Shodan, Zoomeye and Censys

While traditional search engines like Google and Bing are invaluable resources, specialized search engines like Shodan, ZoomEye, and Censys offer a unique advantage in the realm of cybersecurity reconnaissance.

So In simple terms, these search engines act like specialized versions of Google, but instead of searching for websites, they search for and catalogue internet-connected devices and systems. They provide detailed information about these devices, including their IP addresses, software versions, open ports, and potential vulnerabilities.

We will start off with Shodan which is also called the hacker's search engine.

https://www.shodan.io/

- `city` : find devices in a particular city
- `country` : find devices in a particular country
- `geo` : you can pass it coordinates
- `hostname` : find values that match the hostname
- `net` : search based on an IP or /x CIDR
- `os` : search based on operating system
- `port` : find particular ports that are open
- `before/after` : find results within a timeframe
- `org` : Search by organization
- `hash` : Search based on banner hash
- `has_screenshot:true` : Filter search based on a screenshot being present
- `title` : Search based on text within the title
- ssl:"domain.com"

Shodan Browser Extension

- Go to Mozilla HamBurger menu -> Click on Add-ons and themes -> Search Shodan -> Add it to Firefox

Next, we have Zoomeye. It is similar like Shodan but with some additonal features like it allows us to search for specific devices, services, or vulnerabilities, and it provides information about the technologies and products used by the indexed devices.

- https://www.zoomeye.hk/

Third one is Censys. This is also similar like the previous one. However, It focuses more on security aspects, providing information about known vulnerabilities, SSL certificates, and potential security risks. It is valuable for monitoring and securing devices and online services, as well as identifying potential attack vectors.

- https://search.censys.io/
