

Department of

Bachelor of Computer Applications

**Ethical Hacking Fundamentals**

Lab File – CA 03b

**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

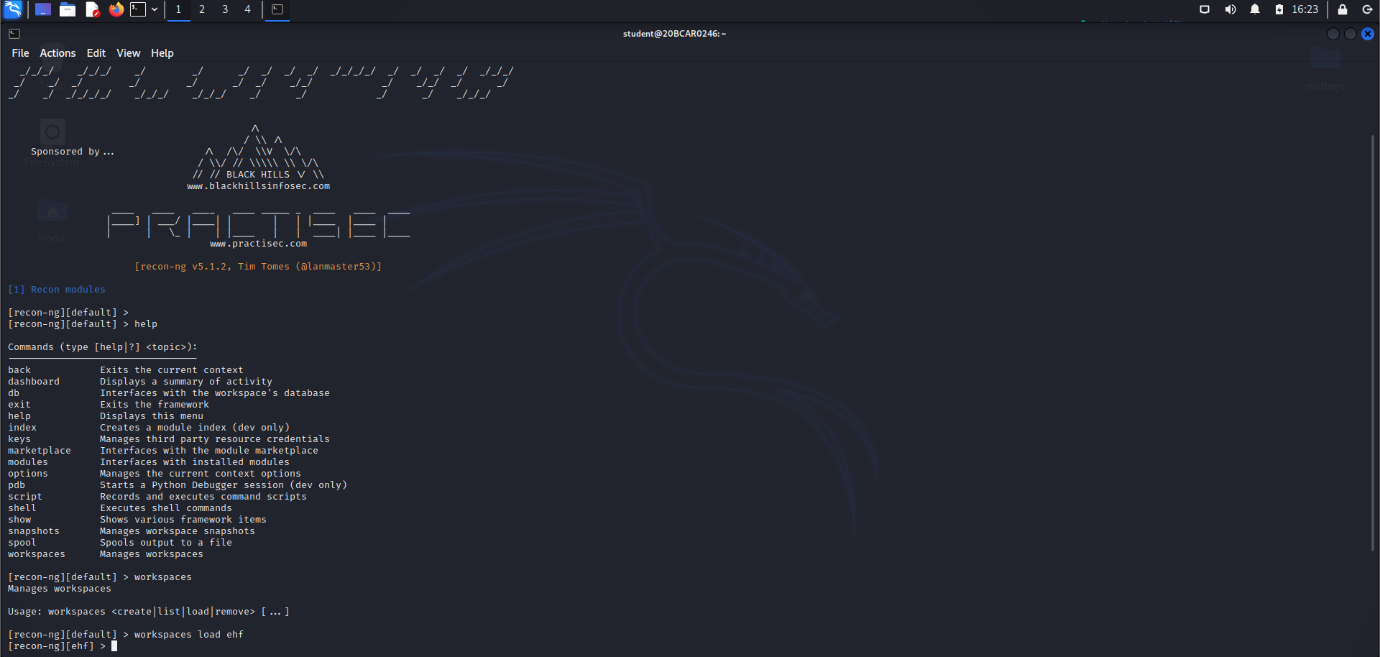
**Objectives :**

To Install & Run any module (with keys and dependencies) any obtain desired information using it. Also, generate report for the same.

