Lab Manual – Shodan: Passive Reconnaissance & Vulnerability Analysis

---

Title: Vulnerability Analysis using Shodan Search Engine (Passive Reconnaissance)

Aim:

To perform passive reconnaissance and vulnerability analysis of publicly accessible systems using Shodan, without performing active scanning, and to interpret the collected metadata.

Objectives:

1. To understand the concept of Shodan as a search engine for Internet-connected devices.
2. To learn how to retrieve system information using Shodan's interface or API.
3. To identify open ports, services, and possible vulnerabilities (CVEs) from indexed data.
4. To practice ethical and legal guidelines in vulnerability analysis.

Theory:

Shodan Overview:

Shodan is a specialized search engine that indexes information from devices connected to the Internet. Instead of indexing website content like Google, Shodan collects banners and metadata from services running on open ports. These may include:

- Web servers (HTTP/HTTPS)
- FTP, SSH, Telnet services
- Database services (MySQL, MongoDB, etc.)
- IoT devices (CCTV cameras, routers, SCADA systems)

Key features of Shodan:

- **Search Filters:** Allows queries by IP, hostname, country, port, organization, product, etc.
- **Metadata Display:** Shows service banners, SSL certificate data, geographic location, and ISP.
- **Vulnerability Data:** Links to CVE IDs for known vulnerabilities in the detected service versions.
- **Passive Reconnaissance:** Data is retrieved from Shodan's own crawlers — no direct probing is performed by the user.

Ethical Use:

- Only analyze systems you have permission to test or those that are public and indexed in Shodan.
- Do not exploit any vulnerability found.
- Report security issues to the concerned authority through responsible disclosure.

Apparatus / Requirements:

- Laptop/PC with Internet access
- Google account for using Google Colab (optional if using API)
- Shodan account (free or paid) and API key (if using API access)
- Web browser (for using Shodan web interface)

Procedure:

Part A – Using Shodan Web Interface

1. Create a free account at https://www.shodan.io.
2. Log in and navigate to the search bar on the Shodan homepage.
3. Enter a search query, e.g., apache country:IN to find Apache servers in India.
4. Review the results: note the IP addresses, organizations, open ports, and banner information.
5. Identify any CVE numbers listed and research their meaning from the CVE database.

Part B – Using Shodan API (Passive Reconnaissance)

1. Obtain your Shodan API key from the **Account** section of the Shodan website.
2. Open Google Colab or any Python environment.
3. Authenticate using your API key (no scanning code included in this manual).
4. Run a query such as hostname:unipune.ac.in to retrieve indexed public information about the university domain.
5. Analyze the results for open ports, running services, and any vulnerabilities listed.

Part C – Documentation

1. Record your observations in a tabular format:

Sr. No.	IP Address	Port	Service/Product	Organization	Vulnerabilities (CVE IDs)
1	50.6.168.217	80	HTTPS	Newfold Digital, Inc.	- CVE-2008-3844
2	204.10.246.45	443	HTTP	Asante Health System	- CVE-2018-15473

2. Mention the source of each vulnerability entry (e.g., CVE database link).
3. Highlight findings relevant to your target domain or device type.

Observations:

- Open ports and their associated services are visible without direct scanning.
- Banner information can reveal software versions, SSL certificates, and device types.
- Vulnerabilities linked to CVEs may exist for outdated or misconfigured services.

Result:

Thus we observed and collected information of various servers using Shodan.

Conclusion:

Shodan is a very effective tool for reconnaissance purpose.

Precautions:

1. Do not attempt to actively exploit any vulnerability found.
2. Use only your own Shodan account and API key.
3. Limit queries to legal, ethical targets or purely academic purposes.
4. Follow responsible disclosure policies when reporting vulnerabilities.