Shodan — Professional Cheat Sheet

One-page professional reference for **Shodan** — the search engine for Internet-connected devices. Quick commands, filters, API examples, scanning notes, and OPSEC for security pros and researchers.

---

1) At-a-glance

- **Tool:** Shodan (https://www.shodan.io) — indexes banners and metadata from devices/services exposed to the Internet (routers, webcams, ICS, servers, IoT, proxies).
- **Primary uses:** Asset discovery, exposure assessment, identifying vulnerable services (CVE/CPE), threat intelligence and incident response enrichment.
- **Access:** Web UI (search + filters), CLI (`shodan`), and API (Python/REST). API key required for most programmatic features.

---

2) Accounts & API keys

- Create a Shodan account and find your API key on the web dashboard.
- Free accounts have limited queries; paid tiers increase query, scan credits, and API rate limits.
- Store API keys securely (env var or vault). Example: `export SHODAN_API_KEY="ABCD..."` or `shodan init <api_key>` .

---

3) Common search filters (use in web UI and API)

- `country:` — country code (e.g., `country:"US"`).
- `city:` — city name (e.g., `city:"Bengaluru"`).
- `org:` — organization name (e.g., `org:"Amazon"`).
- `asn:` — autonomous system number (e.g., `asn:AS15169`).
- `hostname:` — hostnames or reverse DNS.
- `net:` — CIDR range (e.g., `net:192.168.0.0/16` — only public ranges).
- `port:` — TCP/UDP port (e.g., `port:22`).
- `product:` / `version:` / `os:` — banner product/version/OS fields.
- `vuln:` / `cve:` — search by vulnerability (e.g., `vuln:CVE-2017-0144` or `cve:CVE-2021-44228`).
- `before:` / `after:` — filter results by scan date.
- `ssl:` / `http.title:` / `html:` — search within TLS/HTTP details (e.g., `ssl.cert.subject.cn:"example.com"` or `http.title:"Admin"`).
- `device:` / `tag:` — provider-provided tags or device classes (depends on Shodan metadata).

Combine filters with Boolean operators and quotes: `apache country:"DE" port:80 vuln:CVE-2017-5638` .

4) Useful search examples

- Find open SSH in India: `port:22 country:"IN" ssh`
- Cameras with default credentials or common pages: `title:"Live View" port:80`
- Elasticsearch instances with RCE CVE: `product:Elasticsearch cve:CVE-2015-1427`
- Exposed databases (MongoDB default port): `port:27017 has_screenshot:false` (then validate manually)
- Services with specific header: `http.favicon.hash:123456789` (useful for narrow fingerprinting).

---

5) Shodan CLI basics

- Install: `pip3 install --upgrade shodan` or `apt install shodan` (package availability varies).
- Initialize: `shodan init YOUR_API_KEY`
- Common commands:
- `shodan search <query>` — search and show top results.
- `shodan count <query>` — estimate number of results.
- `shodan host <ip>` — get detailed host info and services for an IP.
- `shodan exploit <query>` — search exploit DB (when available).
- `shodan scan` / `shodan scan submit` — submit scan jobs (requires credits/paid plan).
- `shodan download <file> <query>` — download full result set as JSON for offline processing.
- `shodan myip` — show your public IP.

Example: `shodan search --fields ip_str,port,org 'nginx country:"US" port:80'`

---

6) API usage (Python) — quick examples

```
from shodan import Shodan
api = Shodan('YOUR_API_KEY')
# Search
results = api.search('apache country:"US"')
print(results['total'])
for r in results['matches']:
    print(r['ip_str'], r['port'], r.get('location', {}))

# Host lookup
host = api.host('8.8.8.8')
print(host['os'], host['vulns'])
```

- Use `api.search_cursor()` or `api.search()` with pagination for large result sets.
- Respect rate limits and store results; don't brute-force queries programmatically.

7) Exploit & vuln workflows

- Use `vuln:` or `cve:` filters to find hosts with known CVEs.
- Validate results manually: Shodan's banner may show a vulnerability string but not guarantee exploitable state.
- Combine with `nmap -sV --script=vuln` or targeted `sqlmap` / `metasploit` checks only against authorized assets.

---

8) Scanning & monitoring

- Shodan offers on-demand scanning (paid) and monitors/alerts.
- Use `shodan scan` to launch scans (requires credits) or schedule alerts in the web UI.
- Configure email/Slack/webhook alerts for new matches to queries (useful for monitoring exposed assets).

---

9) Exporting & processing results

- Use `shodan download <file> '<query>'` to save JSON results.
- Parse JSON with `jq` or Python to extract IPs, ports, banners, and CVEs for triage.
- Example: `shodan download results 'port:3389 country:"US" vuln:CVE-2020-0796'` then `gunzip -c results.json.gz | jq .`.

---

10) Tips & best practices

- **Start narrow:** filter by net/org/ASN to limit noise and stay within scope.
- **Validate findings:** treat Shodan results as leads — verify with direct probes and human analysis.
- **Respect rate limits and terms:** do not automate abusive query volume.
- **Use monitors for asset inventory:** save queries and get alerts for newly exposed hosts.
- **Protect API key:** avoid embedding in public scripts; use environment variables or configuration management.

---

11) Common pitfalls & caveats

- **Banner accuracy:** banners can be stale or spoofed; Shodan scans periodically — check `timestamp` in results.
- **False positives:** services may report vulnerable strings without exploitable configuration.
- **Legal/ethical:** using Shodan to find targets without permission and then attacking them is illegal. Use only within authorized scope.

---

12) One-liners & examples

```
# Count RDP hosts in India
shodan count 'port:3389 country:"IN"'

# Search and list IPs
shodan search --fields ip_str,port,org 'RDP product:Microsoft-Remote-Desktop'

# Host detail
shodan host 203.0.113.5

# Download results for offline processing
shodan download rdp_india 'port:3389 country:"IN"'
```

---

13) Alternatives & complements

- **Censys, ZoomEye, BinaryEdge** — other Internet-wide scanners with different datasets and query models.
- **Passive DNS / certificate transparency (crt.sh)** — complement Shodan for historical DNS and subdomain discovery.

This cheat sheet is for authorized reconnaissance, threat hunting, and asset discovery. Use Shodan responsibly and only on networks you own or are authorized to test.