Recon-ng

Recon-ng is a free and open-source tool available on GitHub. Recon-ng is based upon Open-Source Intelligence (OSINT), the easiest and most useful tool for reconnaissance. Recon-ng interface is very similar to Metasploit 1 and Metasploit 2. Recon-ng provides a command-line interface that you can run on Kali Linux. This tool can be used to get information about our target(domain). The interactive console provides several helpful features, such as command completion and contextual help. Recon-ng is a Web Reconnaissance tool written in Python. It has so many modules, database interaction, built-in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open-source web-based reconnaissance can be conducted, and we can gather all information.

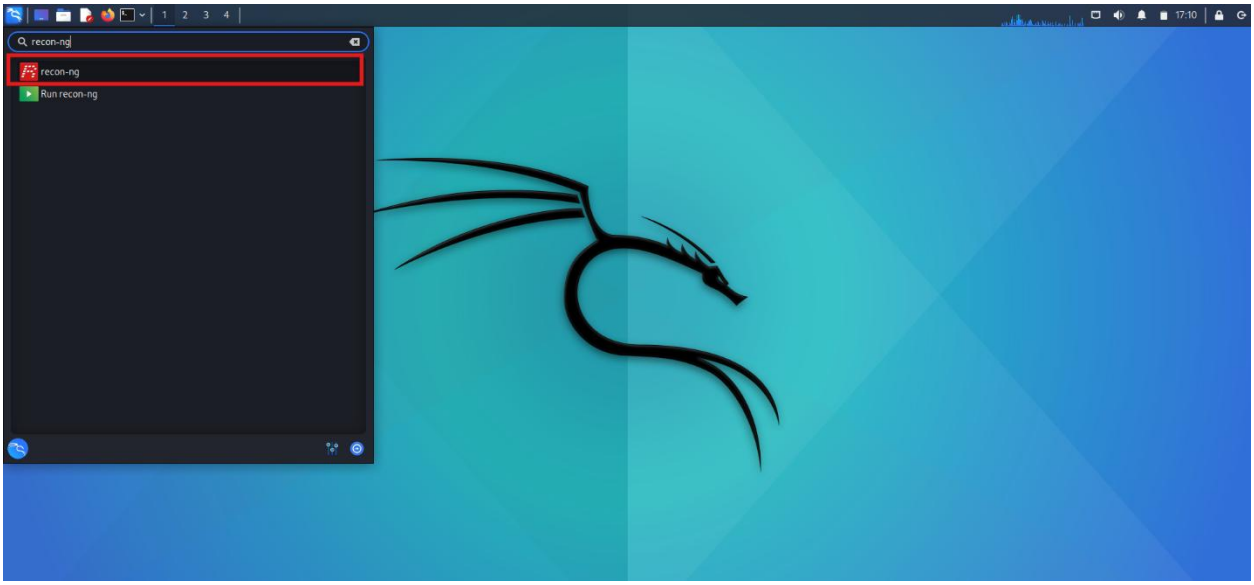
Use Case: -

1. Recon-ng is used to detect the target's IP addresses.
2. Recon-ng is used to detect Content Management Systems (CMS) using a target web application.
3. Recon-ng contains several modules which we can use to gather information about the target.
4. Recon-ng port scanner modules find closed and open ports that are used to maintain access to the server.