**Procedure :**

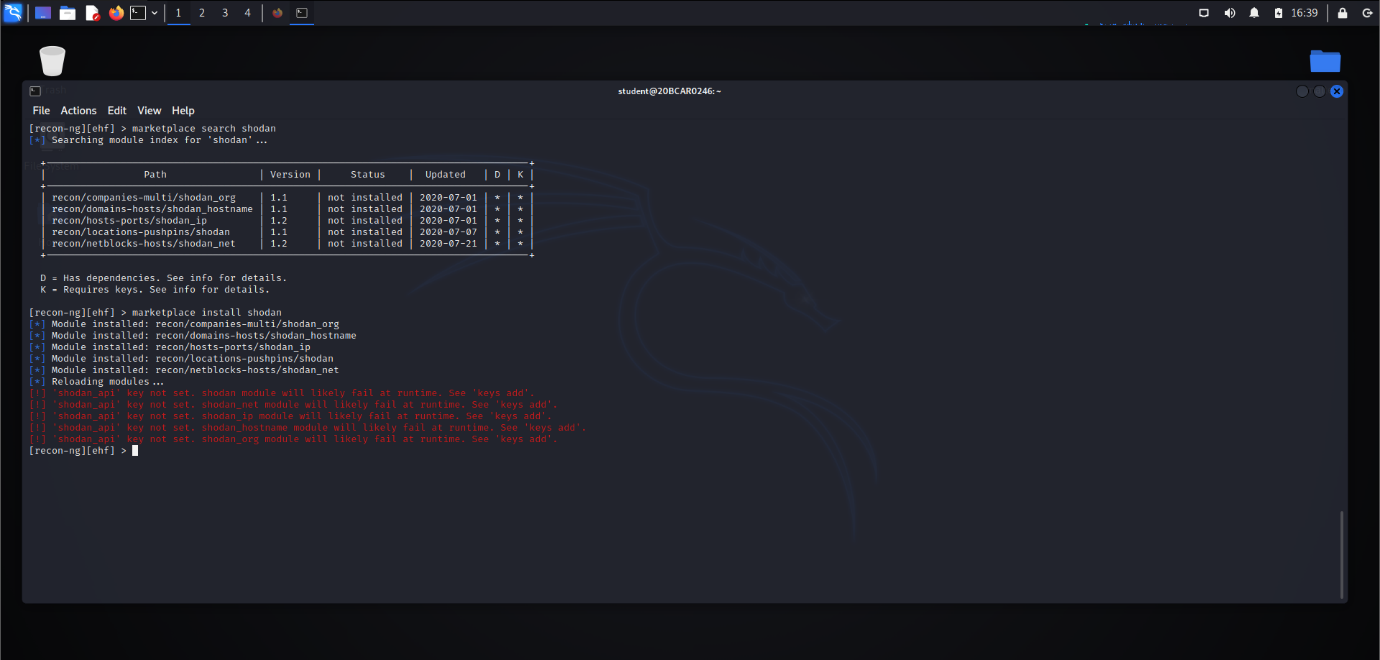
Running Module with Keys

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



As we can see, we are inside the workspace. For this lab, we are going to be using shodan modules.

Now, we will continue with installing required modules using workspaces install shodan.



To work with shodan, as mentioned in the screenshot, we will need keys and dependencies.

Therefore, we are now going to add keys to work with shodan. For that we are going to create a shodan account, after which we will use the api’s of that account, as follows.

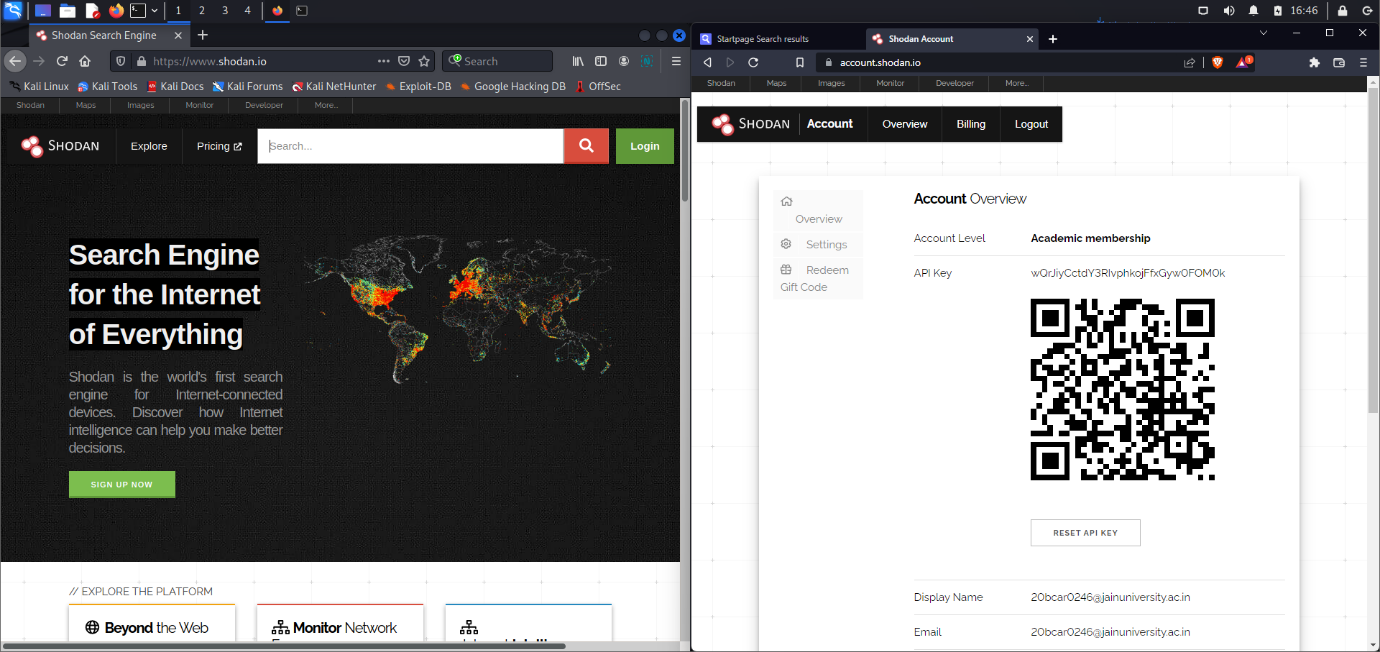


Figure: Obtained API keys

