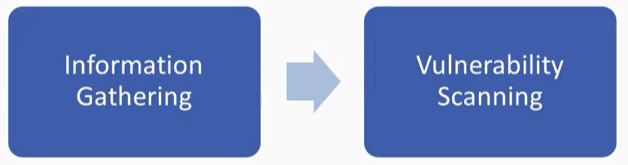
**Vulnerability Scanning with Metasploit**

* Vulnerability Scanning
* Nicto installation
* Uniscan Installation
* Web scanning with Metasploit

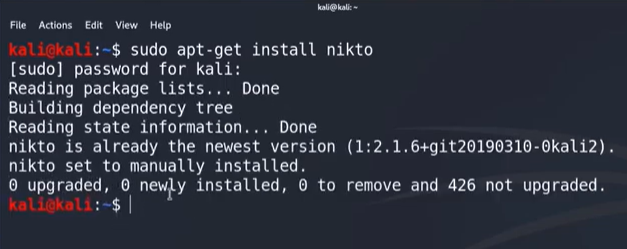
**Vulnerability Scanning:**

* It means finding loopholes in the system
* Examples are network scanning, web scanning, application scanning and so on.

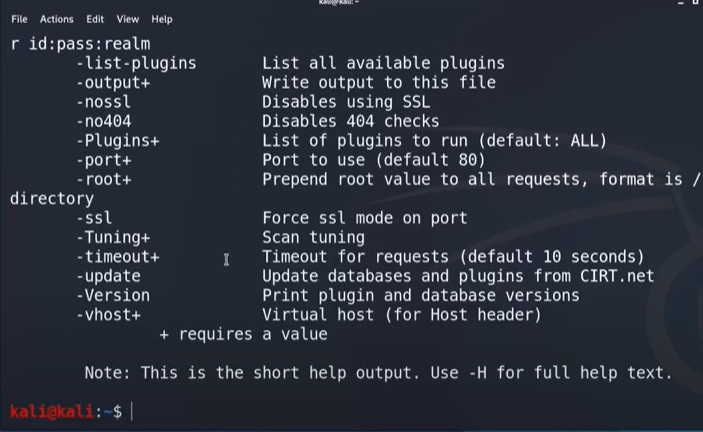


**Nicto Installation:**

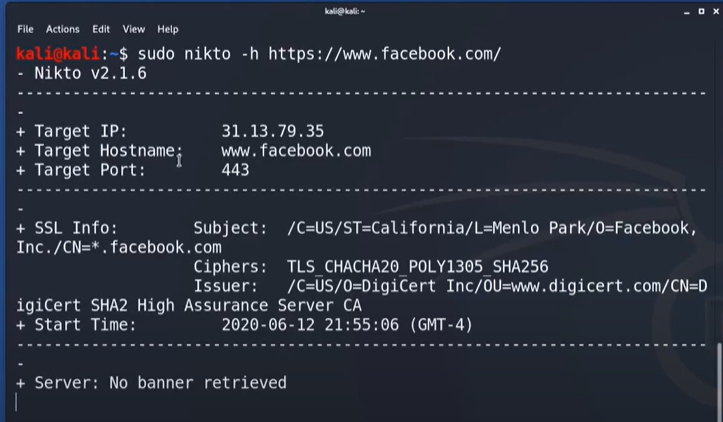
1. Type: “sudo apt -get install nikto”



1. To run Nikto type: “sudo nikto -h” (This command will show all the parameters that we can run using this tool)



1. Now type the command with the host name: “sudo nikto -h <https://www.facebook.com/>”

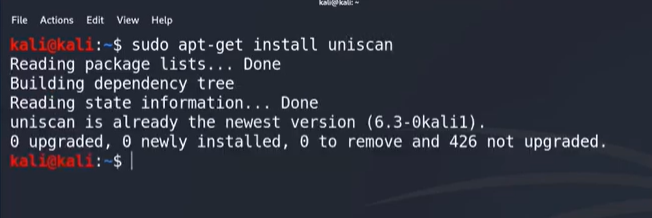


This is the old scanner, so it will take long time and also doesn’t show all the clear-cut information about the host.

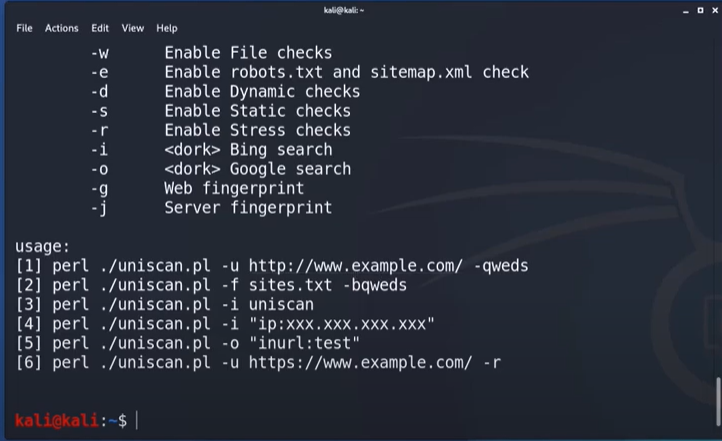
But the next scanner will provide enough information with industry standard.

