

Shodan


Industrial Control Reconnaissance

What is Shodan

- **Shodan** (<http://www.shodan.io/>) -a web based search engine designed by John Matherly
- Different from content search engines (such as Google or Bing)
- **Shodan** interrogates ports and grabs the resulting banners, then indexes the banners for searching

What is Shodan

[Shodan](#) [Developers](#) [Book](#) [View All...](#)


 **SHODAN**

[Explore](#) [Downloads](#) [Reports](#) [Enterprise Access](#) [Contact Us](#) [My Account](#)


Explore

Discover the Internet using search queries shared by other users.


Featured Categories



Industrial Control Systems



Databases



Video Games

Top Voted

7,191

Webcam
best ip cam search I have found yet.

[webcam](#) [surveillance](#) [cams](#)

2010-03-15

2,497

Cams
admin admin

[cam](#) [webcam](#)

2012-02-06

1,622

Netcam

Recently Shared

2

WEBCAM

2016-06-17

1

city:Madrid Apache

2016-06-17

2

ex

Shodan Search

- Basic Operations: Search
- Search terms are entered into a text box
- Quotation marks can narrow a search
- Boolean operators + and - can be used to include and exclude query terms (+ is implicit default)



SHODAN



[Explore](#)

[Downloads](#)

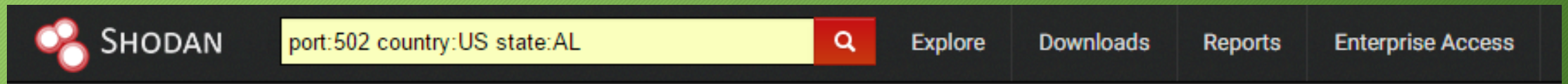
[Reports](#)

[Enterprise Access](#)

[Contact Us](#)

Shodan Search Filters


- **country:** two letter country code
- **hostname:** specify hostname or domain
- **net:** specify IP range or subnet
- **os:** search for specific operating systems
- **port:** specify service port



Shodan Search

[Exploits](#) [Maps](#) [Share Search](#) [Download Results](#) [Create Report](#)

TOP COUNTRIES



United States	8
---------------	---

TOP CITIES

Huntsville	2
Tuscaloosa	1
Montgomery	1
Horton	1
Fort Payne	1

TOP ORGANIZATIONS

Charter Communications	3
University of Alabama	2
Comcast Cable	1
Andycable	1
AT&T Services	1

Total results: 8

146.229.144.113

University of Alabama
Added on 2016-06-11 21:05:59 GMT
 United States, Huntsville
[Details](#)

Unit ID: 0

Unit ID: 1

-- Slave ID Data: d : (0464ff3afd)

-- Device Identification: Square D 15101 14.190

Unit ID: 2

-- Slave ID Data: d ;1 (0464ff3b6c)

-- Device Identification: Square D 15212 10.520

Unit ID: 3

-- Slave ID Data: d ;1 (0464ff3b6c)

-- Device Identification: Square D 15212 ...

12.96.152.234

mail.fleminc.com
AT&T Services
Added on 2016-06-09 09:17:34 GMT
 United States, Montgomery
[Details](#)

Unit ID: 0

-- Slave ID Data: Illegal Function (Error)

-- Device Identification: Illegal Function (Error)

Unit ID: 1

-- Slave ID Data: Illegal Function (Error)

-- Device Identification: Illegal Function (Error)

Unit ID: 2

-- Slave ID Data: Illegal Function (Error)

-- Device Identification: Illeg...

Alternative: Nmap Modbus-discover

- Enumerates SCADA Modbus slave ids (sids) and collects their device information.
- This script does Modbus device information disclosure. It tries to find legal sids (slave ids) of Modbus devices and to get additional information about the vendor and firmware.
- Download the script `modbus-discover.nse` from

<https://nmap.org/nsedoc/scripts/modbus-discover.html>

Alternative: Nmap Modbus-discover

Example:

```
nmap --script modbus-discover.nse --script-args='modbus-discover.aggressive=true' -p 502 <host>
```

Output:

PORT STATE SERVICE

502/tcp open modbus

| modbus-discover: | sid 0x64:

| Slave ID data: \xFA\xFFPM710PowerMeter

| Device identification: Schneider Electric PM710 v03.110

| sid 0x96:

|_ error: GATEWAY TARGET DEVICE FAILED TO RESPONSE