Question-3

Part-a and part-b

This report details the methodology used to fetch all subdomains of a given domain using crt.sh and dnsdumpster, followed by resolving their corresponding IP addresses. The process has been automated using a Python script that employs asynchronous programming for efficiency. The automation is implemented through the following key components:

1. Fetching Subdomains: The script queries crt.sh and dnsdumpster to collect subdomains.
2. Resolving IP Addresses: It resolves the IP addresses of the collected subdomains.
3. Saving Results: The results are stored in a CSV file for further analysis.

Flow of Code

1. The script starts by taking user input for the domain name.
2. It initializes API details for dnsdumpster and the URL for crt.sh.
3. Asynchronous HTTP requests are made to both services to fetch subdomains.
4. The collected subdomains are stored in a list.
5. Each subdomain is resolved to its IP address using socket.gethostbyname().
6. The results are stored in a dictionary with subdomains and their respective IPs.
7. The data is then written to a CSV file named results.csv.
8. The entire process runs asynchronously for efficiency.
9. Finally, the script prints a confirmation message that the results have been saved.