Security Assessment Tool Overview

Table of Contents

The **Security Assessment Tool** is written in **Python** and automates several tasks related to the security assessment of domains and IP addresses. The tool performs **WHOIS lookups**, **DNS queries**, **subdomain discovery**, **Nmap scans**, and **vulnerability assessments**, ultimately generating a detailed **HTML report** for further review.

1. Programming Language and Libraries Used

- **Language**: Python
- **Key Libraries**:
    - **os**: For directory and file management (creating folders, handling file paths).
    - **subprocess**: To run external commands like `whois`, `nmap`, and `sublist3r`.
    - **datetime**: For generating timestamps used in folders and report file names.
    - **html**: To sanitize the command output for safe display in HTML.
    - **re**: To extract IP addresses from raw text using regular expressions.

2. Functionality

The tool automates various processes, each of which uses external tools or scripts to gather security-related information about a domain or IP address:

- **WHOIS Lookup**: Retrieves registration and ownership information for a domain or IP address.
- **DNS Lookup**: Queries Google DNS (8.8.8.8) for DNS records.
- **Subdomain Discovery**: Uses the tool **Sublist3r** to find subdomains associated with a domain.
- **Nmap Scan**: Runs Nmap to scan the identified IPs for open ports and services.
- **Vulnerability Scan**: Uses Nmap's **vulners** script to search for known vulnerabilities associated with the services running on the open ports.

3. Example Workflow

Step 1: Information Gathering

- For domains, WHOIS and DNS lookups are performed.
- For IP addresses, a reverse DNS lookup is conducted.

Step 2: Scanning and Enumeration

- The tool uses Nmap to identify open ports and running services.
- IP addresses are extracted from WHOIS, DNS, and subdomain data to ensure complete coverage.

Step 3: Vulnerability Scanning

- The tool performs a vulnerability scan on the detected services using the **vulners** Nmap script to identify known CVEs (Common Vulnerabilities and Exposures).

Step 4: Report Generation

- After completing all scans, the tool generates a detailed HTML report, including all gathered data, such as subdomain information, Nmap scan results, and vulnerability findings.

4. How the Tool Works

Running a Domain Scan:

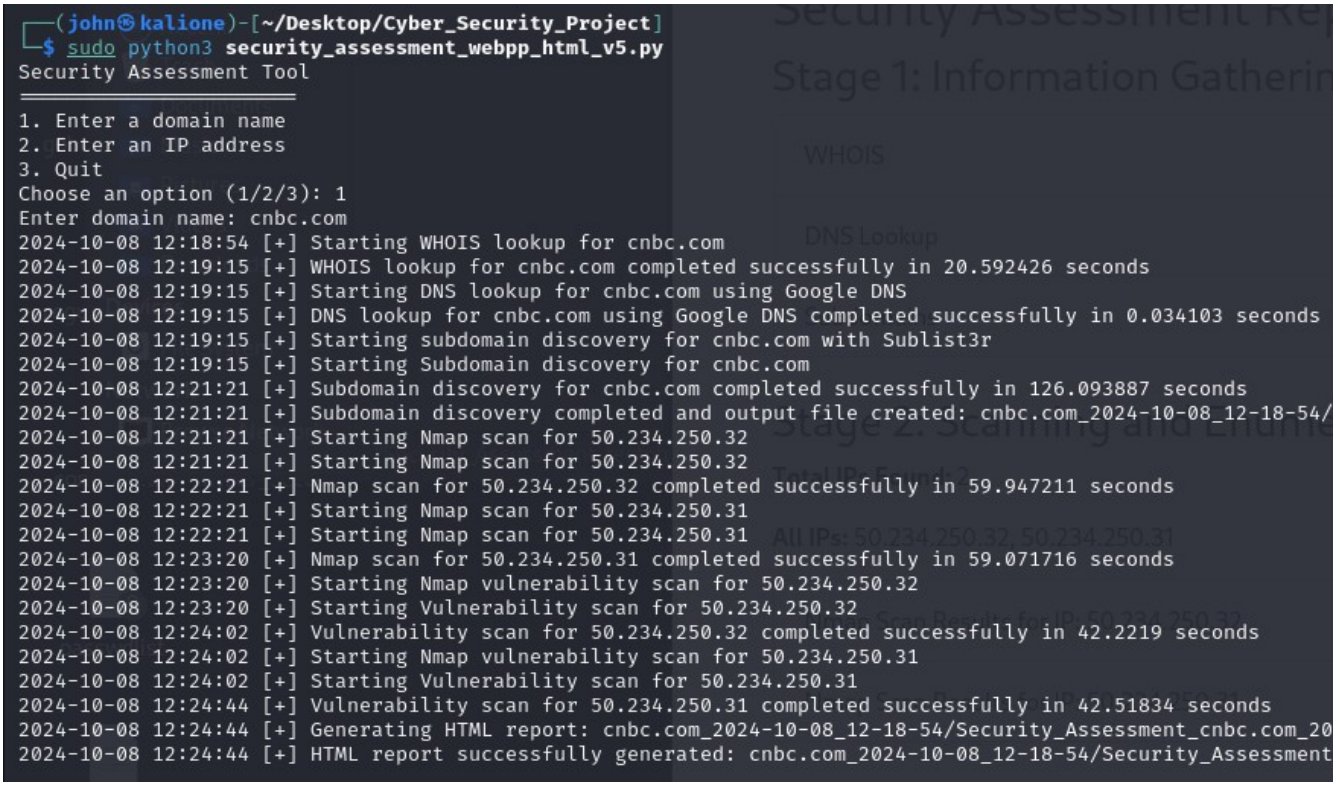
```
$ sudo python3 security_assessment_webpp_html_v5.py
```

