**Experiment no:1**

**Recon-ng tool**

**Aim :** To perform active reconnaissance using reconnaissance tool using reco-ng

**Description:**

Recon-ng is free and open-source tool available on GitHub. Recon-ng is based upon Open-Source Intelligence (OSINT), the easiest and useful tool for reconnaissance. Recon-ng interface is very similar to Metasploit1 and Metasploit2. 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 a number of 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.

***Features of Recon-ng :***

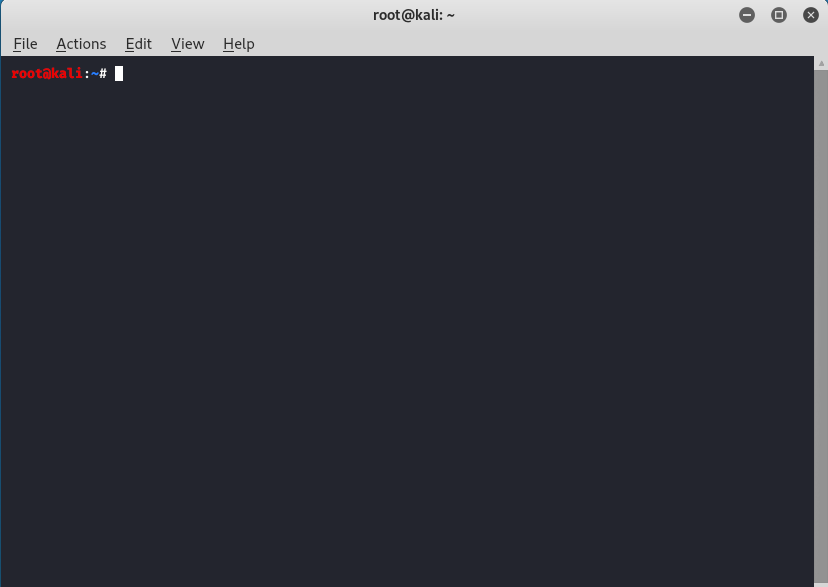
* Recon-ng is free and open-source tool this means you can download and use it at free of cost.
* Recon-ng is a complete package of information gathering modules. It has so many modules that you can use for information gathering.
* Recon-ng works and acts as a web application/website scanner.
* Recon-ng is one of the easiest and useful tool for performing reconnaissance.
* Recon-ng interface is very similar to metasploitable1 and metasploitable2 that makes is easy to use.
* Recon-ng’s interactive console provides a number of helpful features.
* Recon-ng is used for information gathering and vulnerability assessment of web applications.
* Recon-ng uses shodan search engine to scan iot devices.
* Recon-ng can easily find loopholes in the code of web applications and websites.
* Recon-ng has following modules Geoip lookup, Banner grabbing, DNS lookup, port scanning, These modules makes this tool so powerful.
* Recon-ng can target a single domain and can found all the subdomains of that domain which makes work easy for pentesters.

***Uses of Recon-ng :***

* Recon-ng is a complete package of Information gathering tools.
* Recon-ng can be used to find IP Addresses of target.
* Recon-ng can be used to look for error-based SQL injections.
* Recon-ng can be used to find sensitive files such as robots.txt.
* Recon-ng can be used to find information about Geo-IP lookup, Banner grabbing, DNS lookup, port scanning, sub-domain information, reverse IP using WHOIS lookup.
* Recon-ng can be used to detects Content Management Systems (CMS) in use of a target web application,
* InfoSploit can be used for WHOIS data collection, Geo-IP lookup, Banner grabbing, DNS lookup, port scanning, sub-domain information, reverse IP, and MX records lookup
* Recon-ng is a complete package (TOOL) for information gathering. This tool is free and Open Source.
* Recon-ng subdomain finder modules is used to find subdomains of a single domain.
* Recon-ng can be used to find robots.txt file of a website.
* Recon-ng port scanner modules find closes and open ports which can be used to maintain access to the server.
* Recon-ng has various modules that can be used to get the information about target.

