ARYAMAN MISHRA

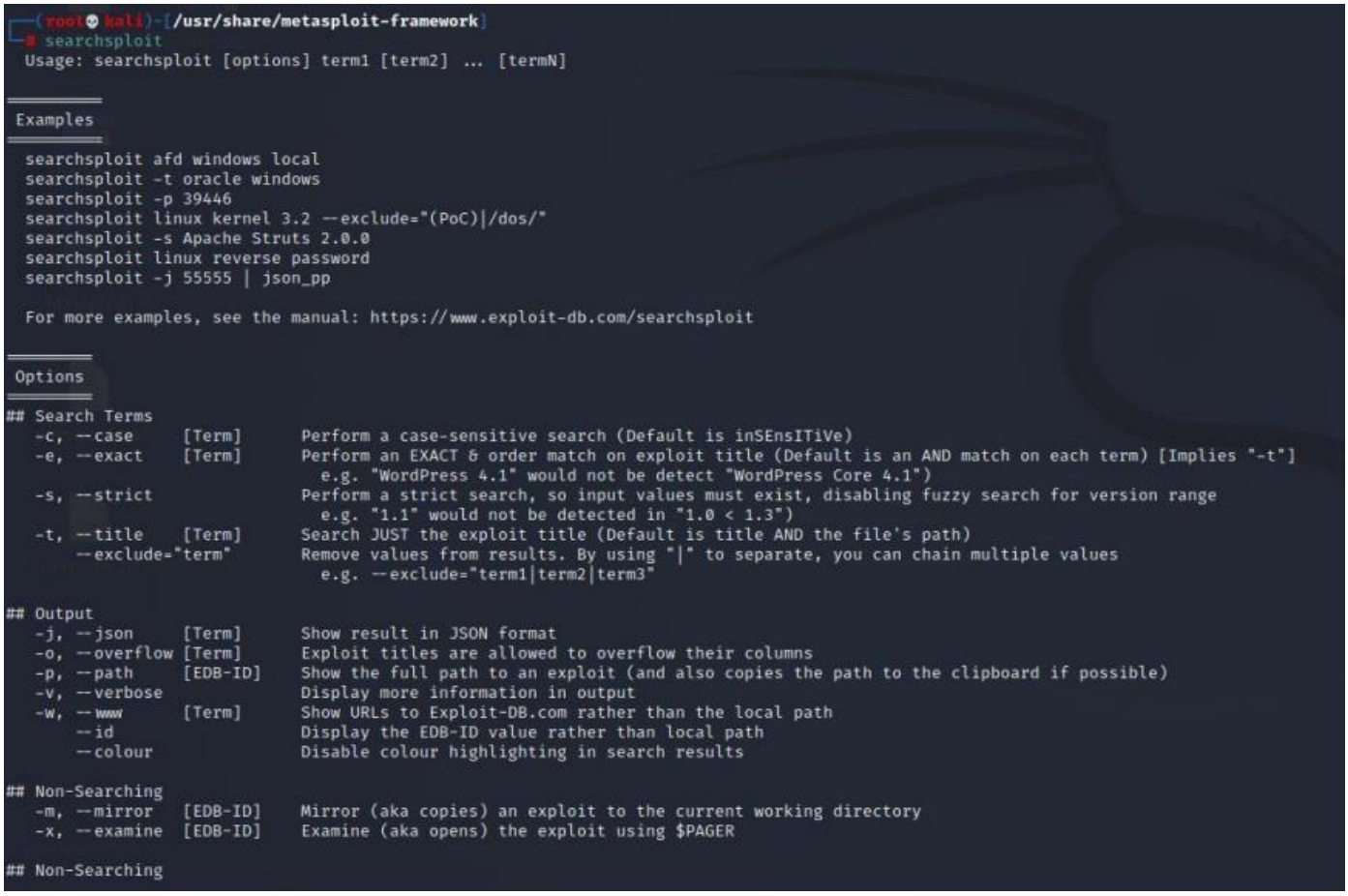
19BCE1027

Lab 7: HUNTING FOR VULNERABILITY

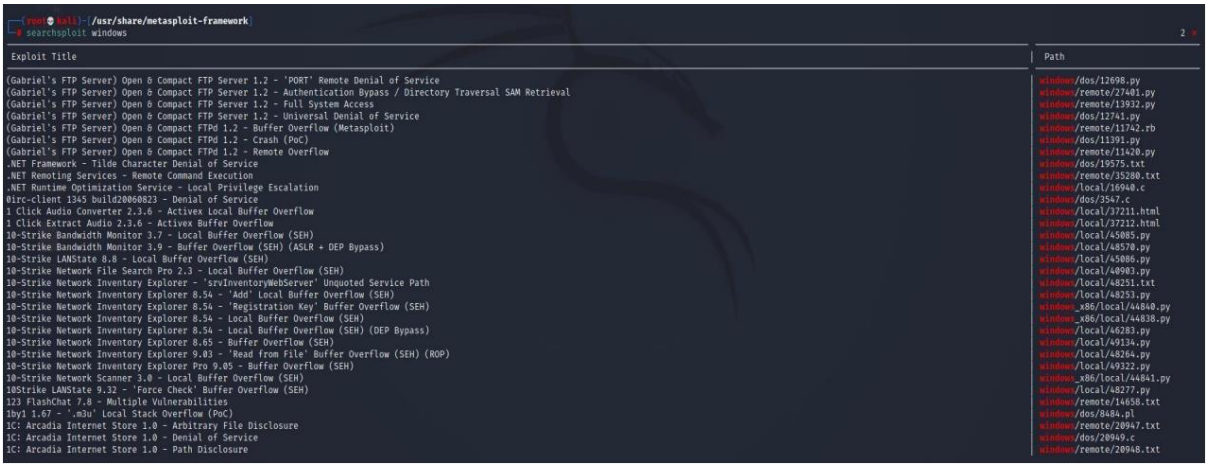
Doing offline exploit

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.



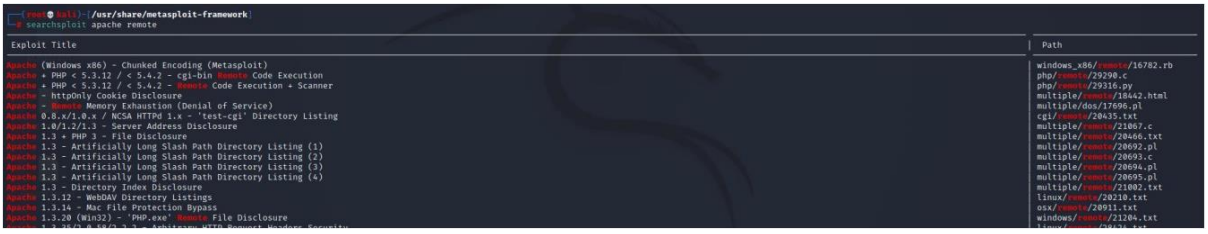
To find all windows-based exploits Exploit can be a local based or remote based



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