Information Gathering Using theHarvester

**Lab Objective:**

Learn how to 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.

**Lab Walkthrough:**

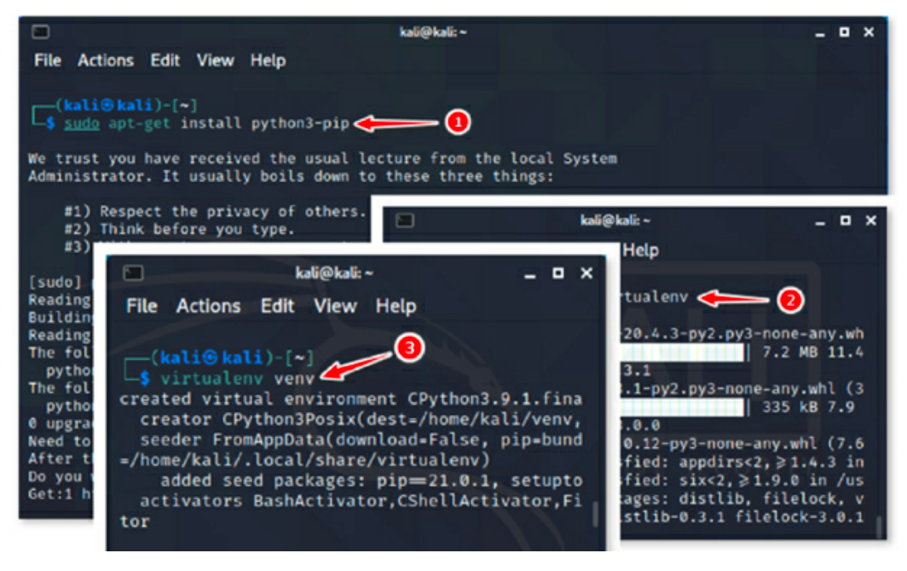
**Task 1:**

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



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.

Task 2:

Launch the Harvester

theHarvester -d Microsoft -l 500 -b google

This will start theHarvester. It will begin searching Google for the top 500 results related to Microsoft.

You can also use “-s” instead of one search engine. The “-s” tag will search shodan for information regarding your site.

As you can see, it is an extremely useful tool for discovering email addresses, names of people associated with the target, sub-domain names and IP addresses.

Task 3:

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

theHarvester -d Microsoft -l 500 -b google -f googleharvest.xml

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