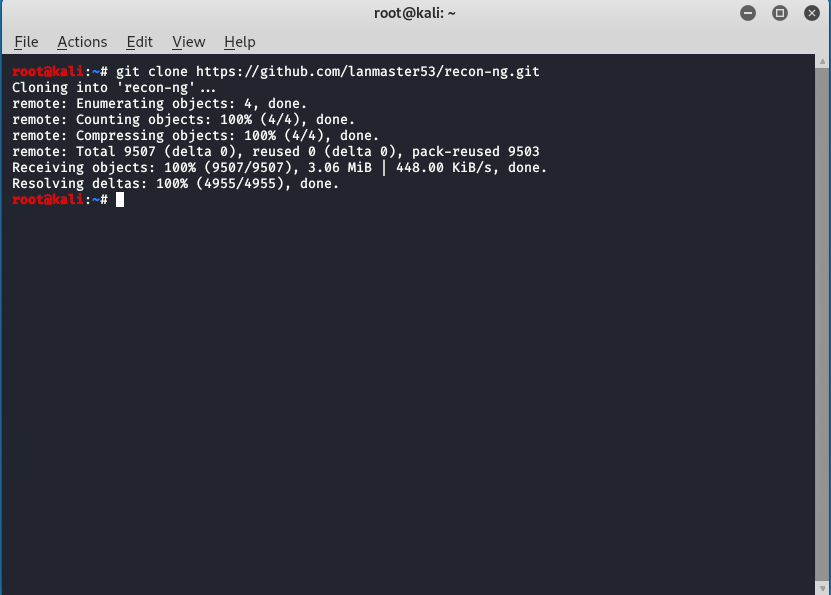
**Procedures:**

**Step 1: Open Terminal of your Kali Linux**



**Step 2:** On Terminal now type command.

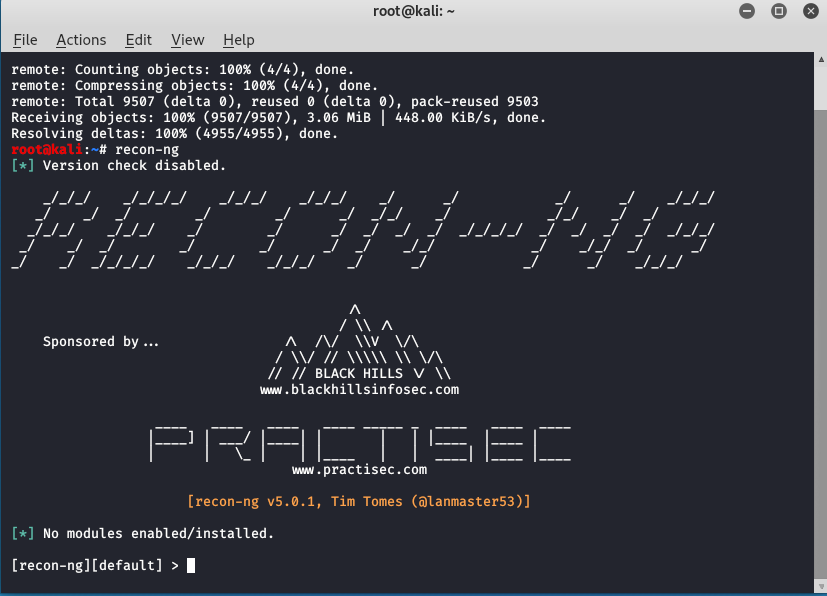
***git clone https://github.com/lanmaster53/recon-ng.git***



recon-ng has been installed on your Kali Linux ,now you just have to run recon-ng.