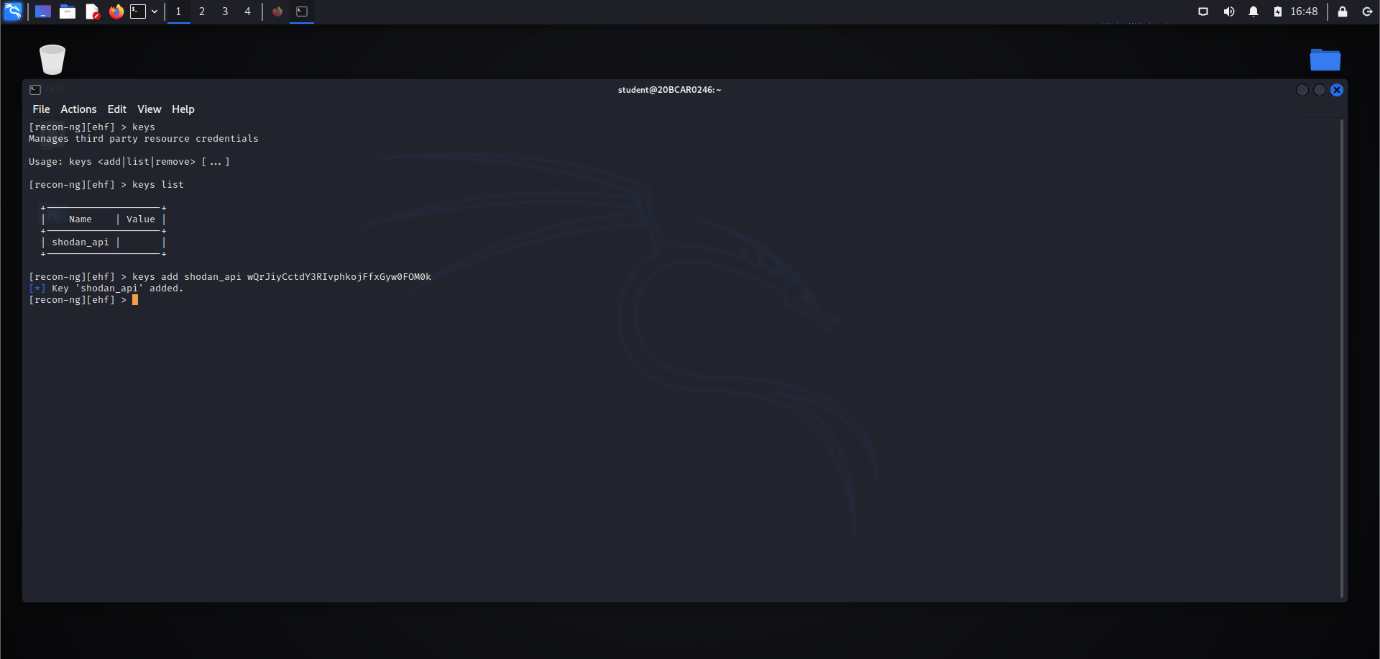
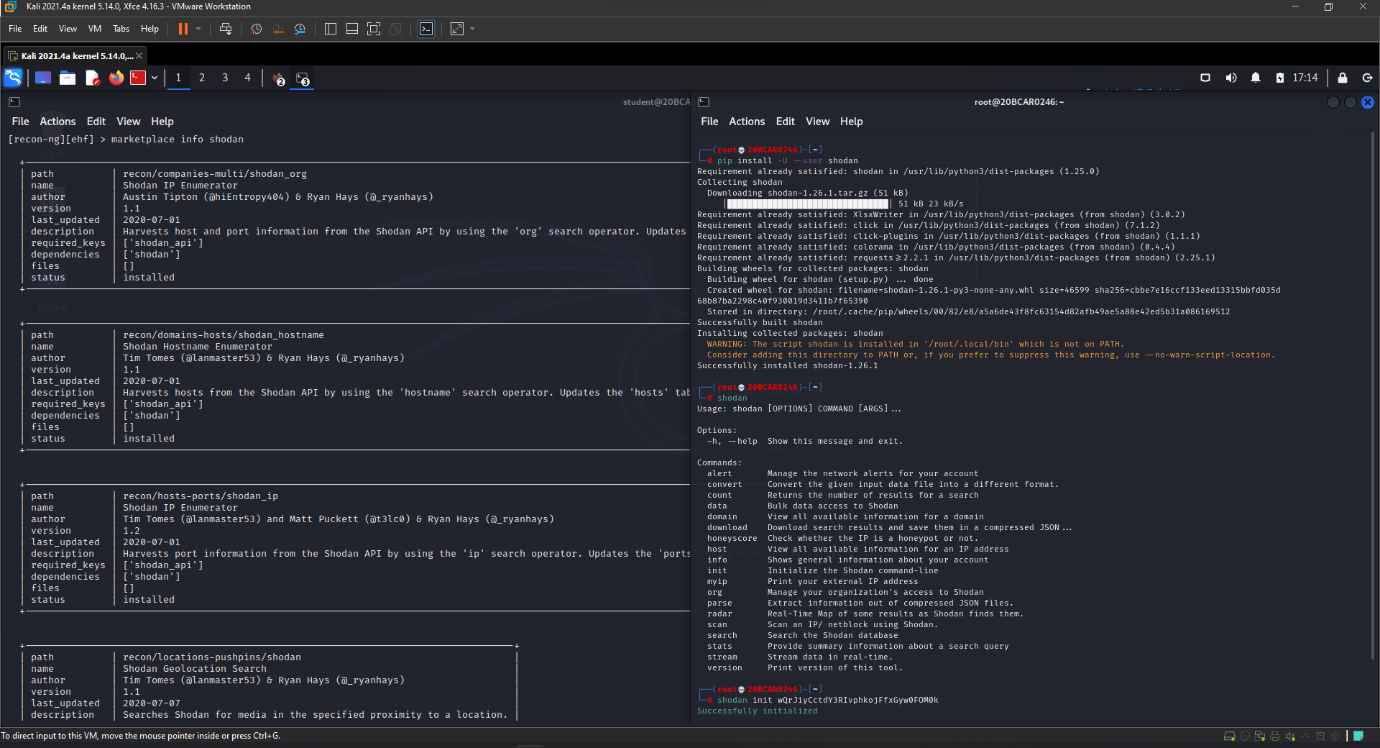


