (TIFF) Integer Overflow	windows	metasploit
2013-10-15	↓	-	✓	Microsoft Internet Explorer - CDisplayPointer Use-After-Free (MS13-080)	windows	metasploit
2013-10-02	↓	-	✓	Microsoft Internet Explorer - SetMouseCapture Use-After-Free	windows	metasploit
2013-02-20	↓	-	✓	MS Office 2010 Download Execute	windows	g11tch
2012-10-10	↓	-	✓	Avaya IP Office Customer Call Reporter ImageUpload.ashx Remote Command Execution	windows	metasploit
2012-07-31	↓	-	✓	Microsoft Office SharePoint Server 2007 Remote Code Execution	windows	metasploit
2012-04-25	↓	-	✓	Windows - MSCOMCTL ActiveX Buffer Overflow (MS12-027)	windows	metasploit
2012-03-28	↓	-	✓	Quest InTrust 10.4.x ReportTree and SimpleTree Classes	windows	rgod
2011-12-13	↓	-	✓	CoDeSys SCADA 2.3 - Webservice Stack Buffer Overflow	windows	metasploit
2011-12-01	↓	-	✓	Serv-U FTP Jail Break	windows	kingcobe
2011-02-25	↓	📄	✓	EDraw Office Viewer Component 7.4 - ActiveX Stack Buffer Overflow	windows	Alexander Gavrun
2011-02-03	↓	📄	✓	FTPGetter 3.58.0.21 - Buffer Overflow (PASV) Exploit	windows	modpr0be
2010-09-20	↓	-	✓	Ultra Shareware Office Control ActiveX HttpUpload Buffer Overflow	windows	metasploit
2010-09-20	↓	-	✓	Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download	windows	metasploit
2010-07-20	↓	-	✓	Microsoft OWC Spreadsheet msDataSourceObject Memory Corruption	windows	metasploit
2009-01-14	↓	-	✓	EDraw Office Viewer 5.4 HttpDownloadFile() Insecure Method Vuln	windows	Cyber-Zone
2009-01-13	↓	-	✓	Office Viewer ActiveX Control 3.0.1 (Save) Remote File Overwrite Exploit	windows	Houssamix
2009-01-13	↓	-	✓	Office Viewer ActiveX Control 3.0.1 - Remote File Execution Exploit	windows	Houssamix
2008-10-30	↓	-	✓	DjVu ActiveX Control 3.0 ImageURL Property Overflow Exploit	windows	Shahriyar Jalayer.