**Step 3:**To launch recon-ng on your kali Linux type the following the command and press enter.

***recon-ng***

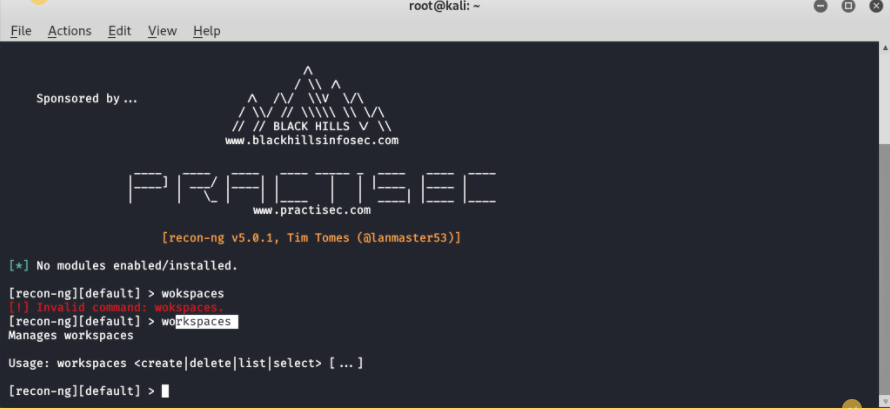


Now Recon-ng has been downloaded and running successfully.

**Step 4:**Now to do Reconnaissance first you have to create a workspace for that. Basically, workspaces are like separate spaces in which you can perform reconnaissance of different targets. To know about workspaces just type the following command.

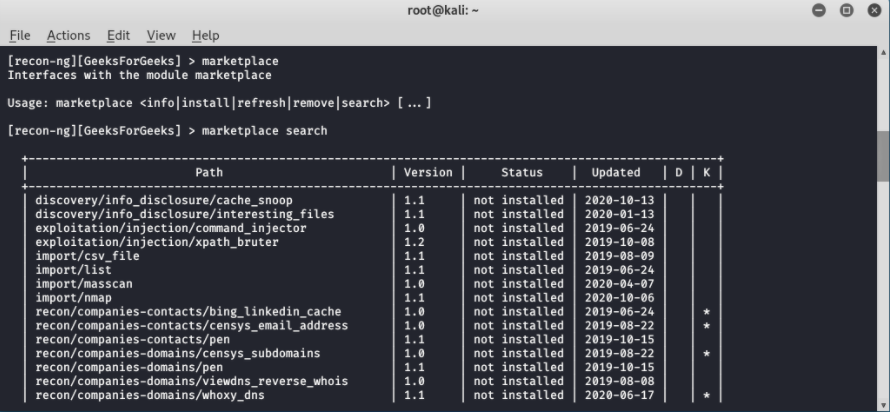
***workspaces***

***workspaces create (name)***



**Step 5:**You have created workspace for you, now you have to go to marketplace to install modules to initiate your Reconnaissance here we have created a workspace called GeeksForGeeks. Now we will Reconnaissance within GeeksForGeeks workspace. Now go to marketplace and install modules.