Figure: Setting API Keys

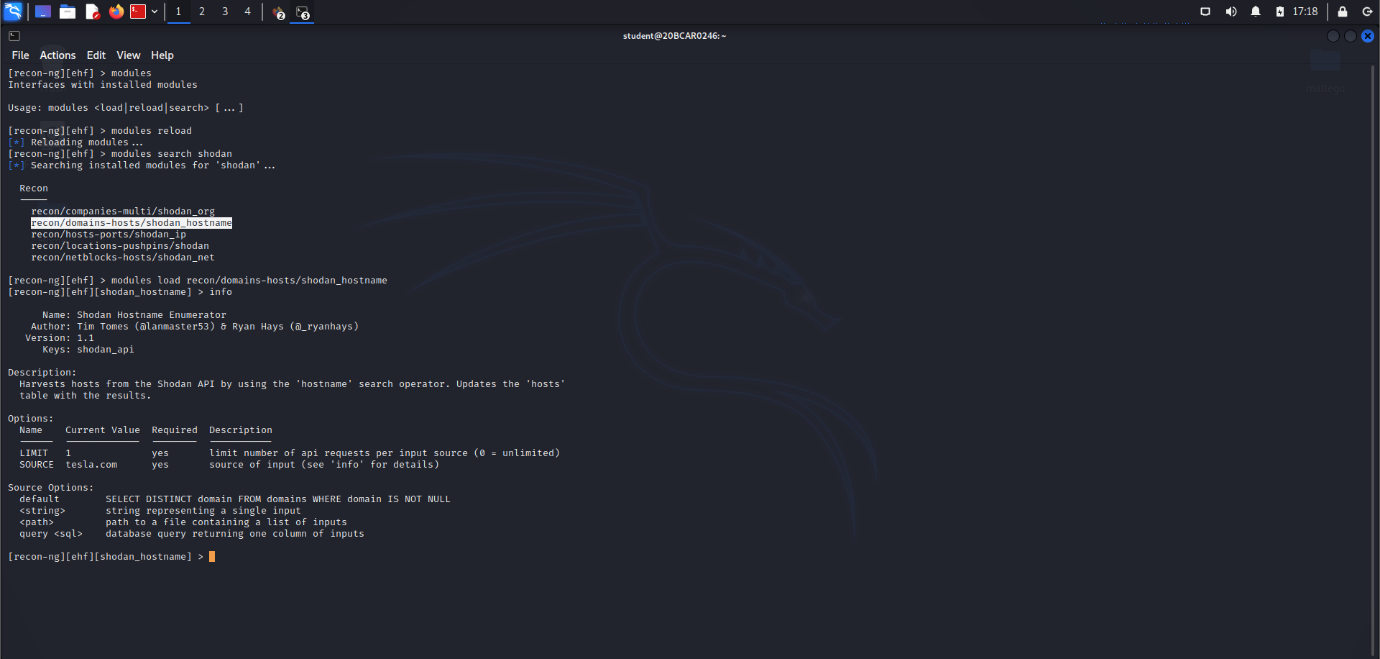
We, would also need to set dependencies before working on the module. For that we are going to follow the steps mentioned here: <https://help.shodan.io/command-line-interface/0-installation>



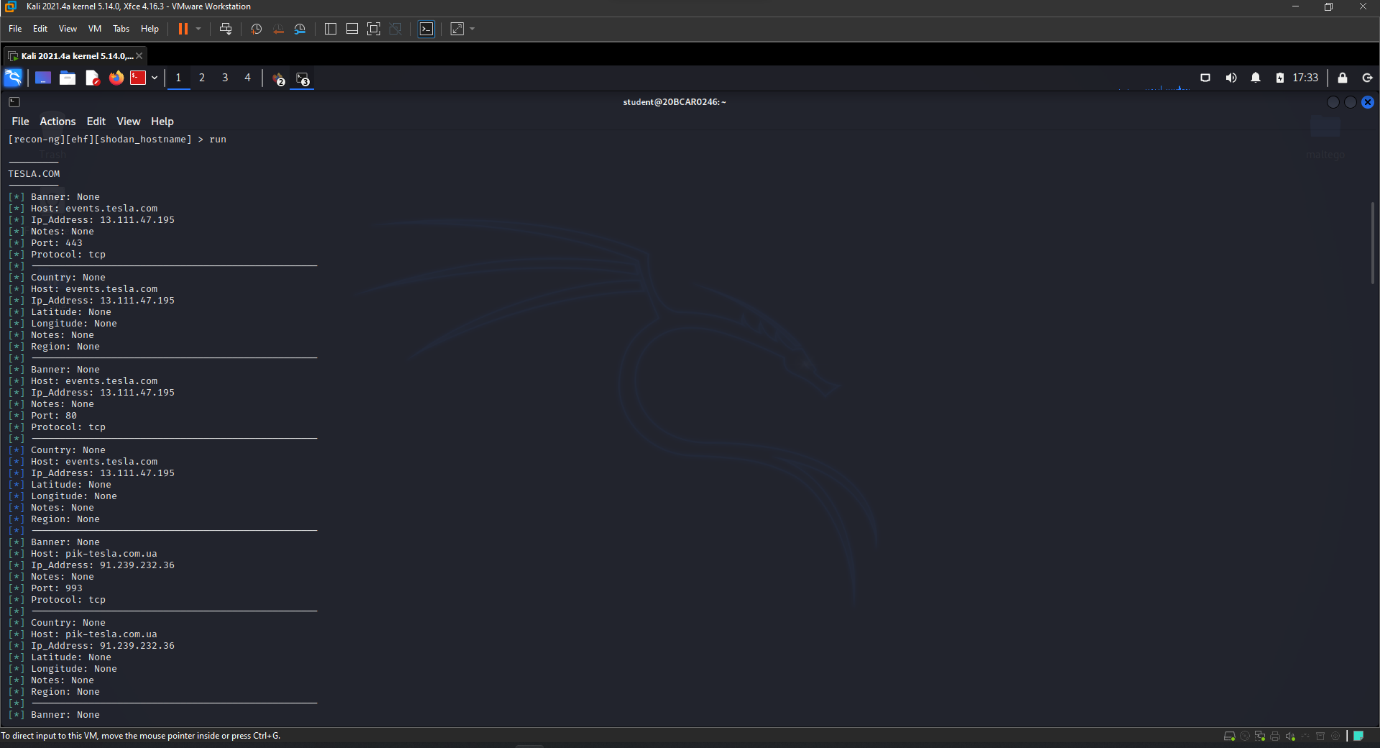
To

After being done with dependencies we will need to refresh the installed modules for once. Now, we being done with this, can continue with module configuration and running the same.

Well, there are a number of shodan modules present in the recon-ng. We need to select the desired, shodan hostname in this case. Using the options command, we have changed the target server.

