**# Custom Reconnaissance Tool**

A modular and lightweight Python-based reconnaissance tool for automating the initial phase of information gathering during penetration testing.

This tool allows users to perform:

- WHOIS lookups

- DNS enumeration

- Subdomain discovery

- Port scanning

- Banner grabbing

- Technology detection

All from a simple command-line interface.

**## Objective**

To help penetration testers and red team members gather critical public information about a target domain using passive and active reconnaissance techniques.

**## Tool Structure and Approach**

To keep the tool clean and modular:

- A folder named `ReconTool` was created.

- Inside it, another folder named `modules` was added to store all the feature files (`whois\_lookup.py`, `dns\_enum.py`, etc.).

- A separate file `main.py` was placed outside the modules folder, but still inside 'ReconTool'.

- All the module files were imported into `main.py` using standard Python import statements.

- Each feature can be called independently using command-line flags like `--whois`, `--dns`, etc.

- Final results are saved in a separate `reports` folder with timestamps.

This approach makes the tool simple to expand, debug, and use.

**## How to Run the Tool (Step-by-Step)**

To run this tool successfully on your local machine using Visual Studio Code (VS Code), follow the steps below in proper sequence:

**### Step 1: Check if Python is Installed**

First, ensure that Python is installed on your system. Open the terminal in VS Code and type:

**python --version**

If python installed then well if not then first install it.

This tool uses some external libraries which must be installed before running. Use the following command in the terminal:

**pip install whois dnspython requests**

Now to Run the code ->

**python main.py github.com --whois --dns --subdomains --portscan --banner --tech**

This will execute the whole tool and result will save in reports so you can get the txt file and see the results of whole tool but if

you want to see seperate results of all then you will run this command ->

**python main.py github.com --whois**

**## Folder Structure**

Create a folder for your tool (e.g., recon\_tool). Inside it:

Make a folder named modules.

Put all your module files (e.g., whois\_lookup.py, dns\_enum.py, etc.) inside the modules folder.

Create a main.py file outside the modules/ folder then run it and got the result txt file.