<< prev 1 2 >> next

Step 3 Open an Exploit

From the search results page, we can click on any of the two pages of search results and it will take us to the particular exploit. I clicked on the very first exploit in the list "Internet Explorer TextRange Use-After Free (MS14_012)". When I do so, I am brought to a screen that displays the exploit code like that below. I have circled the description in the code of the exploit.

```

1  ##
2  # This module requires Metasploit: http://metasploit.com/download
3  # Current source: https://github.com/rapid7/metasploit-framework
4  ##
5
6  require 'msf/core'
7
8  class Metasploit3 < Msf::Exploit::Remote
9    Rank = NormalRanking
10
11   include Msf::Exploit::Remote::BrowserExploitServer
12
13   def initialize(info={})
14     super(update_info(info,
15       'Name' => "MS14-012 Internet Explorer TextRange Use-After-Free",
16       'Description' => %q{
17         This module exploits a use-after-free vulnerability found in Internet Explorer. The flaw
18         was most likely introduced back in 2013, therefore only certain builds of MSHTML are
19         affected. In our testing with IE9, these vulnerable builds appear to be between
20         9.0.8112.16496 and 9.0.8112.16533, which implies August 2013 until early March 2014
21         (before the patch).
22       },
23       'License' => MSF_LICENSE,
24       'Author' =>
25         [
26           'Jason Kratzer', # Original discovery
27           'sinn3r' # Port
28         ],
29       'References' =>
30         [
31           [ 'CVE', '2014-0307' ],
32           [ 'MSB', 'MS14-012' ]
33         ],
34       'Platform' => 'win',
35       'BrowserRequirements' =>
36         {
37           :source => /script/i,
38           :os_name => OperatingSystems::WINDOWS,
39           :ua_name => HttpClients::IE,
40           :office => "2010"
41           #:ua_ver => '9.0' # Some fingerprinting issue w/ os_detect, disabled for now
42         },
43       'Targets' =>
44         [
45           [
46             'Automatic',
47             {
48               # mov eax,dword ptr [edx+0C4h]; call eax
49               'Pivot' => 0x0c0d1020 # ECX
50             }
51           ]
52         ],
53       'Payload' =>
54         {
55           'BadChars' => "\x00",
56           'PrependEncoder' => "\x81\xc4\x0c\xfe\xff\xff" # add esp, -500
57         },
58       'DefaultOptions' =>
59         {
60           'Retries' => false, # You're too kind, tab recovery, I only need 1 shell.
61           'InitialAutoRunScript' => 'migrate -f'
62         }
63     })
64   end
65 end

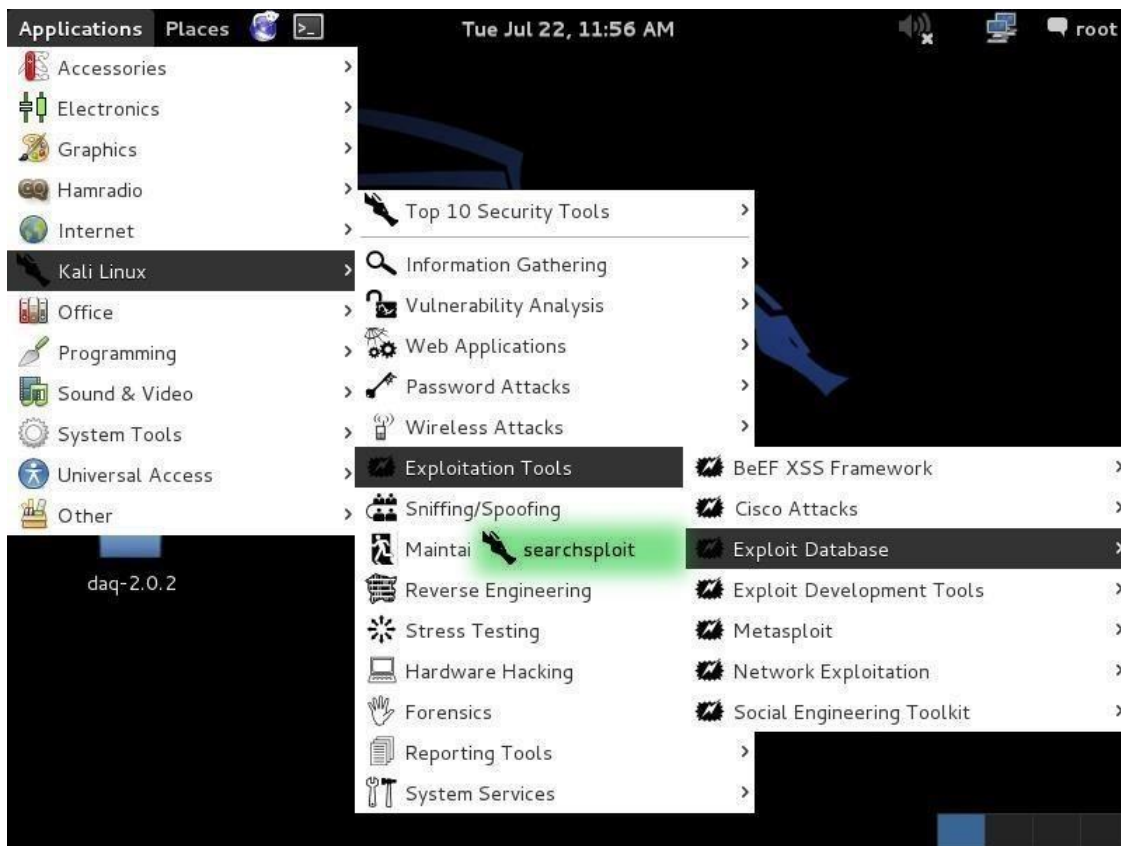
```

This exploit works against Internet Explorer that was built between August 2013 and March 2014. If you want to use it, you can simply copy and paste this text file and put it into the exploit directory in [Metasploit](https://github.com/rapid7/metasploit-framework) (if you are using an up-to-date version of Metasploit, it is already included). This is a good example of how specific an exploit can be.