- **Option 1**: Input a domain name (e.g., `cnbc.com`).
- The tool performs WHOIS lookup, DNS queries, and subdomain discovery, followed by Nmap scans on the identified IPs.
- An HTML report is generated, showing all findings, including IPs, services, and vulnerabilities.

Running an IP Scan:

```
$ sudo python3 security_assessment_webpp_html_v5.py
```

- **Option 2**: Input an IP address (e.g., `192.168.1.8`).
- The tool performs a reverse DNS lookup, WHOIS lookup, and runs Nmap scans followed by vulnerability scans.
- The results are compiled into a detailed HTML report.



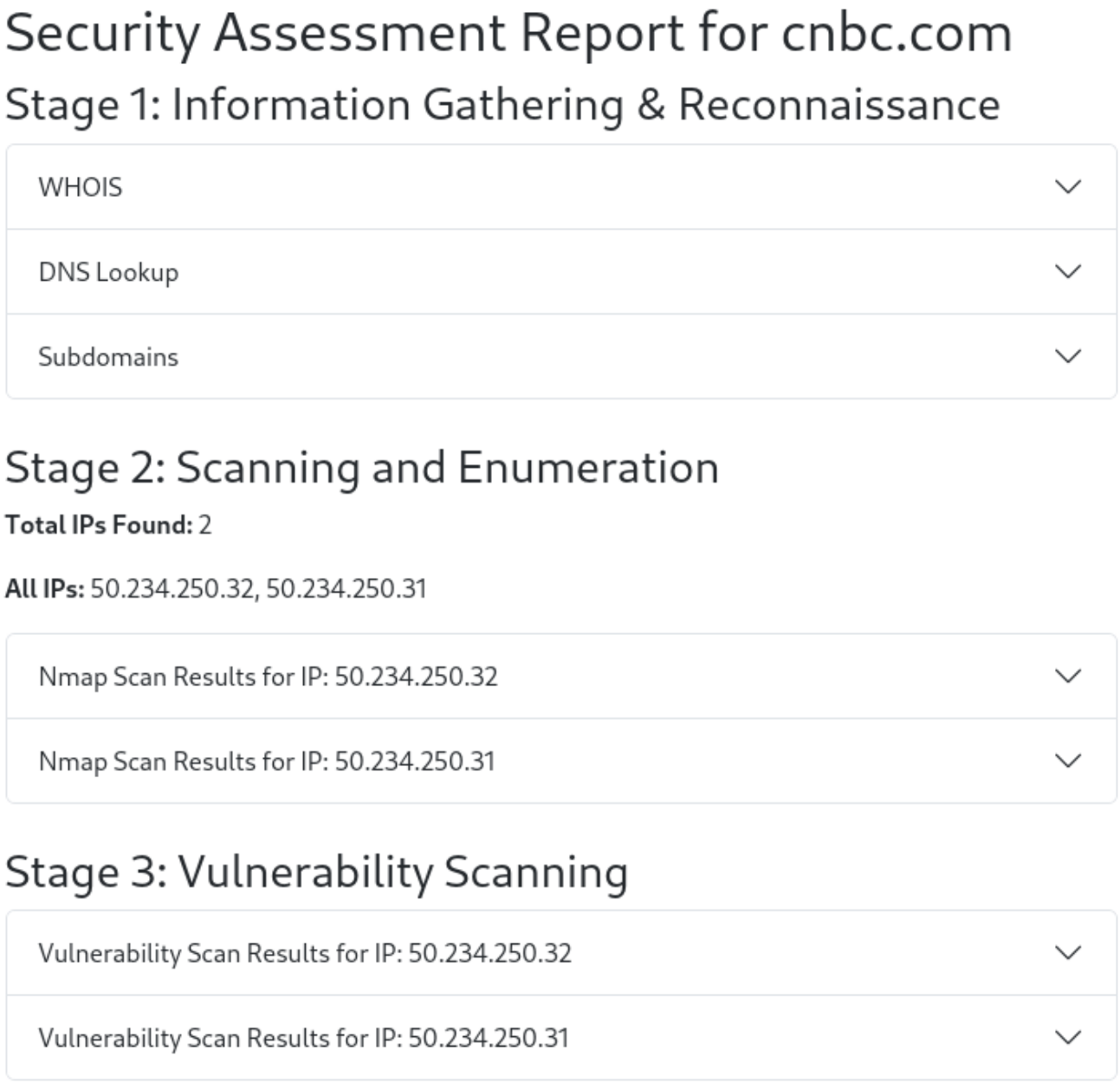
5. Example Output

Sample HTML Report: The HTML report includes collapsible sections for each stage of the scan:

1. **Information Gathering**
2. **Scanning and Enumeration**
3. **Vulnerability Scanning**

Each section provides detailed results, including:

- Subdomain discoveries
- Open ports and services detected by Nmap
- Vulnerabilities detected through the vulners Nmap script (including links to CVE details).



Stage 3: Vulnerability Scanning

Vulnerability Scan Results for IP: 192.168.1.8

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 11:40 CEST
Nmap scan report for 192.168.1.8
Host is up (0.00079s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
20/tcp   closed ftp-data
21/tcp   closed ftp
80/tcp   open   http       Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
| vulners:
|   cpe:/a:apache:http_server:2.4.52:
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A  *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A  *EXPLOIT*
|       F607361B-6369-5DF5-9B29-E90FA29DC565    9.8     https://vulners.com/githubexploit/F607361B-6369-5DF5-9B29-E90FA29DC565  *EXPLOIT*
|       CVE-2024-38476  9.8     https://vulners.com/cve/CVE-2024-38476
|       CVE-2024-38474  9.8     https://vulners.com/cve/CVE-2024-38474
|       CVE-2023-25690  9.8     https://vulners.com/cve/CVE-2023-25690
|       CVE-2022-31813  9.8     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  9.8     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  9.8     https://vulners.com/cve/CVE-2022-22720
|       B02819DB-1481-56C4-BD09-6B4574297109    9.8     https://vulners.com/githubexploit/B02819DB-1481-56C4-BD09-6B4574297109  *EXPLOIT*
