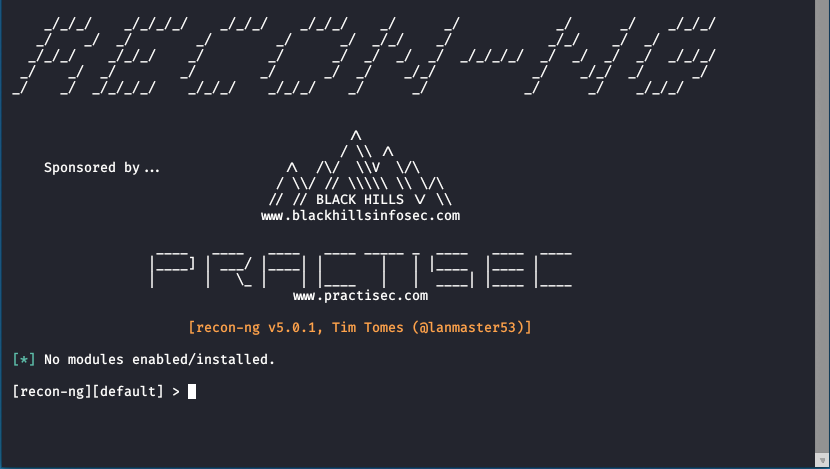
[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@b063bb6addc94ddc80b3c003b9619071?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Information Gathering with Recon-NG**

**Lession:1 Introduction to 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. The 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.

Type recon-ng

Recon-ng framework

**Features of Recon-ng :**

* Recon-ng is a free and open-source tool which means you can download and use it 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 most useful tools for performing reconnaissance.
* The recon-ng interface is very similar to metasploitable 1 and metasploitable 2 which makes it easy to use.
* Recon-ng’s interactive console provides several 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 the following modules GeoIP lookup, Banner grabbing, DNS lookup, and port scanning, These modules make this tool so powerful.
* Recon-ng can target a single domain and can find all the subdomains of that domain which makes work easy for pen-testers.

**Uses of Recon-ng:**

* Recon-ng is a complete package of Information gathering tools.
* Recon-ng can be used to find the IP Addresses of the 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, and reverse IP using WHOIS lookup.
* Recon-ng can be used to detect Content Management Systems (CMS) in the 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 are used to find subdomains of a singer domain.
* Recon-ng can be used to find the robots.txt file of a website.
* Recon-ng port scanner modules find closed and open ports which can be used to maintain access to the server.
* Recon-ng has various modules that can be used to get information about the target.

Please click on these IPS to perform this lab:

172.30.1.1/24

172.30.2.1/24

172.30.3.1/24

172.30.4.1/24

172.30.5.1/24

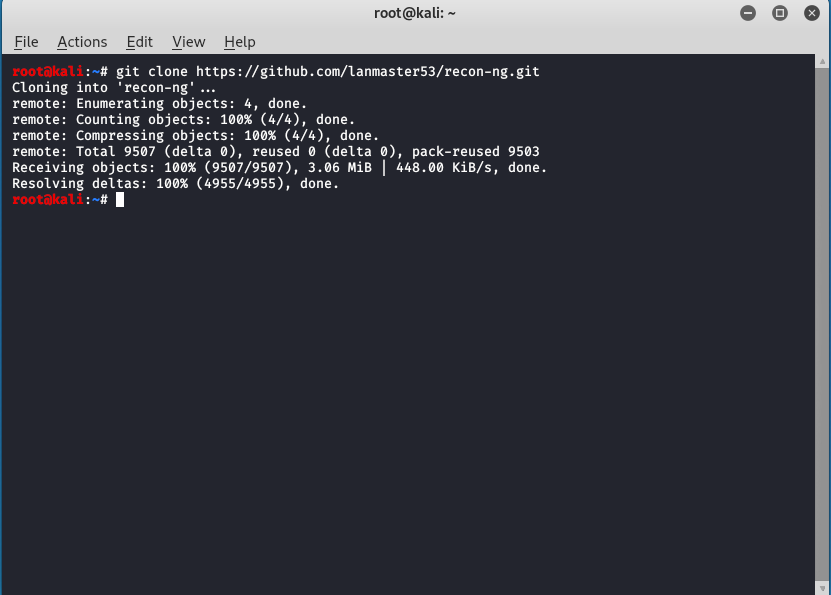
**Lession:2 Deep Dive into Recon-NG**

**Recon-ng Installation:**

Step 1: Open the Terminal of your Kali Linux



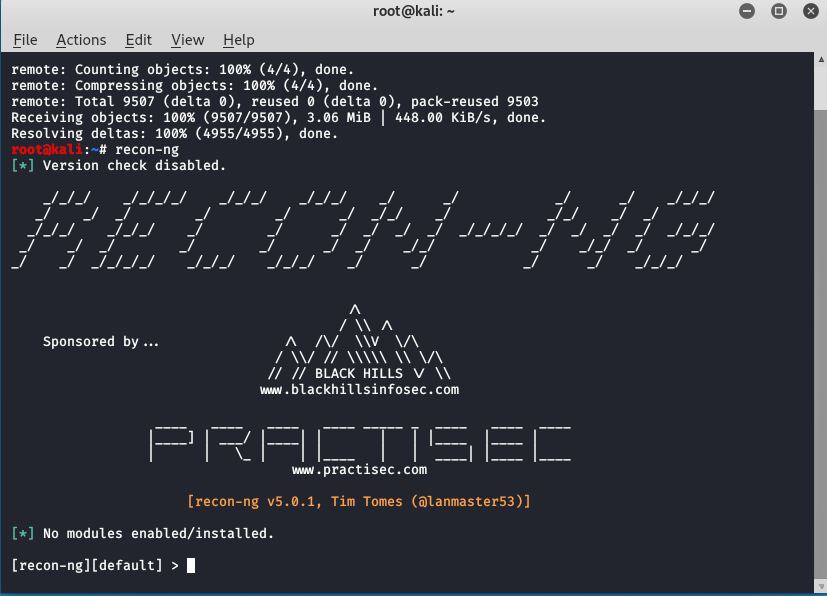
Step 2: On Terminal now type the command.

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

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

Step 3: Type the command.

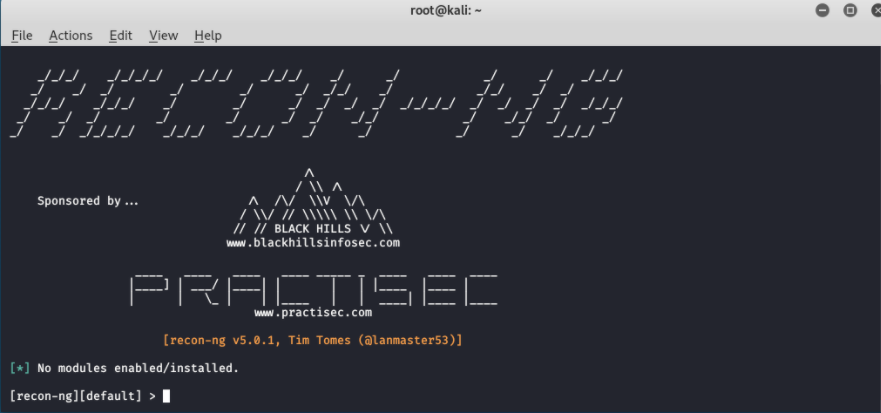
recon-ng



Now Recon-ng has been downloaded and running successfully.

