**🌐 Shodan – The Search Engine for Hackers**

**Level:** Beginner-friendly

**Category:** OSINT / Reconnaissance

**🧠 What is Shodan?**

Shodan is like **Google**, but instead of searching websites, it searches **devices connected to the internet**:  
🖥️ Servers, 🎥 webcams, 🏠 smart home devices, 🛰️ routers, 🔒 industrial control systems (ICS), and more!

* Website: 🌐 [https://www.shodan.io](https://www.shodan.io/)

**🧪 Why Use Shodan in OSINT?**

| **Purpose** | **What You Can Do** |
| --- | --- |
| 🔍 Find exposed services | Discover public IPs running services (SSH, FTP, RDP, HTTP, etc.) |
| 🛡️ Check your own assets | Make sure your devices aren’t exposed |
| ⚠️ Spot misconfigurations | Unsecured databases, webcams, routers |
| 👁️ Detect vulnerable software | Search devices running outdated or vulnerable versions |
| 🌍 Country/ISP monitoring | See what’s exposed in specific regions (like Pakistan!) |

**🚀 How to Use Shodan – Step-by-Step**

**1. Go to** [**https://shodan.io**](https://shodan.io/)

You’ll need a free account for advanced filters and full results.

**2. 🔍 Start with Basic Search Examples**

| **Query** | **What It Does** |
| --- | --- |
| apache | Finds servers running Apache HTTP server |
| port:21 | Shows devices with FTP open |
| country:PK | Only show results from Pakistan |
| org:"PTCL" | Show devices from a specific ISP |
| title:"webcam" | Find open webcams |
| os:"Windows 7" | Find systems running old Windows versions |
| product:"MongoDB" | Find exposed MongoDB databases |

**🔐 Example: Find RDP servers in Pakistan**

port:3389 country:PK

**📸 Example: Search for unsecured webcams**

has\_screenshot:true title:"webcam" country:PK

**⚒️ What Kind of Info You Get**

Each result shows:

| **Field** | **Meaning** |
| --- | --- |
| IP Address | Where the device is hosted |
| Port | Which port is open (e.g. 22 for SSH) |
| Service | What’s running (e.g. nginx, Apache, MySQL) |
| Hostname | Sometimes shows domain/subdomain |
| Location | Country, city, ISP |
| Banner | Full details of service/version |
| CVEs | Vulnerabilities (for paid users) |

**⚠️ Legal & Ethical Reminder**

❗ **Only use Shodan for learning or ethical research.**  
Never use it to exploit or attack systems you don’t own or have permission to test.  
✅ Use it in your **own lab** or for **bug bounty/CTF** practice.

**🧠 Real-World Use Cases**

| **Use Case** | **Example** |
| --- | --- |
| 🏠 IoT Awareness | Find unsecured baby cams or smart fridges |
| 🏢 Enterprise Security | Find exposed company servers by IP/organization |
| 🔍 Threat Hunting | Monitor for vulnerable services in specific regions |
| 🧑‍💻 Red Team Recon | Use before launching a penetration test |
| 🎯 Target Profiling | Combine with SpiderFoot, RITA, or WHOIS data |

**🎯 Bonus: Shodan CLI (for power users)**

You can install Shodan on the command line:

pip install shodan

shodan init YOUR\_API\_KEY

shodan search apache country:PK

**📚 Summary**

| **Feature** | **Benefit** |
| --- | --- |
| Google for Hackers | Search internet-connected devices |
| OSINT & Recon | Great for ethical hackers and researchers |
| Easy to Use | Web UI + CLI available |
| Risk Finder | Identify exposed, misconfigured, or vulnerable services |