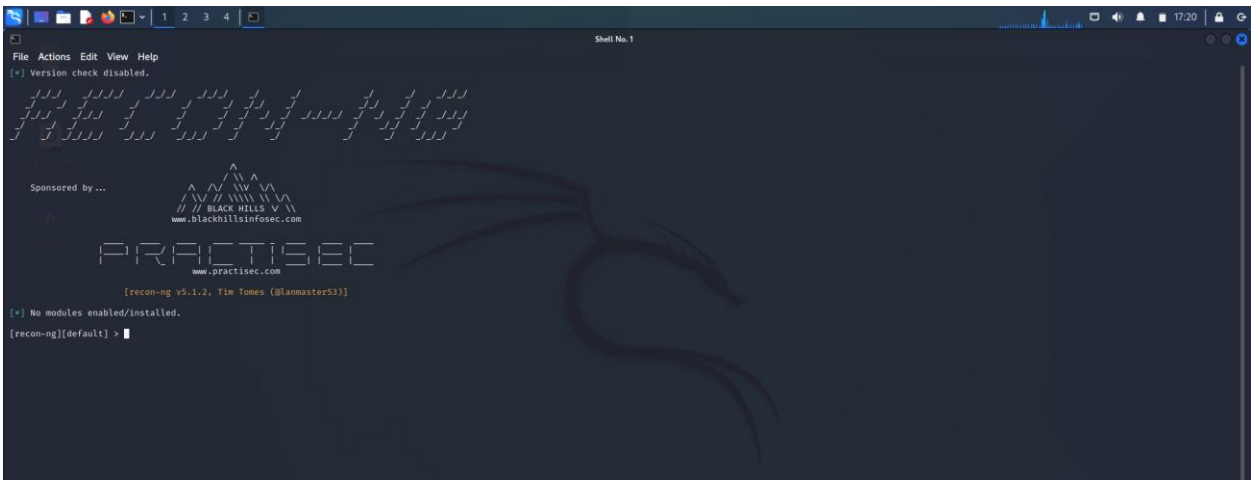
5. Recon-ng subdomain finder modules are used to find subdomains of a singer domain.
6. Recon-ng is used to find information related to the Geo-IP lookup, port scanning, Banner grabbing. Sub-domain information. DNS lookup, reverse IP using WHOIS information.
7. It is used to look for error-based SQL injections.

Steps to Install and Run: -

1. Recon-ng is pre-installed in Linux distribution you can run it by just searching it over start menu.



2. This is the Command Line Interface for the Recon-ng where we can run various commands.



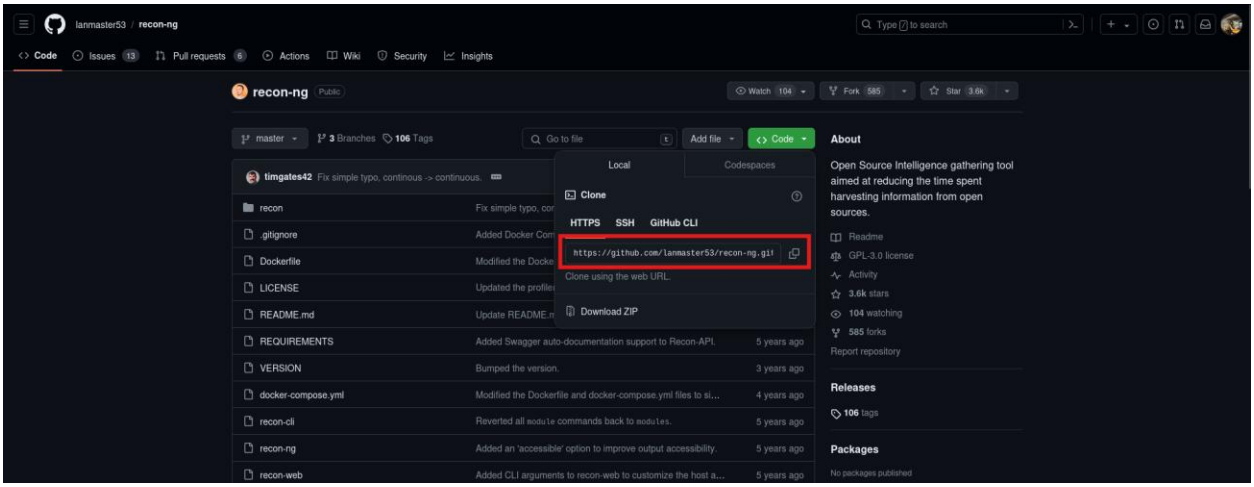
3. By simply typing help we can see all the available flags for the Recon-ng.

```
[recon-ng][default] > help

Commands (type [help|?] <topic>):
---------------------------------
back            Exits the current context
dashboard       Displays a summary of activity
db              Interfaces with the workspace's database
exit            Exits the framework
help            Displays this menu
index           Creates a module index (dev only)
keys            Manages third party resource credentials
marketplace     Interfaces with the module marketplace
modules         Interfaces with installed modules
options         Manages the current context options
pdb             Starts a Python Debugger session (dev only)
script          Records and executes command scripts
shell           Executes shell commands
show            Shows various framework items
snapshots       Manages workspace snapshots
spool           Spools output to a file
workspaces      Manages workspaces

[recon-ng][default] >
```

4. If in case Recon-ng is not pre-installed or we want to install its latest version we can clone it from github.



5. Inside the terminal use git clone command along with the copied path of the github repository. After that go to the directory and just run ./recon-ng command in order to run the tool.