Shodan Cheat Sheet

What is Shodan?

Shodan is a search engine that scans and indexes devices connected to the internet. Unlike Google, which indexes web pages, Shodan indexes **servers, webcams, routers, databases, industrial control systems, and IoT devices**.

Basic Shodan Search Queries

These are the fundamental operators used to find exposed devices and services.

Operator	Description	Example
`hostname:`	Find devices by domain or subdomain.	`hostname:example.com`
`country:`	Filter results by country code.	`country:US`
`city:`	Search for devices in a specific city.	`city:New York`
`org:`	Find devices belonging to an organization.	`org:"Google LLC"`
`isp:`	Search by internet service provider.	`isp:"Comcast"`
`port:`	Find devices with specific open ports.	`port:22` (SSH)
`before:` / `after:`	Find results indexed before/after a date.	`before:2024-01-01`

Finding Specific Devices & Services

1. Webcams & Surveillance Cameras

- `product:"GoAhead WebServer"` → Searches for embedded cameras using GoAhead WebServer.
- `title:"webcam"` → Generic search for webcams.
- `port:554 has_screenshot:true` → Finds RTSP streams.
- `port:80 title:"IP Camera"` → Looks for open IP cameras.

2. Databases

- `port:27017 product:"MongoDB"` → Finds exposed MongoDB databases.
- `port:5432 product:"PostgreSQL"` → Exposed PostgreSQL databases.
- `port:3306 product:"MySQL"` → Exposed MySQL servers.
- `product:"Elasticsearch" port:9200` → Exposed Elasticsearch clusters.

3. Industrial Control Systems (ICS)

- `port:102 Siemens` → Siemens industrial control systems.
- `port:502 Modbus` → Exposed Modbus controllers.
- `port:47808 BACnet` → Building automation controllers.

4. Routers & Network Devices

- `port:22 OpenSSH` → Find SSH servers.
- `port:23 product:"Cisco"` → Look for exposed Cisco devices on Telnet.
- `port:7547` → Exposed TR-069 router management interfaces.

Advanced Search Techniques

Combining Filters

You can combine multiple search operators to refine results.

- `country:IN org:"Reliance Jio" port:23` → Find Telnet services in India by Reliance Jio.
- `org:"Microsoft" port:3389 has_screenshot:true` → Find Microsoft RDP servers with screenshots.

Finding Vulnerable Systems

Shodan helps identify systems with known vulnerabilities.

- `vuln:CVE-2021-26855` → Find devices affected by a specific CVE.
- `product:"Apache httpd" version:"2.4.49"` → Locate Apache servers running a specific vulnerable version.

Shodan Dorks for OSINT Investigations

- `ssl.cert.subject.cn:"example.com"` → Find SSL certificates issued for a domain.
- `net:192.168.1.0/24` → Search for devices in a specific IP range.
- `after:2023-06-01 before:2024-01-01` → Devices indexed in a specific time range.
- `has_screenshot:true` → Show only results with screenshots.

Shodan API & CLI Usage

For automation and deeper analysis, use the Shodan API and CLI.

Installing Shodan CLI

```
pip install shodan
shodan init YOUR_API_KEY
```

Basic Commands

```
shodan search "port:22 country:US"
shodan host 8.8.8.8
shodan count "org:Amazon"
shodan stats "port:443"
```

Exporting Data

```
shodan download results.json.gz "org:Google"
shodan parse results.json.gz
```

Defensive Measures

If you're an organization, protect yourself from Shodan reconnaissance:

- **Restrict unnecessary ports** on firewalls.
- **Use strong authentication** for remote access services.
- **Disable default credentials** on all devices.
- **Monitor Shodan** for your own infrastructure.

Use Cases

✅ **Security Research** – Identify exposed devices and misconfigurations.

✅ **Penetration Testing** – Discover vulnerabilities for ethical hacking.

✅ **Threat Intelligence** – Monitor open ports and internet-facing assets.

❌ **Unauthorized Access** – Exploiting exposed systems without permission is **illegal**.

Shodan is a powerful OSINT tool for cybersecurity professionals. Use it **ethically** and **responsibly** to enhance security, not exploit it. 🚀