MyMap is a Python-based wrapper for Nmap that simplifies working with NSE (Nmap Scripting Engine) scripts. It features an interactive **menu-driven system** for searching, selecting, and executing scripts while providing progress tracking, report generation, and the ability to save custom commands for quick reuse.

MyMap is especially useful for users who find it challenging to remember or locate the extensive library of NSE scripts, providing a streamlined interface for automation and script management. Nmap was originally created by Fyodor.

Acknowledgments

- **Original Code**: Kev Milne
- **Improvements and Contributions**:
    - Hubert Januszewski
    - Sophie Hall

Feel free to add or change it as you wish, just remember to give the above some credit for its origins. 😊

Menu System

MyMap provides a hierarchical menu system designed to make navigation intuitive and efficient.

Structure

1. **Main Menu**:
    - Displays script categories, along with options for search, speed dial, configuration, help, and custom commands.
2. **Submenus**:
    - Category submenus display all scripts in the selected category.
    - Search results and Speed Dial commands are presented in a similar list format.
3. **Interactive Prompts**:
    - Users are guided through selecting targets, ports, and other parameters step by step.
    - Each choice is validated with clear feedback to ensure correct input.

Key Features

- **Search Functionality**:
    - Search by keywords (e.g., auth, ftp) to quickly find relevant scripts.
    - Review script descriptions before execution.
- **Script Categories**:
    - Organized NSE scripts into categories for ease of navigation.
    - Allows running scripts directly after selecting them from a category.
- **Speed Dial**:
    - Save frequently used commands for quick access.
    - Manage saved commands (add/edit/delete) through a dedicated menu.
- **Custom Commands**:
    - Enter and execute custom Nmap commands.
    - Automatically include additional options like output and progress tracking.
- **Configuration**:
    - Modify runtime settings, such as whether to prompt for file output or auto-generate reports.
- **Help Menu**:
    - Access instructions and information directly within the program.

MyMap will also look for certain keywords in the output and highlight them. If you choose to create a (basic) penetration test results paragraph, these will be added at that time. It will state what vulnerabilities have been found based on the keywords and provide them in a paragraph for you.

Example Workflow

1. Starting the Program

Run the script:

Python3 mymap.py

2. Navigating the Main Menu

The program will present the main menu:

```
==============================
    WELCOME TO... MYMAP!
  A wrapper for nmap by Kev
(modified, with improvements)
==============================
SCRIPT CATEGORIES

1. Auth
2. Brute
3. Discovery
4. Exploit
5. External
6. Malware
7. Safe
8. Version
9. Vulnerability
10. Default

OR ENTER:

- number of script category
- 's' search
- 'c' custom
- 'd' speed dial
- 'e' edit settings
- 'h' help
- 'q' quit
->
```

3. Selecting a Script Category

Choose a category (e.g., **2. Brute**) to see its scripts:

```
BRUTE SCRIPTS

1. ftp-brute
2. http-brute
3. ssh-brute
4. telnet-brute
5. smtp-brute
...

Choose a script by number or '0' to go back:
```

4. Running a Script

1. Select a script (e.g., **1. ftp-brute**).
2. The program will guide you to:
    - Enter the **target** (e.g., 192.168.1.1).
    - Specify the **port** (e.g., 21).
    - Choose whether to output results to a file (optional).
3. MyMap runs the script with a progress bar:
4. Progress: 10.00% done
5. Progress: 30.00% done
6. Progress: 50.00% done
7. ...
8. After execution, MyMap displays the output and asks if you'd like to:
    - View the output.
    - Generate a report.
    - Save the script to Speed Dial for future use.

Detailed Example: Using the Search Function

Step 1: Initiate Search

From the main menu, select **Search (s)**:

Enter a search term (max 8 chars):

-> auth

Step 2: View Results

The program displays scripts matching the term:

Search Results

1. ftp-auth

2. http-auth

3. smb-auth

4. snmp-auth

...

Choose script by number, 's' to search again, '0' to menu:

->

Step 3: Run Selected Script

1. Choose a script (e.g., **2. http-auth**).
2. Enter the target and port:
3. Enter target (e.g., 192.168.1.1 or path to target file):
4. -> 192.168.1.100
5. Enter port (e.g., 80):
6. -> 80
7. Optional: Choose to output results to a file or view them on the screen.
8. Review output and decide if a report is needed.

Example: Speed Dial Workflow

1. From the main menu, select **Speed Dial (d)**.
2. If no saved commands exist:
3. No speed dial options.
4. ENTER:
5. - 'a' to add a new speed dial
6. - '0' to go back
7. -> a
8. Add a command:
9. Enter flags/options (no target):
10. -> -p 80 -sV --script=http-title
11. Enter a title:
12. -> HTTP Title Scan
13. Speed dial saved.
14. Use Speed Dial:
15. SPEED DIAL MENU: Quick access to saved commands.
16. 1. HTTP Title Scan: -p 80 -sV --script=http-title
17. Enter number of speed dial, 'a' add, 'e' erase, '0' back:
18. -> 1
19. Enter target (e.g., 192.168.1.1 or path to target file):
20. -> 192.168.1.100
21. MyMap runs the saved command and displays progress/output.

Potential Use Case

A network administrator tasked with scanning a large network for vulnerabilities can use MyMap to:

1. Search for relevant scripts (e.g., vuln).
2. Quickly execute scans and track progress.
3. Save complex scans to Speed Dial for later use.
4. Automatically generate a report for each scan.

By consolidating these tasks into a menu-driven system, MyMap significantly reduces the time and effort required for managing NSE scripts.

Menu Navigation Summary

- **Script Categories**: Browse scripts by type.
- **Search**: Locate specific scripts using keywords.
- **Custom Commands**: Execute custom Nmap commands with progress tracking.
- **Speed Dial**: Save and reuse frequently used commands.
- **Edit Settings**: Configure program behavior for output, reports, and prompts.
- **Help**: Access usage instructions.
- **Quit**: Exit the program.

This structured approach ensures both novice and experienced users can efficiently leverage MyMap for Nmap-based security assessments. Note, I have added a few options already to the speed dial file (config.json). There is also a separate help.txt file which MyMap reads and you can update the config through option 'e' on the menu.

Finally, the custom search facility will allow you to search for keywords such as 'SMTP' which will bring back NSE scripts that may be useful as shown below.

```
-> s

Enter a search term (max 8 chars):
-> smtp

Search Results:
1.                    smtp-brute          7.              smtp-enum-users
2.        smtp-vuln-cve2011-1764          8.               smtp-ntlm-info
3.        smtp-vuln-cve2010-4344          9.              smtp-open-relay
4.        smtp-vuln-cve2011-1720         10.            smtp-strangeport
5.                    smtp-brute         11.      smtp-vuln-cve2010-4344
6.                smtp-commands          12.      smtp-vuln-cve2011-1720
                                          13.       smtp-vuln-cve2011-1764
```

Figure 1- Using the Search Facility to find scripts.