**Uniscan installation:**

1. To install: “sudo apt -get install uniscan”

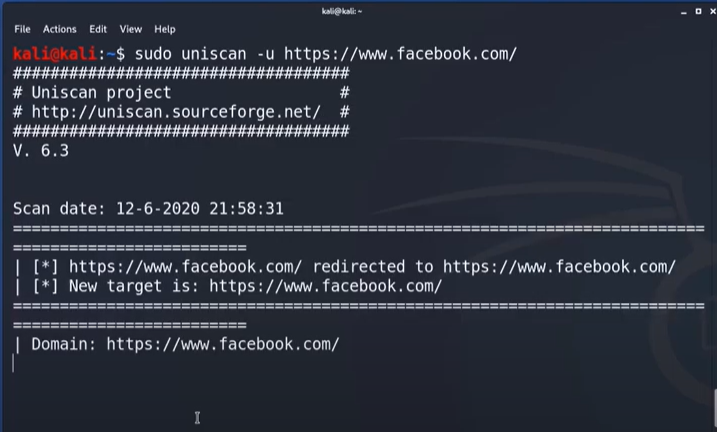


1. To check all the arguments for uniscan type : “sudo uniscan -h”



1. Now we can perform default scanning over the url:

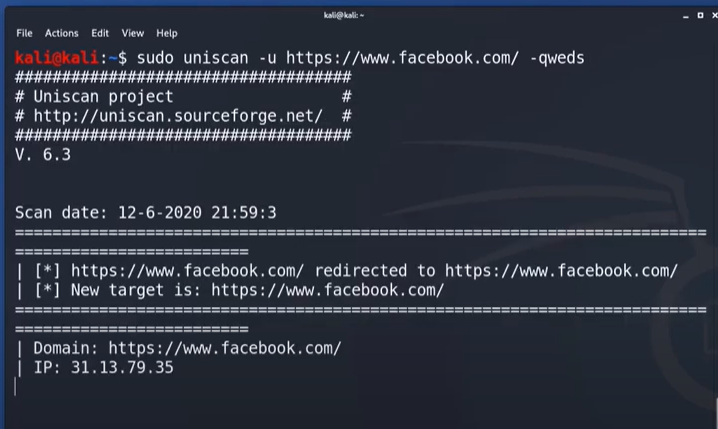
“sudo uniscan -u <https://www.facebook.com/>” (-u – to specify the url)



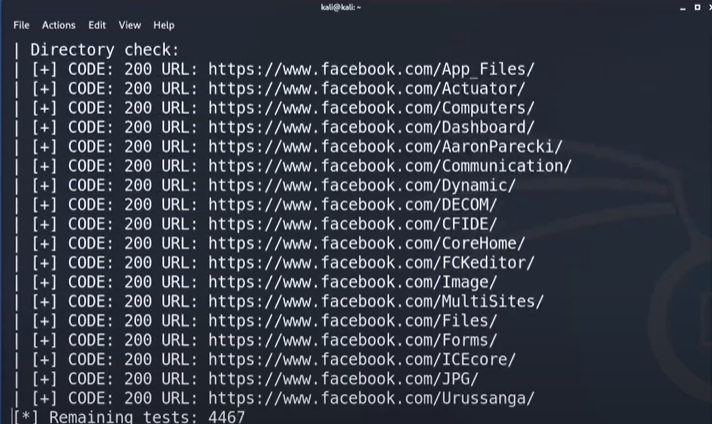
This is a default scanner which will not take much time.

1. To run this tool in more advance way add -qweds with the previous command:

“sudo uniscan -u <https://www.facebook.com/> -qweds”



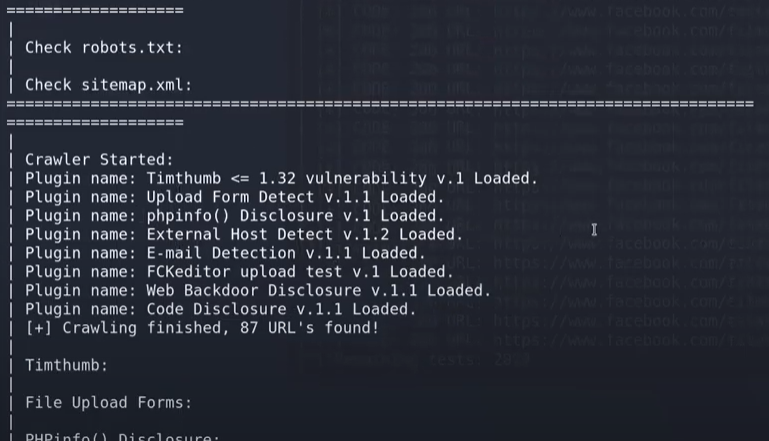
Along with the default check it will perform directory check.



It will perform file check.



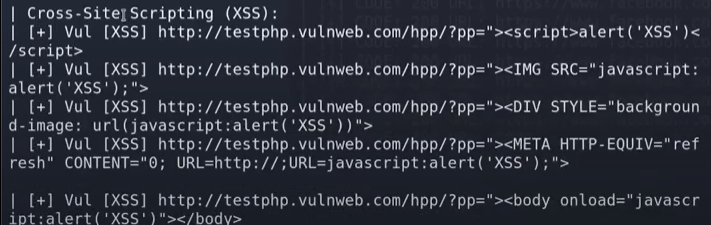
It will check for robots.txt, sitemap.xml, Crawler, External hosts, Emails etc.



It will try for SQL Injection.



It will try for Cross site scripting (XSS).



Finally, the report in the HTML format have been saved:

