

Department of

Bachelor of Computer Applications

**Ethical Hacking Fundamentals**

Lab File – CA 03

**Subject Code:** 19BCA4C02L

**Class:** IInd Year IInd Semester

**Prepared By:**

Suman Garai

20BCAR0246

**Aim :**

To explore and learn Recon-ng (an open-source intelligence tool) for reconnaissance.

**Requirements :**

* Virtualisation Software
* Kali Linux 2021.4a
* Basics of Maltego
* Administrator privilages
* Internet Connection

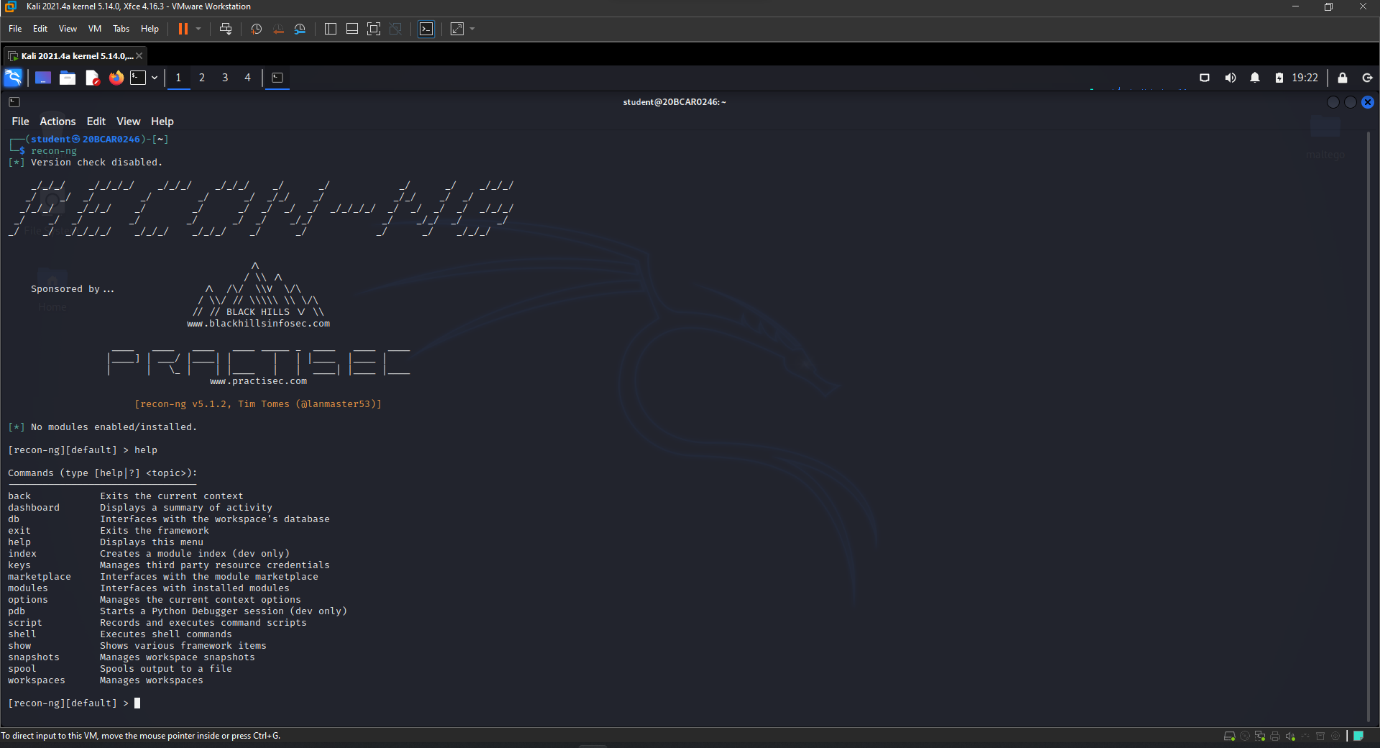
**Objectives :**

To Install & Run any module any obtain desired information using it.

**Procedure :**

Basics

1. Open root terminal in kali linux, and run the command recon-ng to run recon-ng.
2. Type Help for getting the list of working commands in recon-ng.



As we can see, a lot of options are present here. We are going to discuss a few of those as we proceed.

Following are the working/ output of shell, script, snapshot and spool commands in the tool.



Figure: shell & script commands

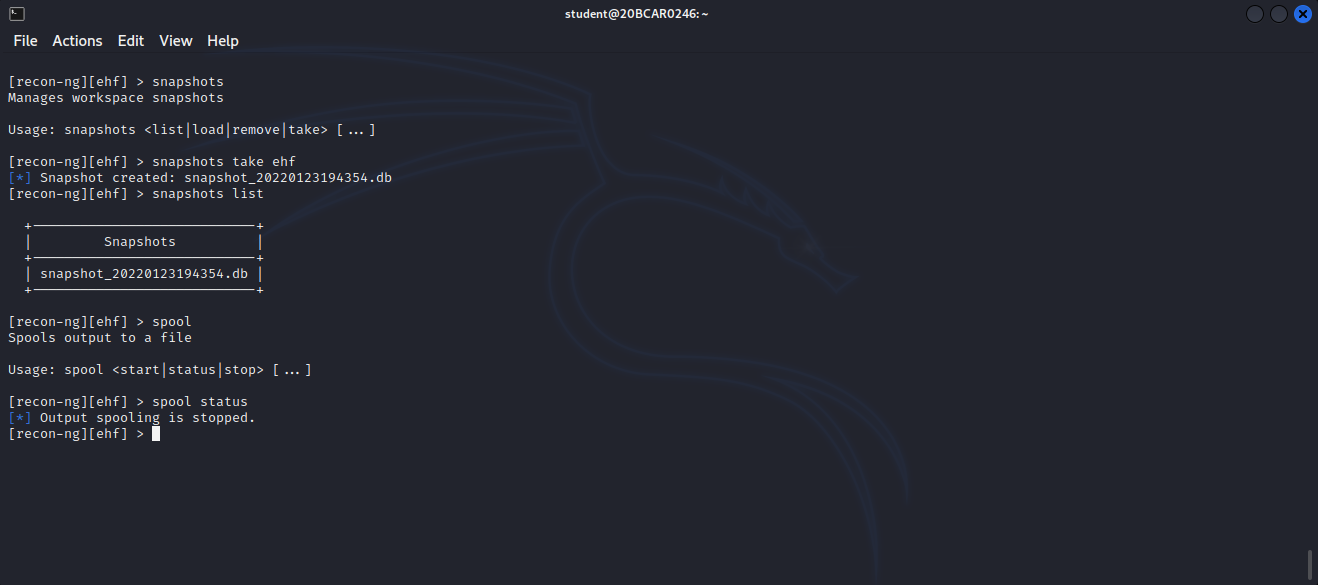


Figure: snapshot & spool

To change NAMESERVER

1. While in reconn-ng default workspace, without activating any module, type options list. We see the existing nameserver.
2. To change, type options unset and enter, to clear the existing one.
3. Then again type, options set NAMESERVER <DNS> and press enter.

The change is displayed as follows.



As we can see, the name server is changed and set, also crosschecked.

Working with Workspaces

1. To create a workspace, type workspaces create <name>. After it gets created, we automatically enter into the workspace, as is displayed as follows:

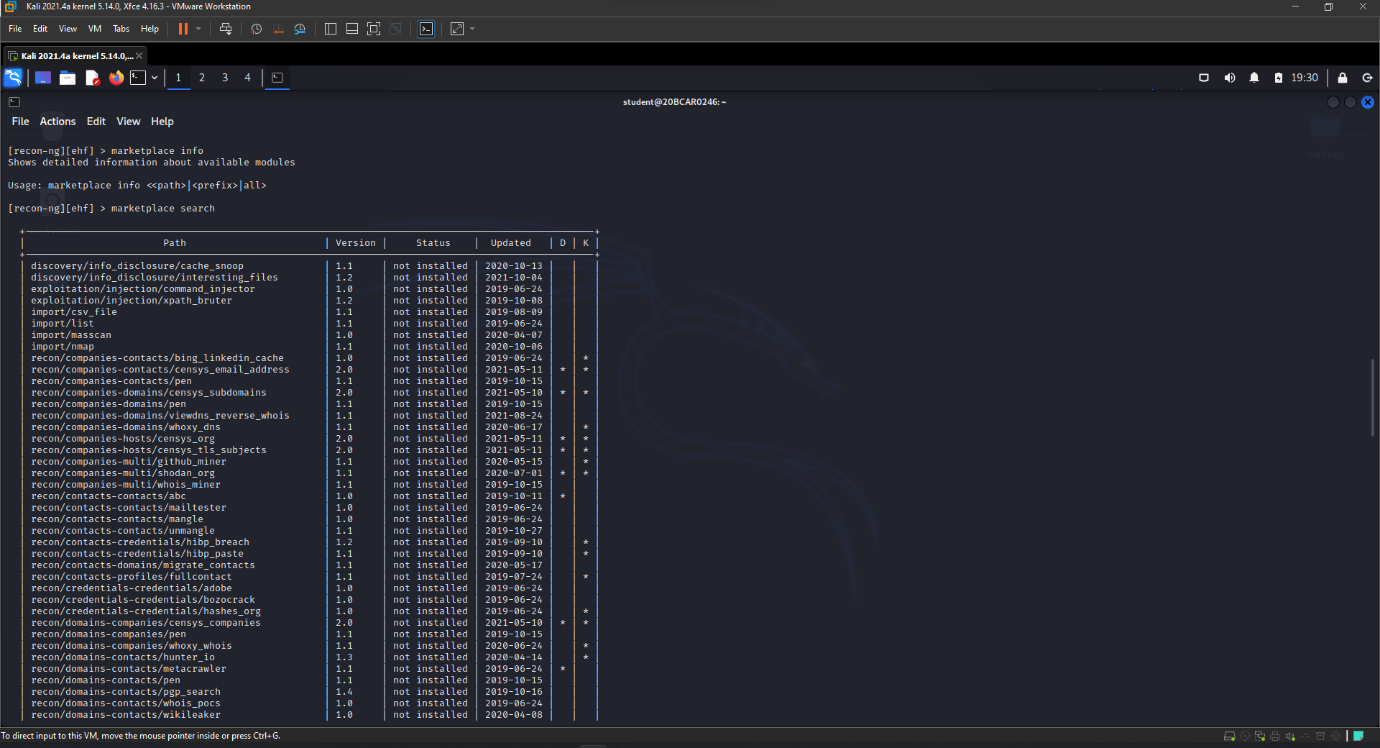


Export graph as Image

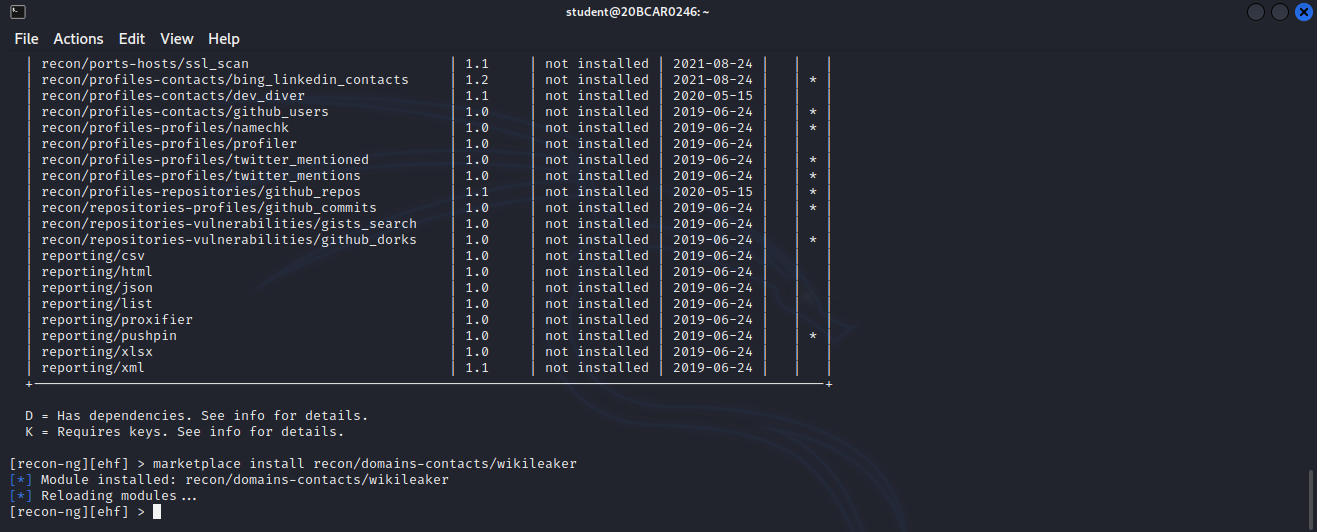
As we can see, we have entered the workspace.