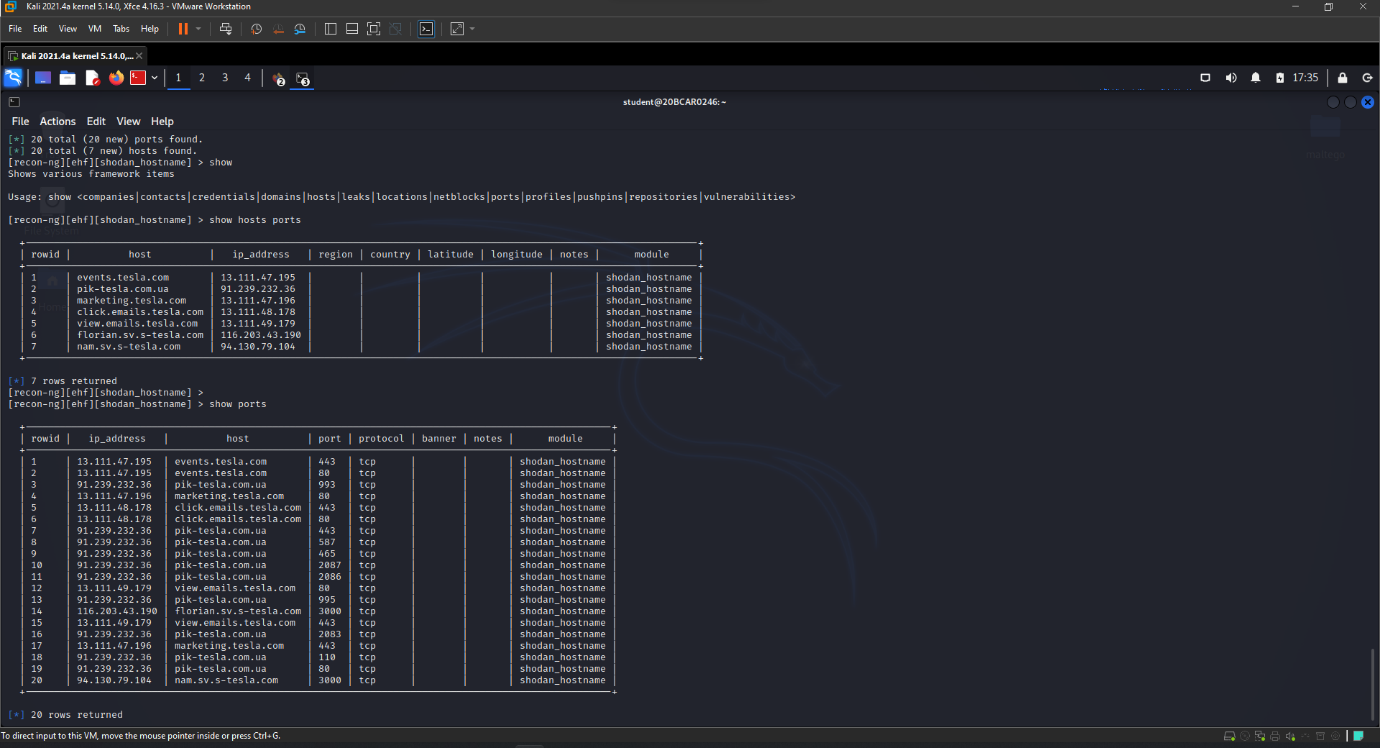


Now, we run the module. Following are the results obtained.



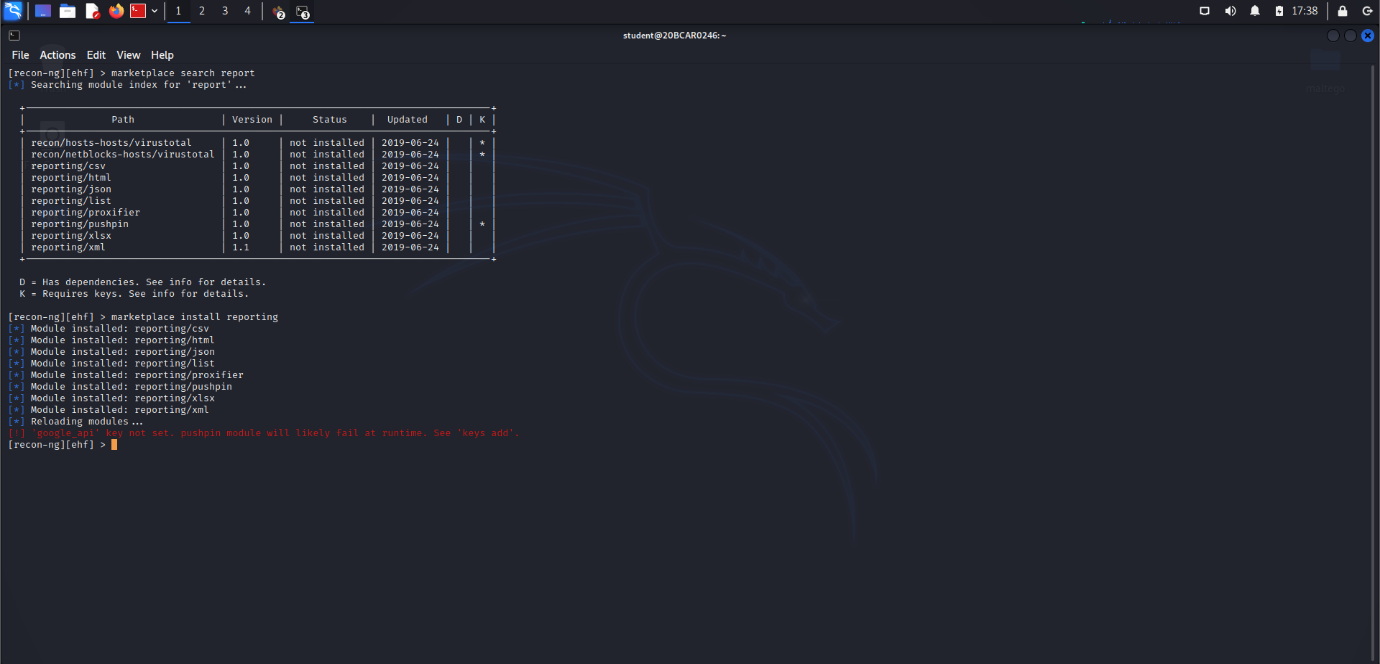
NOTE: We can run multiple modules together as mentioned here: <https://github.com/sharathunni/auto-recon-ng>

