Q3

Report on Subdomain Enumeration and Private IP Filtering Script

1. Overview This script performs subdomain enumeration and filters private IPs using data from two sources: `crt.sh` and `dnsdumpster`. It resolves IP addresses of subdomains and identifies private IPs for further analysis. Additionally, it utilizes the `dnsdumpster` API to fetch domain-related information.

2. Functionality

- **`is_private_ip(ip)`**: Checks if an IP address is private using the `ipaddress` module.
- **`load_subdomains(json_file)`**: Loads subdomains from a JSON file containing `crt.sh` data.
- **`get_private_ips(subdomains)`**: Resolves subdomains to IP addresses and filters private ones.
- **`cert_sh()`**: Main function to process `crt.sh` JSON file and identify private IPs.
- **`dnsdumpster()`**: Queries the `dnsdumpster` API for subdomain information and saves it in a JSON file.
- **`load_dnsdumpster_subdomains(json_file)`**: Parses the `dnsdumpster` JSON response to extract subdomains and associated IPs.
- **Main Execution**: The script first runs `cert_sh()`, then checks for an existing `dnsdumpster.json` file before making a fresh API request. Finally, it loads and prints subdomain-IP mappings.

3. Dependencies

- `json`: For handling JSON files.
- `socket`: For resolving domain names to IPs.
- `ipaddress`: To determine private IPs.
- `requests`: To interact with the `dnsdumpster` API.
- `os`: For checking file existence.

4. API Usage The script makes an HTTP GET request to `https://api.dnsdumpster.com/domain/iiitd.edu.in` with an API key in the headers. It then saves the JSON response to a local file for further processing.

5. Error Handling

- Handles invalid IP addresses in `is_private_ip()`.
- Catches DNS resolution failures in `get_private_ips()`.
- Prints an error message for failed API responses in `dnsdumpster()`.

6. Conclusion This script is effective in enumerating subdomains and identifying private IPs from `crt.sh` and `dnsdumpster`. With some enhancements, it can be further optimized for performance and security.