SHODAN
The Search Engine for the Internet of Things (IoT)

Jeff Tomkiewicz, Sec + | CEH
- What is Shodan?
- History behind Shodan
- How Shodan Works
- How to incorporate Shodan into Kali Linux
- How to conduct searches
- Questions
What is Shodan?

Shodan is considered the first search engine for Internet of Things (IoT) devices.

Any thing from web cams, water treatment facilities, yachts, medical devices, traffic lights, wind turbines, license plate readers, smart TVs, refrigerators and many more.
History Behind Shodan

- Created by John Matherly
- Launched in 2009
- Developed as a “pet project” based on the fact that large numbers of devices and computer systems are connected to the Internet.
- Been described as the “The scariest search engine on the Internet”
How Shodan Works

Shodan works simply by:

- Searches random IPv4 address
- Generate a random port to test from the list of ports that Shodan understands
- Check the random IPv4 address on the random port and grab a banner (Banner Grabbing)
- YES IT IS LEGAL!
How Shodan Works
How to Incorporate Shodan into Kali Linux

First step is to create an account on Shodan.io (https://www.shodan.io/)
How to Incorporate Shodan into Kali Linux

- Next click on “My Account” in the upper right side of the page.
You will now see QR Code and API Key on your account. At this time we will reduce this window and open up our Kali Virtual Machine Box.
Once in on your Kali Linux box open a terminal and type in the prompt “pip install shodan” and press enter.
How to Incorporate Shodan into Kali Linux

➤ Go back to your Shodan account page and copy your API Key.

➤ Then go back to your Kali Linux Box and in the terminal type “shodan init” followed by your API key. Then press enter.
How to Conduct Searches using the Command Line (CLI)

- The Shodan CLI has a lot of commands. For the full list of commands just run the tool without any arguments:
How to Conduct Searches using the Command Line (CLI)

- **count**: Returns the number of results for a search query.
How to Conduct Searches using the Command Line (CLI)

**download**: this command is what you should be using most often. It lets you save the results and process them afterwards using the parse command.

**NOTE**: Because paging through results uses query credits, it makes sense to always store searches that you're doing so you won't need to use query credits for a search you already did in the past.
**parse:** to analyze a file that was generated using the **download** command. It lets you filter out the fields that you're interested in, convert the JSON to a CSV and is friendly for pipe-ing to other scripts.
**How to Conduct Searches using the Command Line (CLI)**

- **host:** See information about the host such as where it's located, what ports are open and which organization owns the IP.
How to Conduct Searches using the Command Line (CLI)

↑ **myip:** Returns your Internet-facing IP address.
How to Conduct Searches using the Command Line (CLI)

**search**: This command lets you search Shodan and view the results in a terminal-friendly way. By default it will display the IP, port, hostnames and data. You can use the **--fields** parameter to print whichever banner fields you're interested in.
Additional Information

- **Complete Guide to Shodan:**
  - [https://leanpub.com/shodan](https://leanpub.com/shodan)

- **Shodan – Search Engine For Hackers – Beginner Guide:**
  - [https://hsplotit.com/shodan-search-engine-for-hackers-beginner-guide/](https://hsplotit.com/shodan-search-engine-for-hackers-beginner-guide/)
Questions?
Conclusion

- What is Shodan?
- History behind Shodan
- How Shodan Works
- How to Incorporate Shodan into Kali Linux
- How to Conduct Searches using the Command Line (CLI)