Using the show command we can from tables detailing the results we want to view.

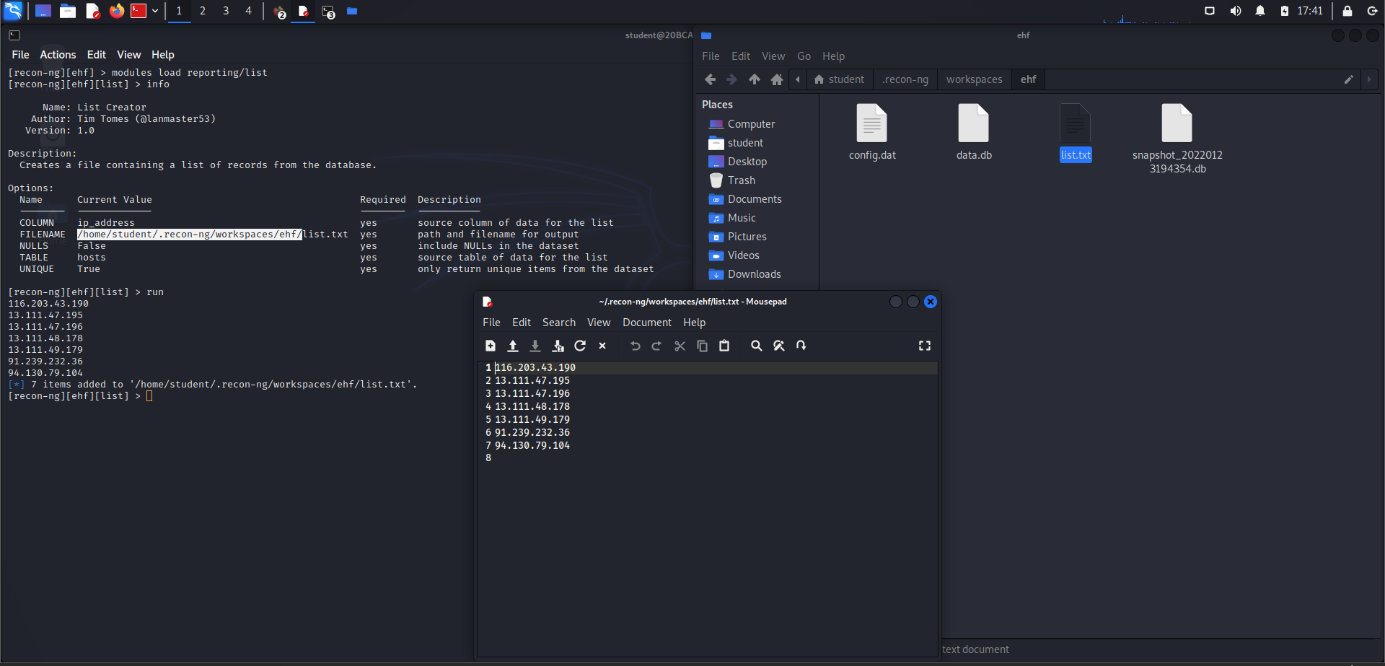


Generating Reports

To begin with, we will need to install the respective modules for reporting from the marketplace.



Using info we can see the path the report is going to be saved. Now, after running the module if we go to the location , we can see the file generated, in this case a .txt file, noting the ip’s, since using reporting/list module.



**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.