searchsploit Cheatsheet (ingenieriainformatica.uniovi.es)

Public exploit offline browsing tool

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

GENERAL USAGE

```
searchsploit [options] term1 [term2] ... [termN]
```

NOTES

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

You can use any number of search terms

By default, search terms are not case-sensitive, ordering is irrelevant, and will search between version ranges

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

And/Or '-s' if you wish to look for an exact version 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 using '--nmap', adding '-v' (verbose), it will search for even more combinations

When updating or displaying help, search terms will be ignored

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

--colour: Disable colour highlighting in search results

--id: Display the EDB-ID value rather than local path

NON-SEARCHING

-h, --help: Show this help screen

-m, --mirror **[EDB-ID]**: Mirror (aka copies) an exploit to the current working directory

-u, --update: Check for and install any exploitdb package updates (brew, deb & git)

-x, --examine **[EDB-ID]**: Examine (aka opens) the exploit using $PAGER

AUTOMATION

```
root@kali:~# searchsploit telnet
---------------------------------------------------------- ---------------------------------
 Exploit Title                                            |  Path
                                                          | (/usr/share/exploitdb/)
---------------------------------------------------------- ---------------------------------
3Com SuperStack II PS Hub 40 - TelnetD                    | exploits/hardware/remote/21011.pl
602Pro LAN SUITE 2002 - Telnet Proxy                      | exploits/windows/dos/21694.pl
APC WEB/SNMP Management Card (9606) Fi                    | exploits/hardware/dos/20654.pl
AbsoluteTelnet 10.16 - 'License name'                     | exploits/windows/dos/46874.py
Apple Mac OSX 10.2 - Terminal.APP Teln                    | exploits/osx/local/21815.txt
Arescom NetDSL-1000 - 'TelnetD' Remote                    | exploits/hardware/dos/1464.c
BSD - 'TelnetD' Remote Command Executi                    | exploits/bsd/remote/19520.txt
BSD - 'TelnetD' Remote Command Executi                    | exploits/bsd/remote/409.c
Beck IPC GmbH IPC@CHIP - TelnetD Login                    | exploits/multiple/remote/20881.txt
Byte Fusion BFTelnet 1.1 - Long Userna                    | exploits/windows/dos/19596.txt
CCProxy 6.2 - Telnet Proxy Ping Overfl                    | exploits/windows/remote/4360.rb
Celestial Software AbsoluteTelnet 2.0/                    | exploits/windows/remote/22229.pl
D-Link Devices - UPnP SOAP TelnetD Com                    | exploits/unix/remote/28333.rb
FreeBSD - Telnet Service Encryption Ke                    | exploits/bsd/remote/18369.rb
FreeBSD 7.0-RELEASE - Telnet Daemon Pr                    | exploits/freebsd/local/8055.txt
GNU inetutils < 1.9.4 - 'telnet.c' Mul                    | exploits/linux/dos/45982.txt
GoodTech Telnet Server 4.0 - Remote De                    | exploits/windows/dos/23506.txt
GoodTech Telnet Server 5.0.6 - Remote                     | exploits/windows/remote/16817.rb
GoodTech Telnet Server < 5.0.7 - Buffe                    | exploits/windows/dos/882.cpp
GoodTech Telnet Server < 5.0.7 - Remot                    | exploits/windows/remote/883.c
GoodTech Telnet Server NT 2.2.1 - Deni                    | exploits/windows/dos/19666.txt
Herospeed - 'TelnetSwitch' Remote Stac                    | exploits/hardware/remote/43997.py
Hilgraeve HyperTerminal 6.0 - Telnet B                    | exploits/windows/dos/20307.txt
IRIX 5.2/5.3/6.x - TelnetD Environment                    | exploits/irix/remote/20149.c
Jordan Windows Telnet Server 1.0/1.2 -                    | exploits/windows/remote/23491.pl
Jordan Windows Telnet Server 1.0/1.2 -                    | exploits/windows/remote/23492.c
Jordan Windows Telnet Server 1.0/1.2 -                    | exploits/windows/remote/23493.txt
Kroum Grigorov KpyM Telnet Server 1.0                     | exploits/windows/dos/23530.c
Linux BSD-derived Telnet Service Encry                    | exploits/linux/remote/18368.rb
Microsoft Internet Explorer 5.0.1/5.5/                    | exploits/windows/remote/20680.html
Microsoft Windows 95/98 Internet Explo                    | exploits/windows/local/19462.c
Microsoft Windows NT 3.5.1 SP2/3.5.1 S                    | exploits/windows/remote/19113.txt
Microsoft Windows Server 2000 - 'telne                    | exploits/windows/remote/20222.cpp
Microsoft Windows Server 2000 - Telnet                    | exploits/windows/dos/20047.txt
Microsoft Windows Server 2000 - Telnet                    | exploits/windows/dos/20907.sh
Multiple Vendor Telnet Client - Env_op                    | exploits/linux/dos/25303.txt
NETGEAR - 'TelnetEnable' Magic Packet                     | exploits/hardware/remote/44245.rb
NUUO NVRMini2 3.8 - 'cgi_system' Buffe                    | exploits/hardware/remote/45427.py
```

--nmap **[file.xml]**: Checks all results in Nmap's XML output with service version. e.g.: nmap [host] -sV -oX file.xml

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
```

by José Manuel Redondo López