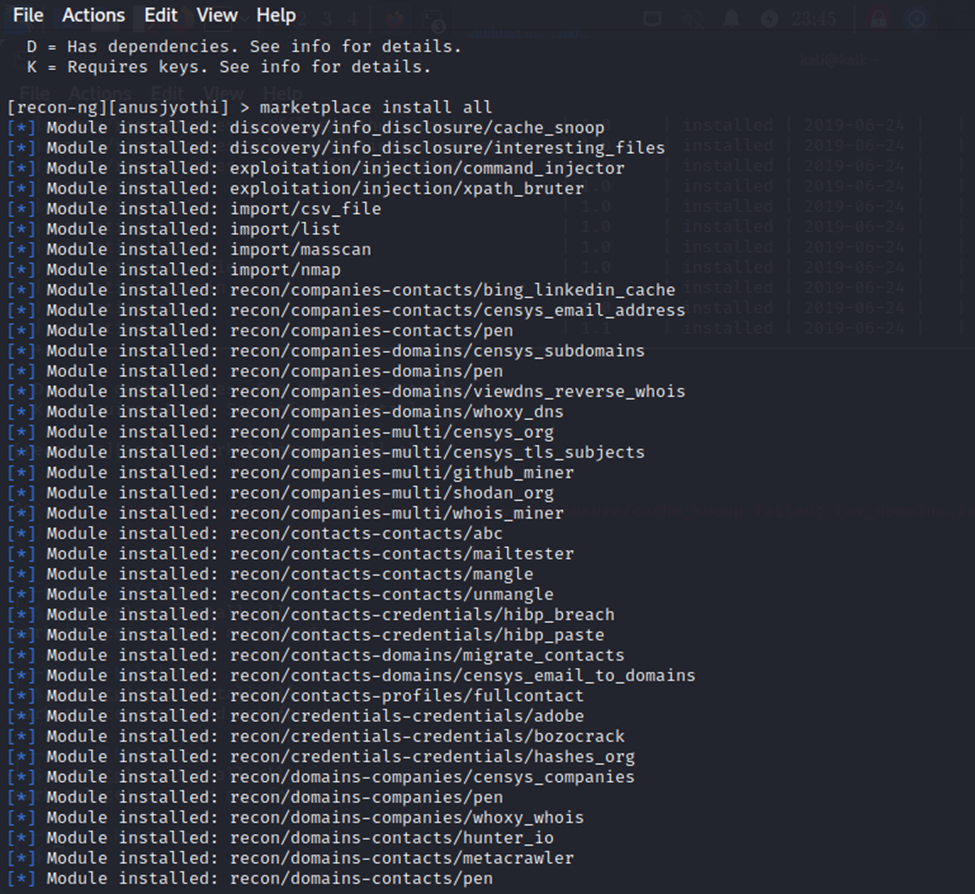
***marketplace search***



**Step 6:** As you can now see a list of modules and so many of them are not installed so to install those modules type following command.

