Kevs Interactive Shodan Simplifier - KISS

Table of Contents

19. **Troubleshooting**
20. **Future Extensions and Customization**

---

1. Introduction

KISS (Kev's Interactive Shodan Simplifier) is a menu-driven Python tool that simplifies the process of constructing and executing queries on Shodan. Instead of memorizing complex syntax and parameters, you navigate through intuitive menus to build, refine, and run powerful searches. KISS also brings in added value by allowing you to manage Shodan Alerts, view statistical facets of your search results, and integrate current trending CVE-based queries, making it a one-stop solution for reconnaissance and analysis.

---

2. What is Shodan?

Shodan is a specialized search engine that indexes internet-connected devices and the services they expose. Rather than focusing on web content like traditional search engines, Shodan reveals which systems are connected, their open ports, banners, and potential vulnerabilities.

Use Cases:

- Identifying exposed IoT devices or servers.
- Finding vulnerable services tied to known CVEs.
- Monitoring networks for changes or new exposures.

Important: Ethical and authorized usage is paramount. Always ensure you have permission and comply with all relevant laws.

---

3. About KISS

KISS aims to:

- Lower the barrier to using Shodan's powerful search capabilities.
- Educate users on query syntax through interactive menus and final-query editing.
- Introduce additional functionalities like trending CVE queries, Alerts management, and statistical analysis.

---

4. Key Features & Enhancements

- **Menu-Based Query Building:** Construct queries step-by-step.
- **Logical Operators (AND/OR):** Combine filters flexibly.
- **Trending CVEs:** Quickly import popular queries referencing current, active vulnerabilities.
- **Shodan Alerts:** Create, list, and delete alerts to monitor networks over time.
- **Stats/Facets:** Obtain top facets (e.g., top ports, top countries) for your query to better understand results distribution.
- **Manual Editing:** Review and refine the final query before execution.
- **Results Pagination & Saving:** Navigate large sets of results page-by-page and export them for offline analysis.
- **Robust Error Handling & Logging:** Track issues and inspect logs for troubleshooting.

These features collectively streamline reconnaissance, helping cybersecurity professionals and researchers work more efficiently.

---

5. Prerequisites

- **Python 3.6+**
- **Shodan API Key:** Obtain from https://www.shodan.io.
- **Internet Connectivity:** Needed for API requests.

---

6. Installation & Configuration

1. **Install Dependencies:**
2. pip install shodan
3. **Configure the API Key:**
    - Open kiss_shodan.py in a text editor.
    - Set SHODAN_API_KEY = "YOUR_API_KEY" to your valid Shodan API key.
4. **Run the Tool:**
5. python kiss_shodan.py

You will see the main menu after launching the program.

---

7. Tool Overview

KISS presents a main menu from which you can:

- Set a target (hostname, organization, network, IP, or start empty).
- Add various filters (ports, vulnerabilities, keywords, OS, etc.).
- Incorporate trending CVEs, manage alerts, and view statistical facets.
- Finalize and manually edit your query before execution.
- Save results to JSON files.

Each step ensures you maintain control and clarity over your searches.

---

8. Menu Options and Usage

8.1. Choose a Target

A target sets the initial scope of your Shodan query. Options include:

- **Domain:** hostname:example.com
- **Organization:** org:"Google LLC"
- **Network (CIDR):** net:192.168.1.0/24
- **IP Address:** 8.8.8.8
- **Nothing:** Start empty and rely solely on filters.

Tip: Starting empty can be useful if you intend to build a very flexible query from scratch.

8.2. Add Filters

Filters refine your search. Common filters:

- **Port:** port:22
- **Vulnerability:** vuln:CVE-2023-12345
- **Key Phrases:** "admin", "default password"
- **Product:** product:Apache
- **Country/City:** country:US, city:"New York"

- **OS:** os:"Windows 10"

For each filter, choose AND or OR to define logical relationships. AND narrows results, OR broadens them.

8.3. Finalize, Edit & Execute Queries

Once satisfied with your query, view the final string:

- **Edit:** Manually correct or refine the query.
- **Run:** Execute it against Shodan.

Manual editing is a powerful learning tool; you see the underlying syntax and can modify it directly.

8.4. Save Results to a File

After retrieving results, choose to save them as a JSON file:

- **Preservation:** Keep a record of your findings.
- **Analysis:** Work offline or integrate with other tools later.

