🛰️ Shodan – Ultimate Cheat Sheet

🔹 1. Basics

Shodan = "Search Engine for Hackers"
It indexes devices & services connected to the internet.

CLI Syntax

```
shodan [command] [options]
```

Authentication (first time only)

```
shodan init YOUR_API_KEY
```

🔹 2. Core Commands

Command	Example	Description
shodan init	shodan init APIKEY	Authenticate with API key
shodan info	shodan info	Show account info & API stats
shodan search	shodan search apache	Search devices/services
shodan count	shodan count nginx	Count results without details
shodan host	shodan host 8.8.8.8	Get info about an IP
shodan domain	shodan domain example.com	Get domain info
shodan myip	shodan myip	Show your public IP
shodan stats	shodan stats nginx --facets country	Statistics breakdown

---

🔷 3. Search Filters

Common Filters

Filter	Example	Description
ip:	ip:8.8.8.8	Search by IP
net:	net:192.168.1.0/24	Search by subnet
port:	port:22	Search by port
org:	org:Google	Filter by organization
hostname:	hostname:example.com	Search by hostname
country:	country:IN	Filter by country
city:	city:Mumbai	Filter by city
before/after:	before:2025-01-01	Filter by crawl date
os:	os:Windows	Filter by operating system
product:	product:nginx	Filter by software

🔷 4. Examples

Find Apache servers in India

```
shodan search "apache country:IN"
```

Find devices on port 22 (SSH)

```
shodan search "port:22"
```

Find MySQL databases exposed

```
shodan search "port:3306 product:mysql"
```

Find webcams

```
shodan search "webcam"
```

Count nginx servers in US

```
shodan count "nginx country:US"
```

🔷 5. Host Information

Get details about an IP

```
shodan host 8.8.8.8
```

Shows:

- Open ports
- Services running
- Organization
- Location

🔷 6. Stats & Facets

Facets = breakdown by category.

Example: Breakdown of Apache servers by country

```
shodan stats apache --facets country
```

Example: Breakdown of MySQL servers by port

```
shodan stats "product:mysql" --facets port
```

🔷 7. Downloading Data

Save results to file

```
shodan download apache_results apache
```

Read results

```
shodan parse apache_results.json.gz
```

🔷 8. Alerts & Monitoring

Create alert for network monitoring

```
shodan alert create "My Home" 192.168.1.0/24
```

List alerts

```
shodan alert list
```

Delete alert

```
shodan alert delete ALERT_ID
```

🔷 9. Advanced Search Strings

Query	Finds
port:21 Anonymous user logged in	FTP servers with anonymous login
port:23 "Welcome to"	Telnet banners
ssl:"Google"	Certificates mentioning "Google"
http.title:"WebcamXP"	Webcam interfaces
default password	Devices with default credentials in banners
port:3389 has_screenshot:true	RDP servers with screenshots

🔷 10. Tips & Notes

- Always start with **shodan info** to check API credits left.
- Use **filters** (port:, org:, country:) to narrow down results.
- Combine filters for laser-focused searches:
- shodan search "apache port:80 country:US"
- Shodan has **rate limits** – use downloads for bulk analysis.
- Great for **OSINT, pentesting, red team recon**.

⚡ With this cheat sheet, you can leverage Shodan for **IP/port/device discovery, banner analysis, monitoring networks, and OSINT research** like a professional hacker.