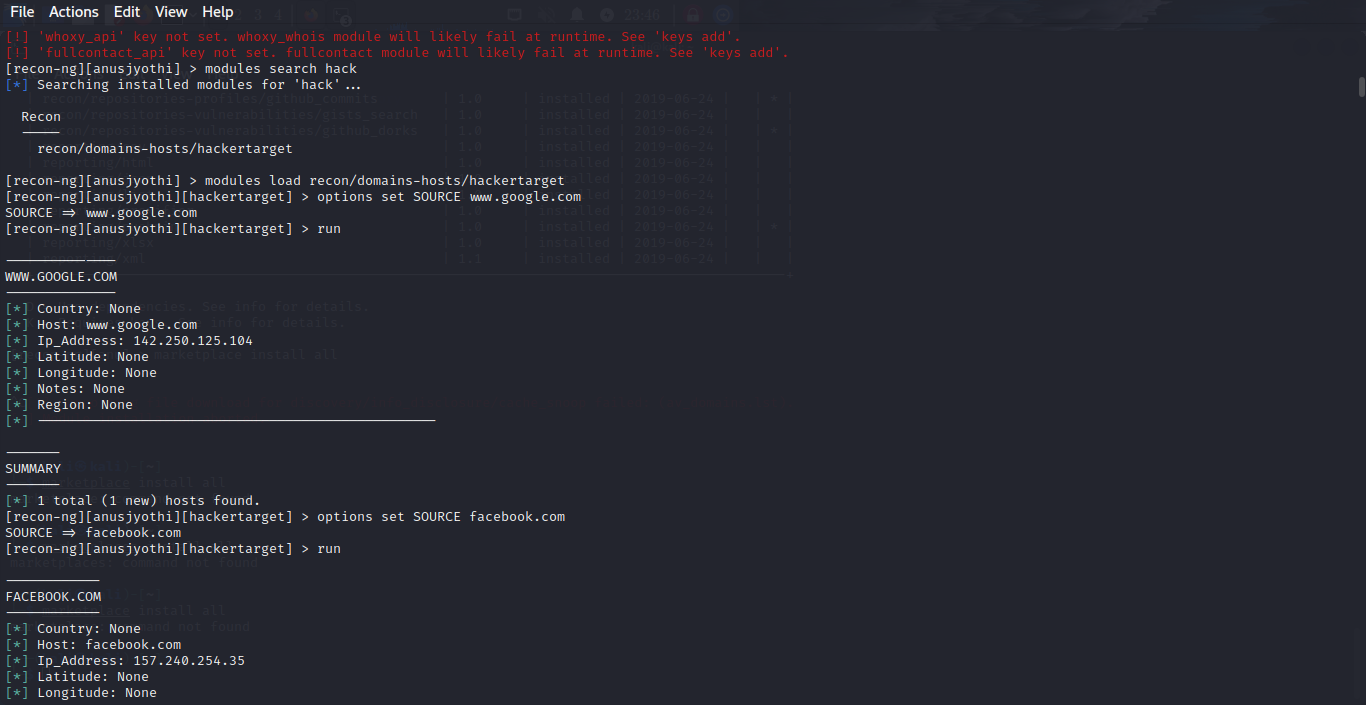
***marketplace install (module name)***

***marketplace install all***



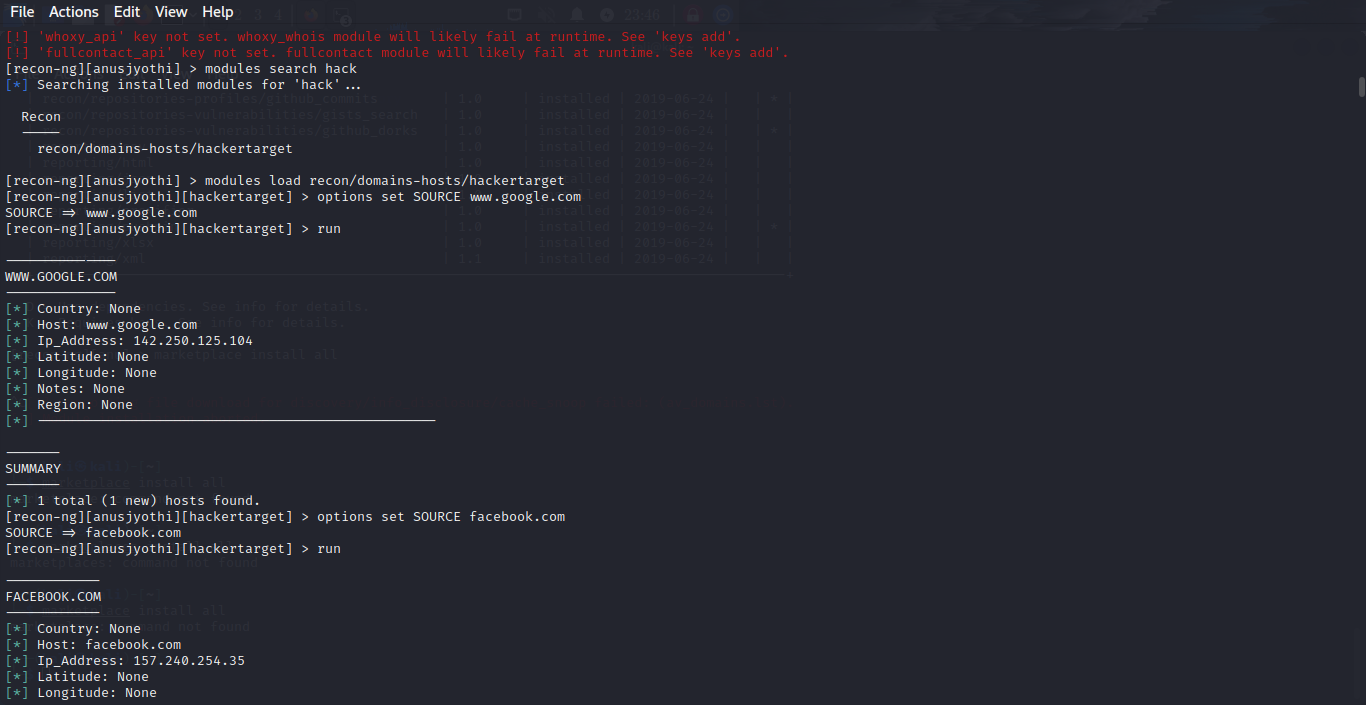
**Step 7:** Type the command

***modules search hack***



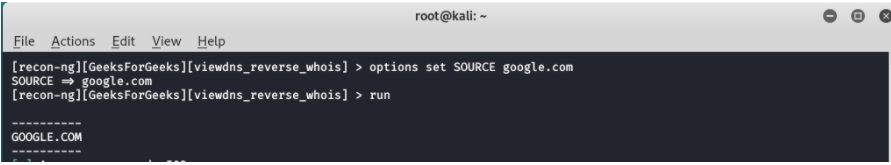
**Step 8:** As you can see that we have installed the module names recon/domains-hosts/hackertarget. Now we will load this module in our workspace.

