Lab 8 – Information Gathering using theHarvester

Lab Objective:

Gather information on a target site using theHarvester.

Lab Purpose:

Information gathering is often the first step of any penetration test. theHarvester is a very powerful OSINT (Open-Source Intelligence Tool) for finding information on a target URL. It searches multiple sites for information about the target URL and displays all the information it finds. It is particularly useful for finding names of people and their email addresses as well as subdomains of the target site.

Lab Tool:

Kali Linux

Lab Topology:

You can use either Kali Linux in a VM for this lab.

STEP 1:
We can use theHarvester which is bundled in Kali, but this tool is updated frequently. We will download and use the latest version, in this lab.

To begin, boot up Kali Linux in your VM and open a terminal. Follow the steps below:

```
sudo apt-get install python3-pip
 sudo pip3 install virtualenv
 virtualenv venv
```

STEP 2:

Clone the git repo:

```
git clone https://github.com/laramies/theHarvester.git
 cd theHarvester

pip3 install -r requirements.txt
```

Close this terminal and open a new one. Now, we are ready to use “theHarvester.py” in “kali” user’s home directory. Type:

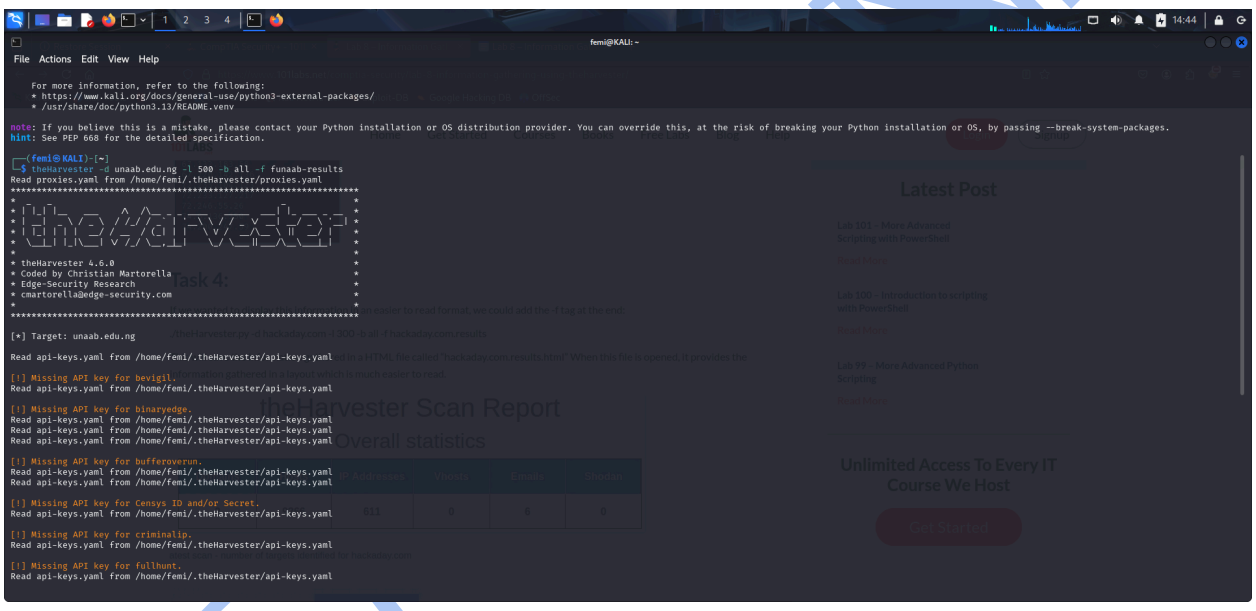
cd /home/kali/theHarvester/
./theHarvester.py -v

STEP 3:

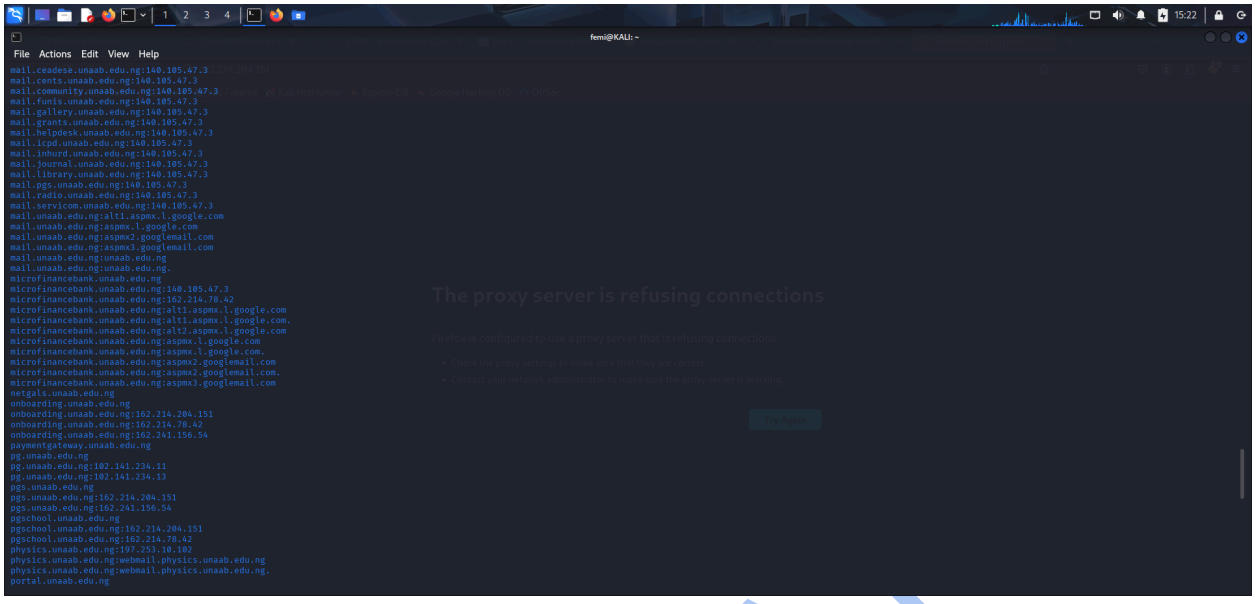
To launch an information gathering campaign on a target, type the following:

theHarvester.py -d unaab.edu.ng -l 500 -b all

This will start theHarvester. It will begin searching Google for the top 300 results related to hackaday.com.



END



If we wanted to display this information in an easier to read format, we could add the -f tag at the end:

./theHarvester.py -d unaab.edu.ng -l 300 -b all -f unaab.results

This will save the information gathered in a HTML file called “unaab.results.html” When this file is opened, it provides the information gathered in a layout which is much easier to read.