# 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.

```
/usr/share/metasploit-framework
   Usage: searchsploit [options] term1 [term2] ... [termN]
 Examples
   searchsploit afd windows local
  searchsploit and windows total 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
                                                  Perform a case-sensitive search (Default is inSEnsITiVe)
     -c, —case
-e, —exact
                              [Term]
                                                  Perform an EXACT 6 order match on exploit title (Default is an AND match on each term) [Implies "-t"]
                                                 Perform an EXACT 6 order match on exploit title (Default is an AND match on each term) [Implie e.g. "WordPress 4.1" would not be detect "WordPress Core 4.1")

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")

Search JUST the exploit title (Default is title AND the file's path)

Remove values from results. By using "|" to separate, you can chain multiple values e.g. —exclude="term1|term2|term3"
     -s. -strict
           -title [Term]
-exclude="term"
## Output
    -j, -json [Term]
-o, -overflow [Term]
-p, -path [EDB-ID]
                                                  Show result in JSON format Exploit titles are allowed to overflow their columns
                                                  Show the full path to an exploit (and also copies the path to the clipboard if possible)
     -v, -verbose
                                                  Display more information in output
                                                  Show URLs to Exploit-DB.com rather than the local path Display the EDB-ID value rather than local path
                              [Term]
           -- hour
                                                  Disable colour highlighting in search results
           -colour
## Non-Searching
                                                  Mirror (aka copies) an exploit to the current working directory Examine (aka opens) the exploit using $PAGER
                              [EDB-ID]
    -m, -mirror
-x, -examine
## Non-Searching
```

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



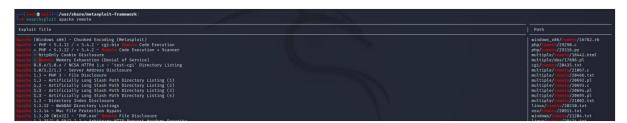
#### This will list out all remote based windows attack



### Listing windows local exploit



### Listing all remote Apache based exploits



## Searching exploit by name



### Different exploits present in ftp 2.3.4 version number

```
| Path | Juny (April American Spain | France Spain | Path | Path
```