INFORMATION GATHERING USING THEHARVESTER.

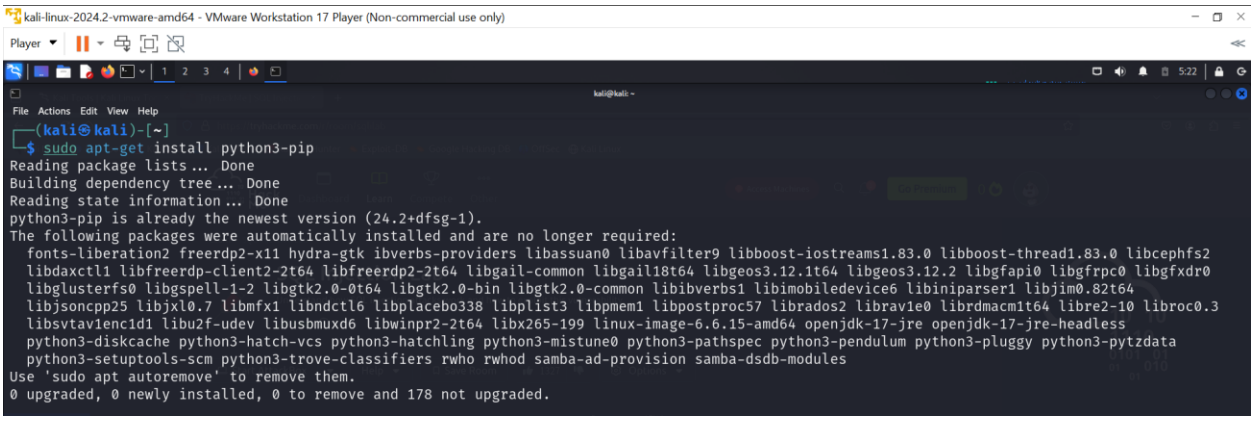
TOOL: THEHARVESTER

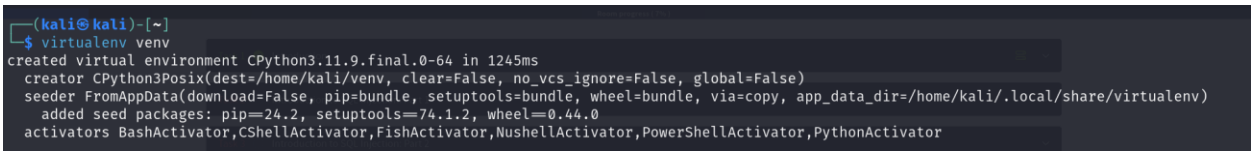
theHarvester is an open-source tool used for gathering information (reconnaissance) about a target during the early stages of penetration testing or ethical hacking. It helps security professionals collect publicly available data about domains, email addresses, employee names, IP addresses, subdomains, and other details that can be useful in mapping a target's attack surface.

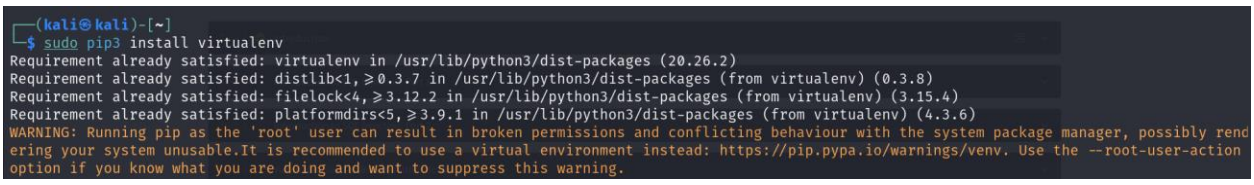
The tool works by querying various public search engines, such as Google, Bing, and specialized databases like LinkedIn or Shodan

Task 1

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

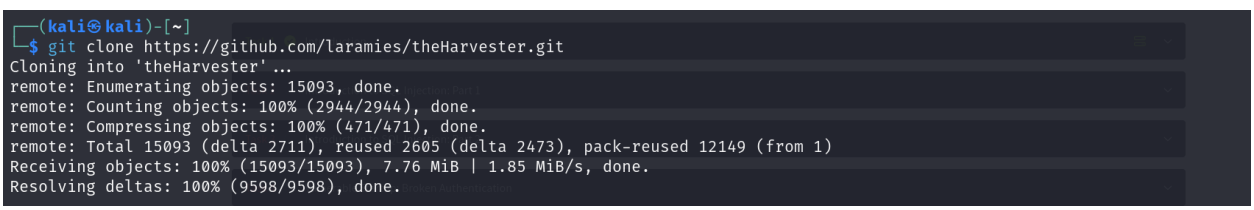






Clone the git repo:

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



cd theHarvester pip3 install -r requirements.txt

./theHarvester.py -v

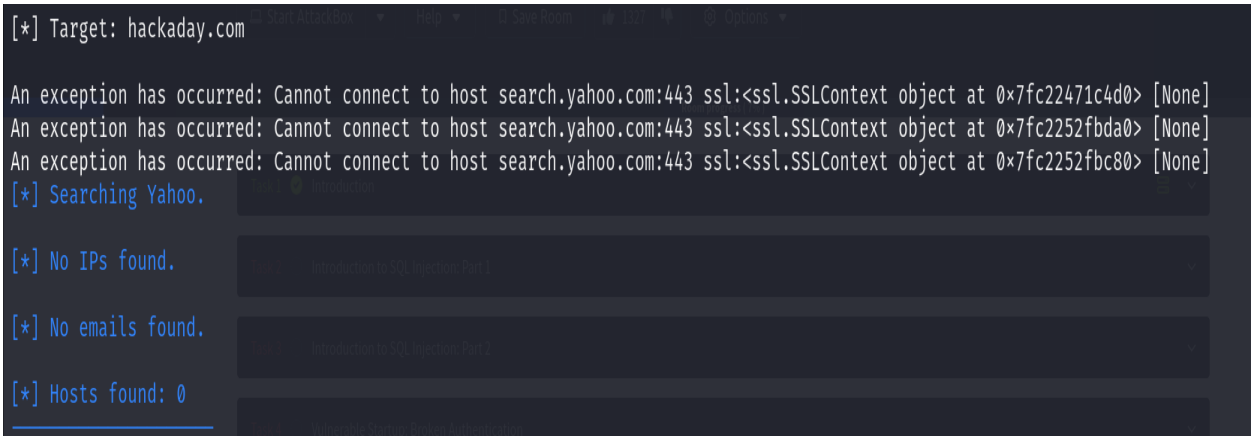
Task 2

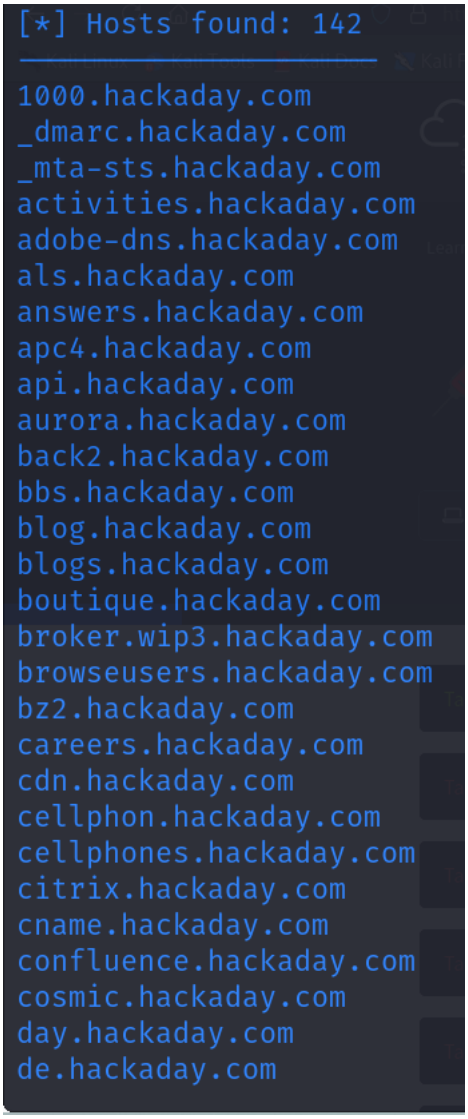
To launch an information gathering campaign on a target, type the following:

./theHarvester.py -d hackaday.com -l 300 -b yahoo

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

For this target, we could not find any information on Google. Let us dig deeper.

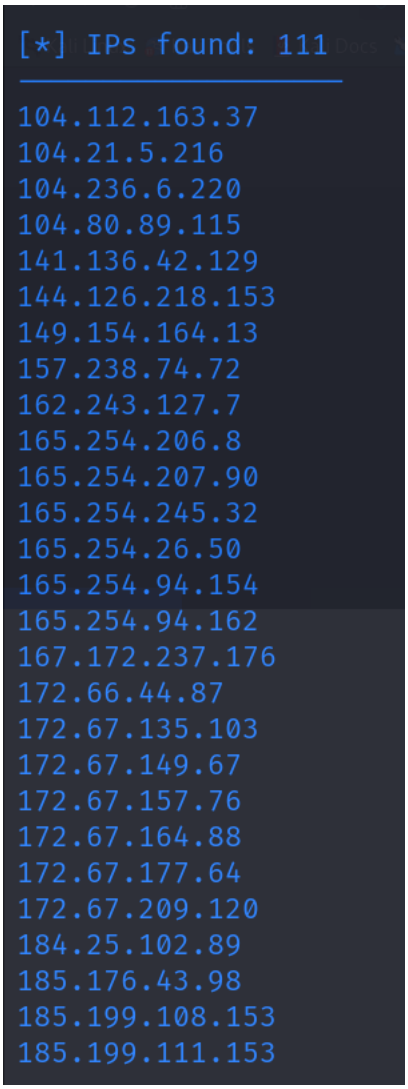




Task 3

If we want to gather even more information about our target, we can specify the following:

./theHarvester.py -d hackaday.com -l 300 -b all


[*] IPs found: 111
104.112.163.37
104.21.5.216
104.236.6.220
104.80.89.115
141.136.42.129
144.126.218.153
149.154.164.13
157.238.74.72
162.243.127.7
165.254.206.8
165.254.207.90
165.254.245.32
165.254.26.50
165.254.94.154
165.254.94.162
167.172.237.176
172.66.44.87
172.67.135.103
172.67.149.67
172.67.157.76
172.67.164.88
172.67.177.64
172.67.209.120
184.25.102.89
185.176.43.98
185.199.108.153
185.199.111.153

Task 4