Knowing the Marketplace

1. While in reconn-ng newly created workspace, without activating any module, type marketplace search. A list of modules available to install appears, displayed as follows:

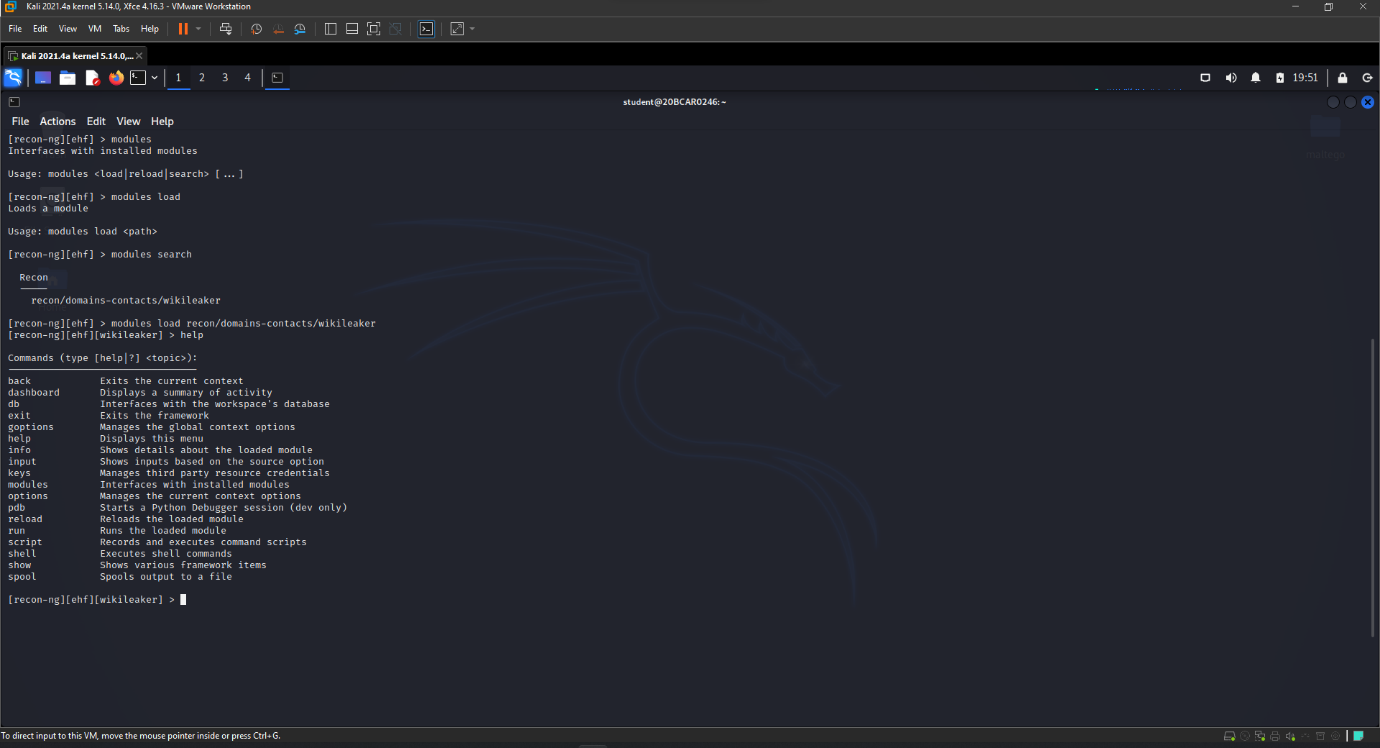


1. Type marketplace install <module path wanted to install> and hit enter, say, recon/domains-contacts/wikileaker.

