Programming-CYS

Documentation:

The purpose of this documentation is to provide a clear understanding of the flow and steps involved in the given task. According to the task, we are required to write a program to perform a brute force attack on a specific URL. The implementation is divided into four separate files:

1. **brute_force.py**
2. **scrape_data.py**
3. **extract_ips.py**
4. **confirm_dns.py**

Each file handles a specific part of the task, and the code is well-documented for better comprehension. Upon completion, the program generates the following output files:

1. **logs.txt**
2. **ips.txt**
3. **confirmed_dns.txt**

Key Notes:

- In **brute_force.py**, 10,000 combinations are defined for the brute force attack.
- The program may take some time to complete the attack depending on the computational resources.

Order of Execution:

The following steps outline the correct order to execute the files and describe their respective purposes:

1. **Run brute_force.py:**
   a. Performs the brute force attack to find the password.
   b. Once the password is identified, note it down for subsequent steps.

   Command : python brute_force.py

Run scrape_data.py:

- Logs into the website using the identified password.
- Scrapes data from the website.
- Generates the output file logs.txt.

Command: python scrape_data.py

Run extract_ips.py:

- Reads the logs.txt file and extracts IP addresses.
- Generates the output file ips.txt.

Command: python extract_ips.py

Run confirm_dns.py:

- Reads the ips.txt file.
- Checks port 53, performs reverse DNS lookups, and validates DNS servers.
- Generates the output file confirmed_dns.txt.

Command: python confirm_dns.py