***modules load (module name)***



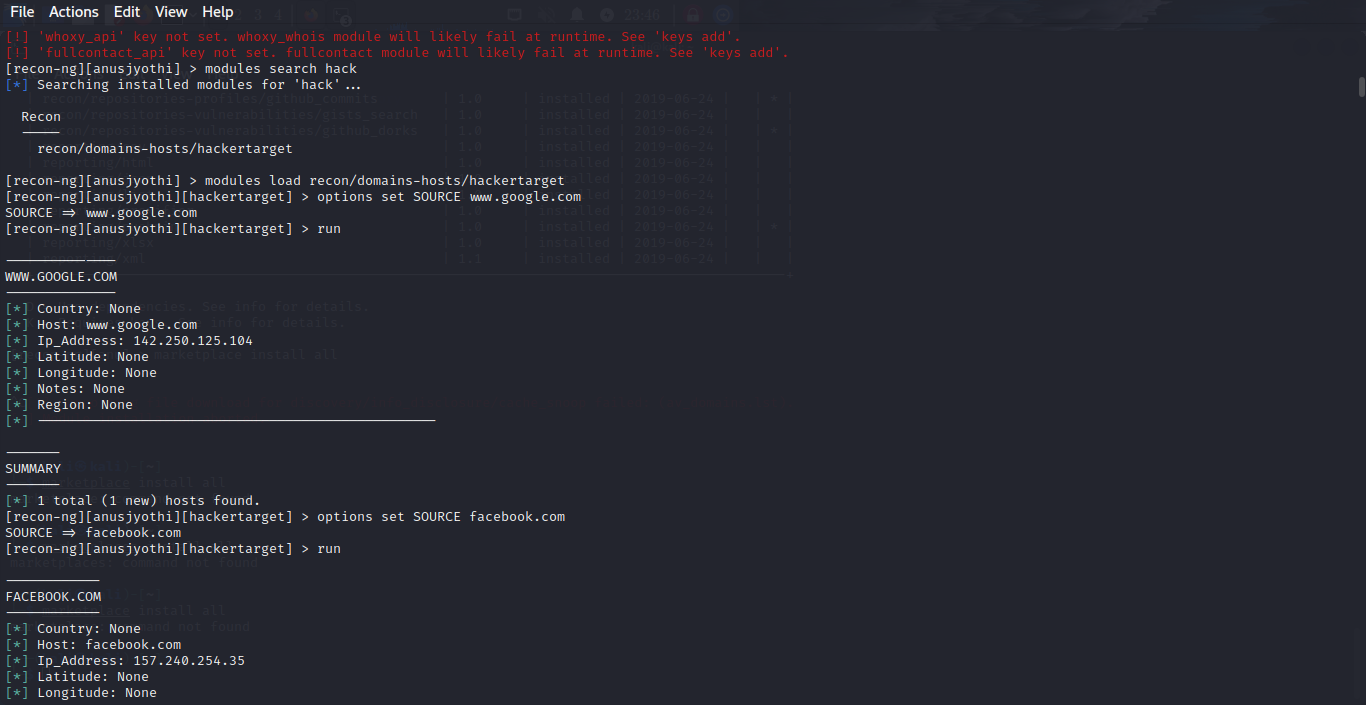
**Step 9:**As you can see now we are under those modules. Now to use this module we have to set the source.

***options set SOURCE (domain name)***



**Step 10:** Type the command

***run***



We have set google.com as a source by command options set SOURCE google.com. Recon-ng is Open-Source Intelligence, the easiest and useful tool for reconnaissance.

***RESULT***

Active reconnaissance using reconnaissance tool using recon-ng is performed.