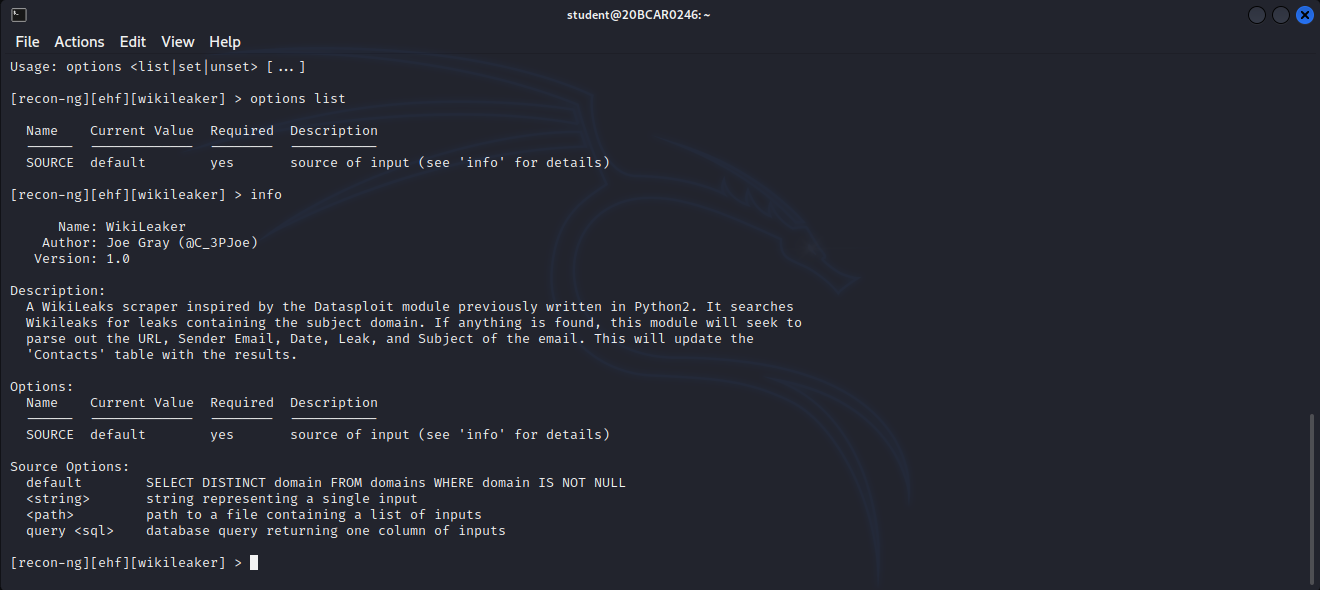


Using the Modules

1. While in reconn-ng newly created workspace, without activating any module, type modules search. A list of installed modules appears.
2. Type modules load <name of the module to work with> say, recon/domains-contacts/wikileaker. It should appear somewhat as follows:



1. To know about the module, info can be used as follows:



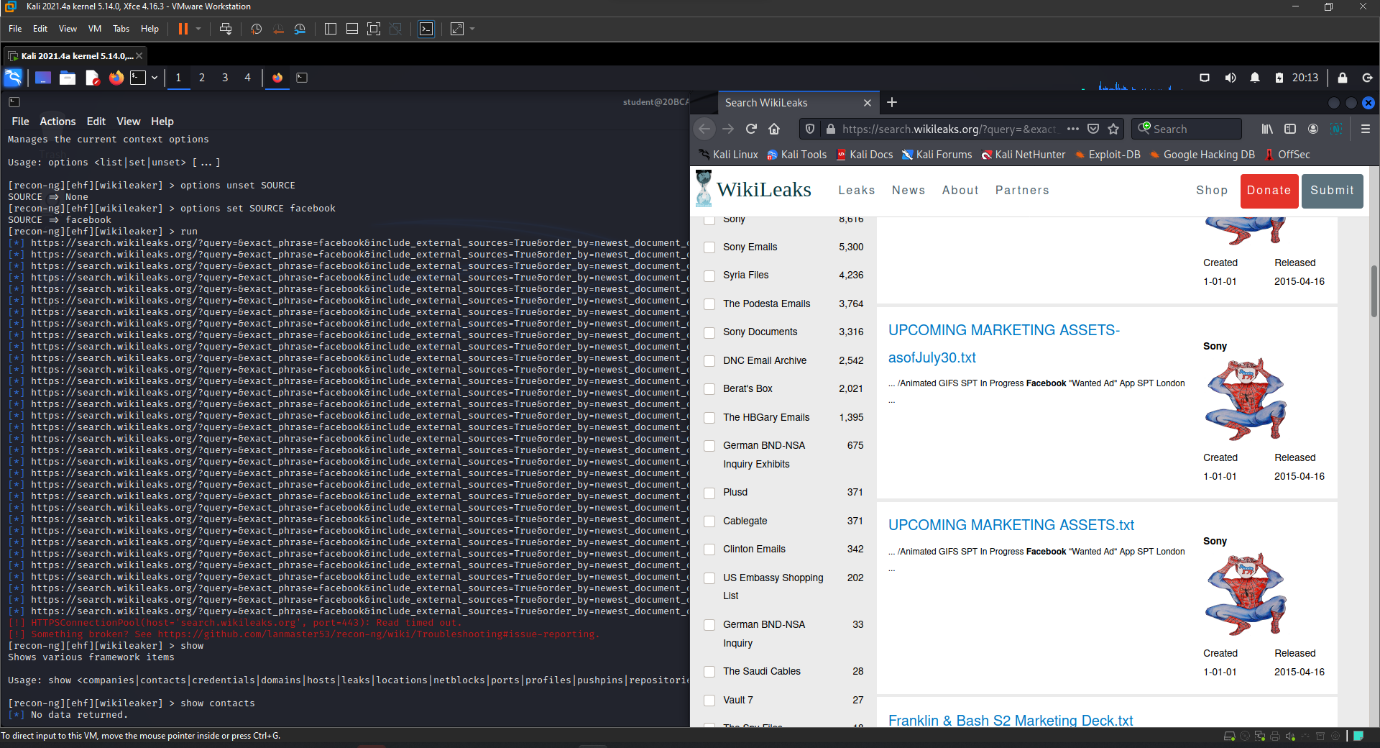
1. Using the input command check if the module has the required info which needs to be searched.
2. If not, set the input using options as did while setting the name server. Then run the command. The display goes as follows:

As we can see, wikileaks beinng a searh engine for classified documents, it shows the search output links to its website.

Summary of Events

To see a summary of what has been done with the tool till now, command dashboard helps us to obtain the same. The results are as follows:





As we can see, it shows all the info of info obtained as of now along with the modules installed in the tool.

**Conclusion :**

Recon-ng is a powerful tool that can be further explored by looking through the list of modules. The help within the console is very clear and with a bit of playing around it won’t take long to become an expert.

Once you start to become more familiar with the layout of the tool you will discover options such as workspaces that allow you to segment based on organization or network.

The rise of bug bounties allows you to play with new tools and explore organizations internet-facing footprint. Have fun and don’t break the rules.