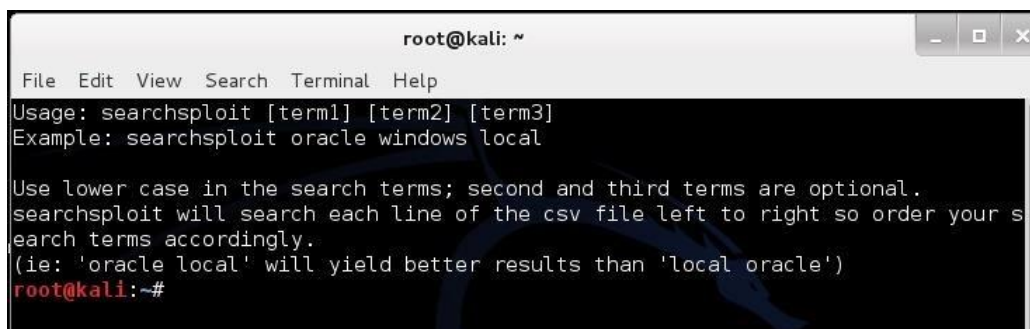
Step 4 Open up Searchsploit

Kali, having also been developed by Offensive Security, has built into it a local database of exploits based on the same Exploit Database. We can access it by going to

Applications -> Kali Linux -> Exploitation Tools -> Exploit Database and clicking on **searchsploit** as shown below.



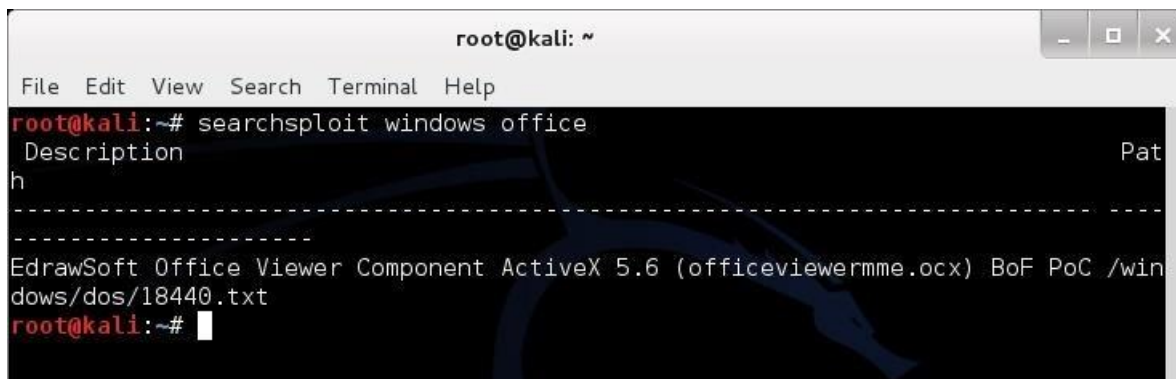
It will open a screen like that below that details the basic syntax on how to use searchsploit. Note that it explains that you must use lowercase search terms and that it searches a CSV (comma separated values) file from left to right, so search term order matters.



Step 5 Search the Exploit Database with Searchsploit

Now that we have opened a terminal for searchsploit, we can now use this tool to search our local copy of the Exploit Database. As you might expect, our local copy of the exploit database is much faster to search, but does NOT have all the updates that the online database does. Despite this, unless we looking for the very latest exploits, the local database works fast and is effective.

One other note on its use. As the information is organized in CSV files, searches locally often will yield results slightly differently than the online database. In the screenshot below, I searched for "Windows" and "Office" and only received a single result, unlike what I received when I used the online database.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# searchsploit windows office  
Description Pat  
h  
-----  
-----  
EdrawSoft Office Viewer Component ActiveX 5.6 (officeviewermmme.ocx) BoF PoC /win  
dows/dos/18440.txt  
root@kali:~#
```

Exploit Database is an excellent repository for exploits and other hacks that we might need, including new Google hacks, white papers on security and hacking, denial of service (DOS) attacks, and shellcode that you can use out the box or tailor for your unique attack.