**Lab 8- Information Gathering using the Harvester**

**Objective:**Learn how to gather information on a target site using **theHarvester**, an open-source intelligence (OSINT) tool for discovering publicly available information.

### **Lab Purpose:**

Information gathering is a crucial phase in penetration testing. **theHarvester** is designed to automate the collection of data such as email addresses, subdomains, and other information associated with a given target. It searches through multiple public sources, making it an essential tool for reconnaissance.

### **Tools Needed:**

* **Kali Linux** (running in a VM)

### **Lab Walkthrough**

#### **Task 1: Installing the Latest Version of theHarvester**

**Update Kali Linux** (if necessary) and install dependencies:  
bash  
Copy code  
sudo apt-get install python3-pip

sudo pip3 install virtualenv

virtualenv venv

1. **Clone the theHarvester repository** from GitHub:  
   git clone https://github.com/laramies/theHarvester.git

cd theHarvester

1. **Install required packages** using pip:  
     
   pip3 install -r requirements.txt
2. **Navigate to theHarvester directory** and verify the installation:  
   cd /home/kali/theHarvester/
3. ./theHarvester.py -v

#### **Task 2: Basic Information Gathering**

To begin gathering information on a target, you can specify the domain and source. For example, to gather results from Google, use the following command:

1. ./theHarvester.py -d hackaday.com -l 300 -b google
   * **-d**: Specifies the domain (e.g., hackaday.com).
   * **-l**: Limits the number of results to 300.
   * **-b**: Sets the source search engine, in this case, Google.
2. TheHarvester will search Google for the top 300 results related to hackaday.com. If no information is found, you can attempt a broader search.

#### **Task 3: Expanding the Search**

To search across multiple sources for information on hackaday.com, use the following command:

1. ./theHarvester.py -d hackaday.com -l 300 -b all
   * **-b all**: Instructs theHarvester to search across all available search engines.
2. This will broaden the search, collecting email addresses, names, subdomains, and IP addresses related to the target domain.

#### 

#### **Task 4: Saving Results in a Readable Format**

To make the results easier to review, you can save them in an HTML file:

1. ./theHarvester.py -d hackaday.com -l 300 -b all -f hackaday.com.results
   * **-f**: Specifies the output file format (e.g., hackaday.com.results.html).
2. After running this command, theHarvester will generate an HTML file with the gathered information. Open this file in a web browser to see a neatly formatted report of the discovered data.

### **Takeaways:**

* **OSINT Tools:**theHarvester is a powerful OSINT tool that can help penetration testers gather key information about their target.
* **Data Types Collected:**
  + Email addresses
  + Subdomains
  + Names of associated individuals
  + IP addresses
* **Use Cases:**
  + Reconnaissance for penetration testing.
  + Collecting data for social engineering attacks.
* **Best Practices:**
  + Always ensure permission when performing any type of reconnaissance on a target.
  + Use this tool ethically to gather publicly available information.

By following these steps, you will have successfully used theHarvester to gather valuable intelligence on a target site, aiding in your penetration testing or OSINT efforts.