|       A5425A79-9D81-513A-9CC5-549D6321897C    9.8     https://vulners.com/githubexploit/A5425A79-9D81-513A-9CC5-549D6321897C  *EXPLOIT*
|       5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9    9.8     https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9  *EXPLOIT*
|       3F17CA20-788F-5C45-88B3-E12DB2979B7B    9.8     https://vulners.com/githubexploit/3F17CA20-788F-5C45-88B3-E12DB2979B7B  *EXPLOIT*
|       1337DAY-ID-39214        9.8     https://vulners.com/zdt/1337DAY-ID-39214        *EXPLOIT*
|       CVE-2024-38475  9.1     https://vulners.com/cve/CVE-2024-38475
|       CVE-2022-28615  9.1     https://vulners.com/cve/CVE-2022-28615
|       CVE-2022-22721  9.1     https://vulners.com/cve/CVE-2022-22721
|       0486EBEE-F207-570A-9AD8-33269E72220A    9.1     https://vulners.com/githubexploit/0486EBEE-F207-570A-9AD8-33269E72220A  *EXPLOIT*
|       CVE-2022-36760  9.0     https://vulners.com/cve/CVE-2022-36760
|       B0A9E5E8-7CCC-5984-9922-A89F11D6BF38    8.2     https://vulners.com/githubexploit/B0A9E5E8-7CCC-5984-9922-A89F11D6BF38  *EXPLOIT*
```

6. Potential Improvements

6.1 Enhancing Subdomain Discovery

- Further DNS mapping can be done by resolving each subdomain to its IP address, repeating the scan on those new IPs to enhance the scope of the security assessment.

6.2 Integrating Third-Party APIs

- **Vulnerability Assessment**: Integrating third-party APIs such as Shodan or the CVE database API can provide real-time vulnerability assessments with enhanced accuracy.

6.3 Performance Optimization

- **Parallelizing Scans**: Currently, scans run sequentially. This could be improved by parallelizing Nmap scans and subdomain lookups to reduce the overall time.

Conclusion

This tool provides an efficient way to automate and streamline security assessments for domains and IPs, applying practical cybersecurity concepts learned during training. By using Python's versatility and integrating tools like Nmap and Sublist3r, the tool offers a comprehensive approach to vulnerability management. Future improvements could further enhance its effectiveness, making it a robust solution for continuous security monitoring.