

Module 2: Footprinting Lab 2: theHarvester

Description: In this lab, we are going to use a tool called theHarvester. This tool is useful for gathering information on subdomains, employee names, emails, open ports, and banners. It gathers the information from public sources, like regular search engines and Shodan. You can read more about it here: <https://tools.kali.org/information-gathering/theharvester>

Requirements for the lab: Kali Linux

Step 1: Launch your Kali machine and login (Username is normally: root and the password is normally: toor)

Step 2: Open a Terminal window

Step 3: At the prompt, type theharvester -h to view the help file for the tool.

Step 4: We are just going to use one of the example statements from the help section. Please type this command: **theharvester -d microsoft.com -l 50 -b google -h myresults.html**

-d is the domain or company name to search. In this case, we are searching microsoft.com

-l is used to limit the results. In this case, we are limiting to just 50 results.

-b is used to define our data source. In this case, we are just using google.

-h allows us to use the Shodan database to query any discovered hosts.

Question 1: Were you able to see any ip addresses in the output? If yes, write at least two of them here _____

Question 2: What other information did you find? _____

