

ARYAMAN MISHRA

19BCE1027

Lab 7: HUNTING FOR VULNERABILITY

Doing offline exploit

Searchsploit is a command-line search tool for Exploit-DB that allows you to take a copy of the Exploit Database with you. Searchsploit is included in the Exploit Database repository on GitHub. Searchsploit is very useful for security assessments when you don't have Internet access because it gives you the power to perform detailed offline searches for exploits in the saved Exploit-DB.

To run SearchSploit in Kali Linux, open the terminal and type "searchsploit" to run SearchSploit as "exploitdb" package is already included in Kali Linux.

```
(root@kali)~/usr/share/metasploit-framework
# 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/"
searchsploit -s Apache Struts 2.0.0
searchsploit linux reverse password
searchsploit -j 55555 | json_pp

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

Options

## Search Terms
-c, --case [Term]      Perform a case-sensitive search (Default is inSensITive)
-e, --exact [Term]     Perform an EXACT & order match on exploit title (Default is an AND match on each term) [Implies "-t"]
                        e.g. "WordPress 4.1" would not be detect "WordPress Core 4.1")
-s, --strict           Perform a strict search, so input values must exist, disabling fuzzy search for version range
                        e.g. "1.1" would not be detected in "1.0 < 1.3")
-t, --title [Term]     Search JUST the exploit title (Default is title AND the file's path)
--exclude="term"       Remove values from results. By using "|" to separate, you can chain multiple values
                        e.g. --exclude="term1|term2|term3"

## Output
-j, --json [Term]      Show result in JSON format
-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)
-v, --verbose          Display more information in output
-w, --www [Term]       Show URLs to Exploit-DB.com rather than the local path
--id                  Display the EDB-ID value rather than local path
--colour              Disable colour highlighting in search results

## Non-Searching
-m, --mirror [EDB-ID]  Mirror (aka copies) an exploit to the current working directory
-x, --examine [EDB-ID] Examine (aka opens) the exploit using $PAGER

## Non-Searching
```

To find all windows-based exploits Exploit can be a local based or remote based

Exploit Title	Path
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - 'PORT' Remote Denial of Service	windows/dos/12698.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Authentication Bypass / Directory Traversal SAM Retrieval	windows/remote/27441.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Full System Access	windows/remote/13932.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Universal Denial of Service	windows/dos/12741.py
(Gabriel's FTP Server) Open & Compact FTPD 1.2 - Buffer Overflow (Metasploit)	windows/remote/11742.rb
(Gabriel's FTP Server) Open & Compact FTPD 1.2 - Crash (PoC)	windows/dos/11391.py
(Gabriel's FTP Server) Open & Compact FTPD 1.2 - Remote Overflow	windows/remote/11420.py
.NET Framework - Tilde Character Denial of Service	windows/dos/19575.txt
.NET Remoting Services - Remote Command Execution	windows/remote/35280.txt
.NET Runtime Optimization Service - Local Privilege Escalation	windows/local/16948.c
BitCr-client 1345 build20060203 - Denial of Service	windows/dos/2547.c
1 Click Audio Converter 2.3.6 - ActiveX Local Buffer Overflow	windows/local/37211.html
1 Click Extract Audio 2.3.6 - ActiveX Buffer Overflow	windows/local/37212.html
10-Strike Bandwidth Monitor 3.7 - Local Buffer Overflow (SEH)	windows/local/44585.py
10-Strike Bandwidth Monitor 3.9 - Buffer Overflow (SEH) (ASLR + DEP Bypass)	windows/local/44578.py
10-Strike LANState 8.8 - Local Buffer Overflow (SEH)	windows/local/45886.py
10-Strike Network File Search Pro 2.3 - Local Buffer Overflow (SEH)	windows/local/44893.py
10-Strike Network Inventory Explorer - 'svInventoryWebServer' Unquoted Service Path	windows/local/48231.txt
10-Strike Network Inventory Explorer 8.54 - 'Add' Local Buffer Overflow (SEH)	windows/local/48233.py
10-Strike Network Inventory Explorer 8.54 - 'Registration Key' Buffer Overflow (SEH)	windows_x86/local/44840.py
10-Strike Network Inventory Explorer 8.54 - Local Buffer Overflow (SEH)	windows_x86/local/44838.py
10-Strike Network Inventory Explorer 8.54 - Local Buffer Overflow (SEH) (DEP Bypass)	windows/local/48243.py
10-Strike Network Inventory Explorer 8.65 - Buffer Overflow (SEH)	windows/local/49116.py
10-Strike Network Inventory Explorer 9.03 - 'Read from File' Buffer Overflow (SEH) (ROP)	windows/local/48244.py
10-Strike Network Inventory Explorer Pro 9.05 - Buffer Overflow (SEH)	windows/local/49122.py
10-Strike Network Scanner 3.8 - Local Buffer Overflow (SEH)	windows_x86/local/44841.py
10Strike LANState 9.32 - 'Force Check' Buffer Overflow (SEH)	windows/local/48277.py
123 FlashChat 7.8 - Multiple Vulnerabilities	windows/remote/14658.txt
13y1.67 - '.mdu' Local Stack Overflow (PoC)	windows/dos/8484.pl
1C: Arcadia Internet Store 1.0 - Arbitrary File Disclosure	windows/remote/20847.txt
1C: Arcadia Internet Store 1.0 - Path Disclosure	windows/dos/20949.c
1C: Arcadia Internet Store 1.0 - Denial of Service	windows/dos/20949.c
1C: Arcadia Internet Store 1.0 - Path Disclosure	windows/remote/20948.txt

