SHODAN Quick Start Reference shodan.io

What is Shodan?

Shodan is a publicly available search engine which scans the entire Internet for a limited number of services and enumerates any discovered services by their banner responses, indexes that data and makes it searchable.

Shodan stores the information and indexes across five main fields: **data, ip_str, port, org** and **location.country_code**.

Be sure to use the **'View Raw Data'** option on any discovered host to see all of the data Shodan has stored and learn possible new techniques of use.

While not always required, **surround each search team in quotes** to reduce confusion and broken queries.

IP Addresses & Subnets

Single IP Address – Search findings on single IP
Example: **52.179.197.205**

Hostname – Search for string in any hostnames
Example: **hostname:"microsoft.com"**

Subnet – Search across a specific subnet range
Example: **net:"52.179.197.0/24"**

Port – Find any instances of active services on a port
Example: **port:"21"**

Service – Search for instances of specific services
Example: **"ftp"**

Service on Specific Port
Example: "**ftp" port:"21"**

Internet Service Provider – Search by ISP name
Example: **isp:"Spectrum"**

Autonomous System Number (ASN) – Search by ASN
Example: **ASN:"AS8075"**

Physical Location

Country – Search by country code
Example: **country:"US"**

City – Search by city name
Example: **city:"New York"**

State – Search by state code abbreviation
Example: **state:"NY"** *or* **region:"NY"**

Zip Code – Search by postal ZIP code
Example: **postal:"92127"**

Geo – Search by GPS coordinates
Example: **geo:"40.759487,-73.978356"**

Geo – Search by GPS (within a range - of 2 Km)
Example: **geo:"40.759487,-73.978356,2"**

Operating Systems, Products

Operating System – Search by operating system type
Examples: **os:"Windows Server 2008"**
os:"Linux 2.6.x"

Organization/Company – Search by organization name
Example: **org:"Microsoft"**

Product – Search by known product name
Example: **product:"Cisco C3550 Router"**

Version – Search for specific version number
Example: **product:"nginx" version:"1.8.1"**

Category – Search by Shodan category
Example: **category:"ics"** *or* **category:"malware"**

Microsoft SMB – Search for specific SMB versions
Example: **smb:"1"** *or* **smb:"2"**

Microsoft Shared Folders – Find exposed shared folders
Example: **port:"445" "shares"**

Web Apps

Page's Title – Search for text in page's title
Example: **title:"Index of /ftp"**

Page's HTML Body – Search body of webpage for text string
Example: **html:"XML-RPC server accepts"**

Web Technologies – Search for specific web technologies
Example: **http.component:"php"**

SSL/TLS – Search for SSL/TLS versions supported
Example: **ssl.version:"sslv3"***or* **ssl.version:"tlsv1.1"**

Expired Certificates – Search for expired HTTPS certs
Example: **ssl.cert.expired:"true"**

Other

Date: After – Search for findings that appear after a date
Example: **after:"01/01/18"**

Date: Before – Search for findings that appear before a date
Example: **before:"12/31/17"**

Screenshot – Display results which only have screenshots
Example: **port:"80" has_screenshot:"true"**
* Watch the webcams roll in!

port:"3389" has_screenshot:"true"
* Watch for exposed Window domain & users!

Limited Access

There are number of useful operators that require premium paid accounts (Enterprise, Academic, etc)

Vulnerability – Search by CVE ID number
Example: **vuln:"CVE-2017-0143"**

Tags – Search based on Shodan tagged data
Example: **tag:"ics"** *or* **tag:"database"**

A special thank you to John Matherly (@achillean) and the rest of the Shodan team (@shodanhq)!!!

By Michael Holcomb (@mdholcomb)