8.5. Add Trending CVE-based Queries

Stay current by exploring what the community is querying:

- **Fetch Trending Queries:** Filter them for queries containing CVE-.
- **Incorporate with AND/OR:** Blend these known high-impact vulnerabilities into your current query for timely insights.

This helps you tap into the security zeitgeist and prioritize relevant exposures.

8.6. Manage Shodan Alerts

Shodan Alerts monitor IPs, ranges, or networks over time and notify you of new discoveries. Within KISS, you can:

- **Create Alerts:** Specify a name and CIDR to watch.
- **List Alerts:** See all currently active alerts.
- **Delete Alerts:** Remove alerts when no longer needed.

This integration enables ongoing security intelligence, turning Shodan from a one-off search engine into a continuous monitoring tool.

8.7. View Stats/Facets

For a given query, gain statistical insights using facets:

- **Select Facets:** e.g., port, country, org.
- **View Top Values:** Understand distribution patterns, top ports, leading countries, or main organizations.

These stats guide further refinements and strategic decision-making, helping you focus on the most relevant results.

8.8. Exit

Close KISS when done. Your saved results and logs remain on your system.

---

9. Syntax Handling & Logical Operators

Shodan treats space-separated terms as AND conditions. OR is explicit and requires careful grouping:

- **AND Example:** hostname:example.com product:Apache (Both must be true)
- **OR Example:** (hostname:example.com) OR (port:443) (Either condition satisfies)

KISS handles these syntactic details for you, ensuring valid queries.

---

10. Trending CVEs & Their Significance

Trending CVE-based queries connect you to current exploits in the wild. By adding these:

- Focus on known vulnerabilities currently drawing attention.
- Stay agile in response to rapidly evolving threat landscapes.

---

11. Shodan Alerts Management

Alerts maintain continuous coverage:

- **Create:** Set an alert on a network to track new open ports or devices.
- **List:** Keep an eye on all monitored ranges.
- **Delete:** Clean up old alerts as conditions change.

This turns passive searches into proactive security workflows.

---

12. Shodan Stats/Facets

Facets provide quick analytics:

- **Ports Distribution:** Which ports are most common in your results?
- **Geographic Insights:** Top countries or cities hosting exposed devices.
- **Organizational Breakdown:** Identify top organizations involved.

Armed with these stats, you make more informed decisions.

---

13. Manual Query Editing

Before running the query, you can revise it. This helps you:

- Correct typos.
- Add unsupported filters directly.
- Understand and perfect Shodan syntax.

Manual editing transforms KISS into both a learning platform and a power user's tool.

---

14. Results & Pagination

Shodan results can be large. KISS paginates them:

- **N**: Next Page
- **P**: Previous Page
- **M**: Return to Main Menu

Manageable navigation ensures you don't get lost in massive data sets.

---

15. Error Handling & Logging

Errors (API issues, invalid keys, network downtime) are displayed and logged in shodan_tool.log. Refer to the log for:

- Debugging configuration issues.
- Reviewing past errors for continuous improvement.

---

16. Tips & Best Practices

- **Start Broad, Then Narrow:** Don't overspecialize too soon. Add filters incrementally.

- **Use OR Sparingly:** OR conditions can broaden searches drastically. Use them thoughtfully.
- **Leverage Facets & Alerts:** Move beyond static searches to continuous monitoring and analytical insights.
- **Save Early and Often:** Don't lose valuable results—export regularly.

---

17. API Key Management

- Keep your API key secure (treat it like a password).
- If compromised, regenerate it from your Shodan account.
- Be mindful of Shodan's usage limits; higher-tier plans may offer more queries or alerts.

---

18. Legal & Ethical Considerations

- **Authorized Testing:** Only investigate systems you have permission to assess.
- **Data Privacy:** Respect sensitive information uncovered by searches.
- **Compliance:** Know and follow the laws of your jurisdiction.

---

19. Troubleshooting

- **No Results:** Loosen filters or add OR conditions.
- **Slow Performance:** Shodan queries may be rate-limited or network-bound.
- **API Errors (Unauthorized):** Check your API key and account status.
- **Logs:** Consult shodan_tool.log for deeper insight.

---

20. Future Extensions and Customization

KISS is designed for adaptability. Potential extensions:

- **More Filters:** Include SSL certificates, HTTP favicon hashes, etc.
- **Integration with Other Tools:** Export results in different formats.
- **Automated Workflows:** Schedule queries or alerts to run periodically.

Your contributions or modifications can tailor KISS even more closely to your operational needs. As always with Kev's scripts, feel free to use them and improve them as you see fit!