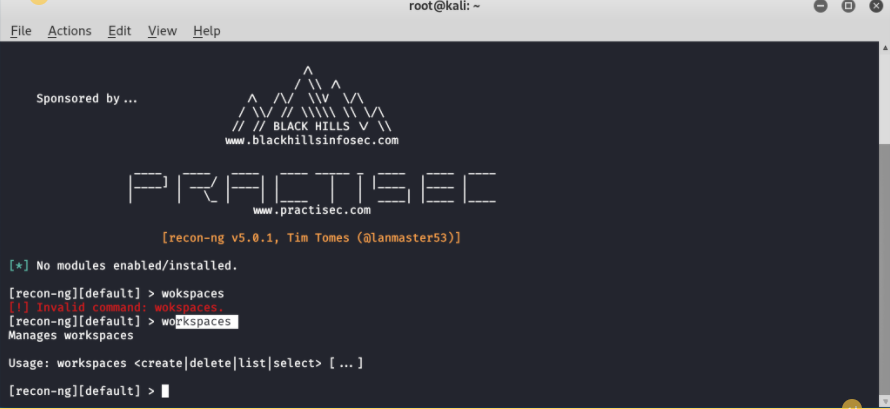
Step 4: To launch recon-ng on your kali Linux type the following command and press enter.

recon-ng



Step 5: Now to do Reconnaissance first you have to create a workspace for that. Workspaces are like separate spaces in which you can perform reconnaissance of different targets. To know about workspaces just type the following command.

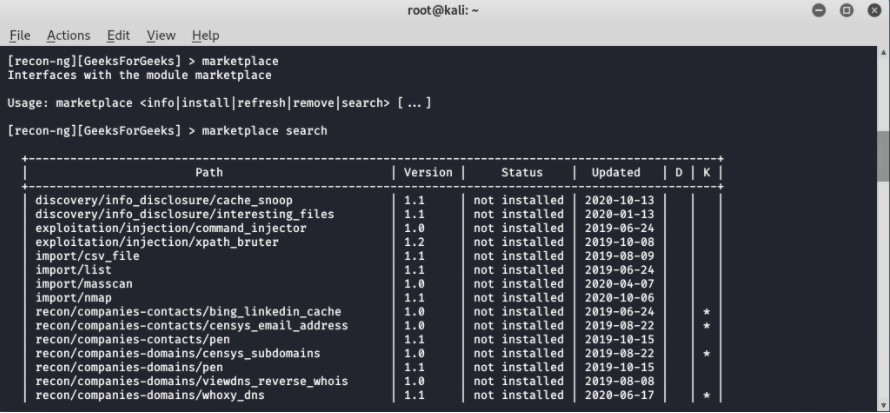
Workspaces



Step 6. You have created a workspace for yourself now you have to go to the marketplace to install modules to initiate your Reconnaissance here we have created a workspace called GeeksForGeeks. Now we will Reconnaissance within the GeeksForGeeks workspace. Now go to the marketplace and install modules.

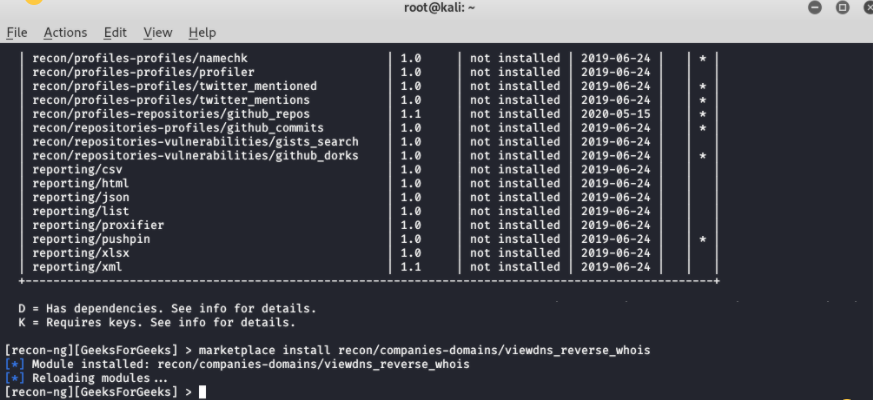
**Lession:3 Recon-ng Marketplace and Modules**