This will list out all remote based windows attack

Exploit Title	Path
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - 'PORT' Remote Denial of Service	windows/dos/12698.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Authentication Bypass / Directory Traversal SAM Retrieval	windows/remote/27441.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Full System Access	windows/remote/13932.py
(Gabriel's FTP Server) Open & Compact FTPD 1.2 - Buffer Overflow (Metasploit)	windows/remote/11742.rb
(Gabriel's FTP Server) Open & Compact FTPD 1.2 - Remote Overflow	windows/remote/11420.py
.NET Remoting Services - Remote Command Execution	windows/remote/35280.txt
123 FlashChat 7.8 - Multiple Vulnerabilities	windows/remote/14658.txt
1C: Arcadia Internet Store 1.0 - Arbitrary File Disclosure	windows/remote/20847.txt
1C: Arcadia Internet Store 1.0 - Path Disclosure	windows/remote/20948.txt
1CLICK DVD Converter 2.1.7.1 - Multiple DLL Loading Arbitrary Code Execution Vulnerabilities	windows/remote/34848.c
20RE HomePortal Series - Directory Traversal	windows/remote/22562.html
2X ApplicationServer 10.1 - 'TuxSystem Class ActiveX Control' Remote File Overwrite	windows/remote/18625.txt
2X Client for RDP 10.1.3204 - 'ClientSystem Class ActiveX Control' Download and Execute	windows/remote/18624.txt
2X ThinClientServer 5.0 sp1-r3497 /FTP Service - Directory Traversal	windows/remote/21562.txt
3.0/4.0/4.2 MEDCOM MailServer - Control-Service Buffer Overflow	windows/remote/21526.c
32bit FTP (09.04.24) - 'Banner' Remote Buffer Overflow	windows_x86/remote/8614.py
32bit FTP (09.04.24) - 'Banner' Remote Buffer Overflow (PoC)	windows_x86/dos/8611.pl

Listing windows local exploit

Exploit Title	Path
Armitage 4.2 - 'log file name' Local Stack-based Buffer Overflow	windows/local/46922.py
Freebind 1.3.1 - 'FreebindService' Unquoted Service Path	windows/local/48844.txt

Listing all remote Apache based exploits

Exploit Title	Path
Apache (Windows x86) - Chunked Encoding (Metasploit)	windows_x86/remote/16782.rb
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution	php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution - Scanner	php/remote/29290.c
Apache - httpOnly Cookie Disclosure	multiple/remote/18442.html
Apache - Remote Memory Exhaustion (Denial of Service)	multiple/dos/17696.pl
Apache 0.8.x/1.0.x / MCSA HTTP 5.x - 'test.cgi' Directory Listing	CS/remote/28435.txt
Apache 1.0/2.0/2.2 - Server Address Disclosure	multiple/remote/21807.c
Apache 1.3 + PHP 3 - File Disclosure	multiple/remote/28686.pl
Apache 1.3 - Artificially Long Slash Path Directory Listing (1)	multiple/remote/28692.pl
Apache 1.3 - Artificially Long Slash Path Directory Listing (2)	multiple/remote/28693.c
Apache 1.3 - Artificially Long Slash Path Directory Listing (3)	multiple/remote/28694.pl
Apache 1.3 - Artificially Long Slash Path Directory Listing (4)	multiple/remote/28695.pl
Apache 1.3 - Directory Index Disclosure	multiple/remote/21802.txt
Apache 1.3.12 - WebDAV Directory Listings	linux/remote/28210.txt
Apache 1.3.14 - Mac File Protection Bypass	osx/remote/28911.txt
Apache 1.3.20 (Win32) - 'PHP.exe' Remote File Disclosure	windows/remote/22184.txt

Searching exploit by name

Exploit Title	Path
Microsoft Windows 7 (x64) - 'afd.sys' Dangling Pointer Privilege Escalation (MS14-040)	windows_x86-64/local/19525.py
Microsoft Windows 7 (x86) - 'afd.sys' Dangling Pointer Privilege Escalation (MS14-040)	windows_x86/local/19446.py

Different exploits present in ftp 2.3.4 version number

Exploit Title	Path
FileZilla 3.0.10 Professional < 3.0.10 - Local Buffer Overflow (SEH)	windows/dos/13115.py
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	hardware/remote/1881.c
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	multiple/remote/13748.py
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	multiple/remote/28733.c
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	linux_x86-64/remote/45088.c
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	linux/remote/45081.py
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	windows/local/13148.txt
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	windows/remote/17859.py
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	ruby/local/13181.rb
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	linux/local/17989.c
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	multiple/local/17177.sh
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	windows/dos/13115.py
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	windows/dos/13115.py
FileZilla 3.0.10 Professional < 3.0.10 - Remote Buffer Overflow (Metasploit)	unix/remote/17495.py