marketplace search



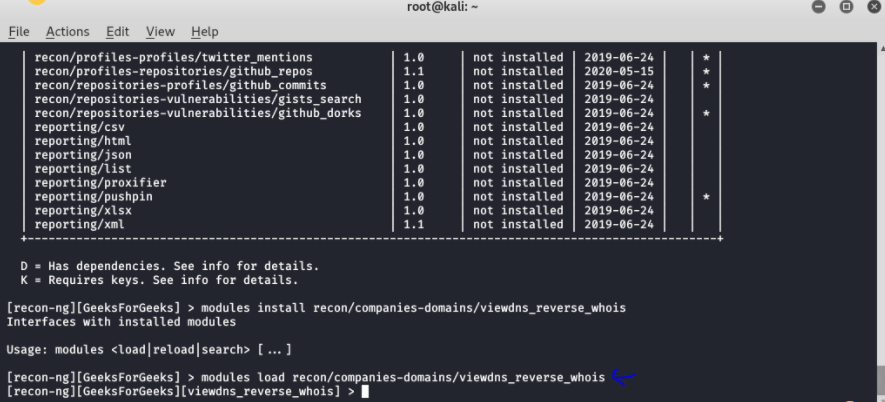
Step 7: As you can now see a list of modules and so many of them are not installed so to install those modules type the following command.

marketplace install (module name)



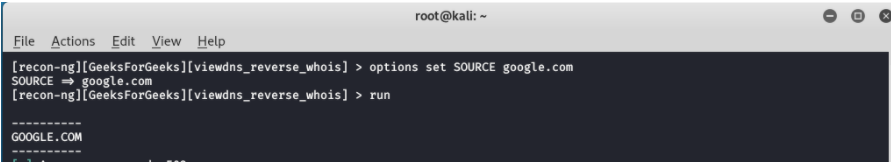
Step 8: As you can see we have installed the module names recon/companies-domains/viewdns\_reverse\_whois. Now we will load this module in our workspace GeeksForGeeks.

modules load (module name)



Step 9: As you can see now we are under those modules i.e  viewdns\_reverse\_whois. Now to use this module we have to set the source.

options set SOURCE (domain name)



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

**Lession:4 Generate Report in Recon-NG**

Recon-NG is a web reconnaissance framework that is written in Python and built on top of the Metasploit Framework. It is designed to perform various reconnaissance activities on a target domain, such as discovering subdomains, gathering email addresses, and collecting public data.

To generate a report in Recon-NG, follow these steps:

1. Run Recon-NG and select the target domain.
2. Run the desired modules to gather data about the target domain.
3. Once the data gathering is complete, use the "report" command to generate a report.
4. Specify the format of the report (HTML, CSV, or JSON).
5. Provide a filename for the report.
6. The report will be generated and saved to the specified location.

Here is an example of how to generate an HTML report in Recon-NG:

recon-ng > report html report.html

You can also generate a report for a specific module or set of modules by using the "-m" option and specifying the module(s) you want to include in the report. For example, to generate a report for the "hosts" and "contacts" modules, you can use the following command:

recon-ng > report html report.html -m hosts,contacts

I hope this helps! Let me know if you have any other questions.

**Lession:5 Recon-ng Keys**

Recon-NG keys are API keys that are used to authenticate and authorize access to certain APIs or services when using the Recon-NG web reconnaissance framework. These keys are provided by the service or API provider and are required to access and use the service.

Here is an example of how you might use a Recon-NG key:

Suppose you want to use the Recon-NG module "linkedin\_search" to search for LinkedIn profiles of specific individuals. This module requires you to have a LinkedIn API key to use it. To use the module with your LinkedIn API key, you would first need to obtain the key from LinkedIn and then add it to the Recon-NG configuration file or specify it as an option when running the module.

For example, you might run the following command to use the LinkedIn search module with your API key:

recon-ng -m linkedin\_search --api-key YOUR\_API\_KEY --first-name John --last-name Smith

In this example, "YOUR\_API\_KEY" would be replaced with the actual API key that you obtained from LinkedIn. This would allow the module to use your API key to authenticate and authorize access to the LinkedIn API, allowing you to search for LinkedIn profiles as part of your web reconnaissance.