Shodan: Search Engine for Hackers

|  |
| --- |
| Copyrights 2016-2017 Frank Xu, Bowie State University.  The lab manual is developed for teaching cybersecurity courses.  Comments and suggestions can be sent to wxu@bowiestate.edu |

**Introduction**

Sentient Hyper-Optimized Data Access Network (Shodan) has been getting a lot of publicity lately as a "scary" search engine that can be used to facilitate hacking.

(Wiki) Shodan is a search engine that lets the user find specific types of computers (web cams, routers, servers, etc.) connected to the internet using a variety of filters. Some have also described it as a search engine of service banners, which are meta-data the server sends back to the client. This can be information about the server software, what options the service supports, a welcome message or anything else that the client can find out before interacting with the server.

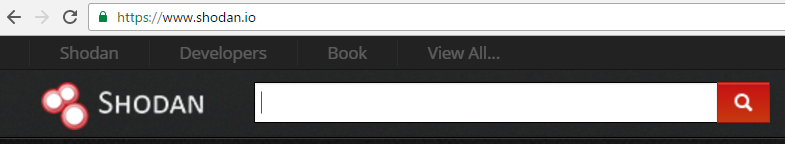
Shodan collects data mostly on web servers (HTTP, port 80), as well as FTP (port 21), SSH (port 22) Telnet (port 23), SNMP (port 161), SIP (port 5060), and Real Time Streaming Protocol (RTSP, port 554). The latter can be used to access webcams and their video stream.

It was launched in 2009 by computer programmer John Matherly, who, in 2003, conceived the idea of searching devices linked to the Internet. The name Shodan is a reference to SHODAN, a character from the System Shock video game series.

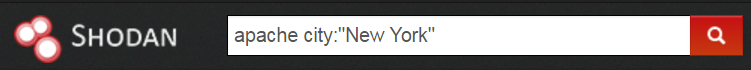
The trick to using Shodan effectively is to know the right keywords. Usually they are the manufacturer’s name, or a device model number, but sometimes they are the name of a very obscure embedded web server that you would never think to look for. But once you know these magic keys, in seconds you can search the world for these devices. Or by using filter commands you can refine your search to certain devices and areas.

A security tester can use Shodan to very quickly assess what systems on their network are being displayed publicly, when maybe they should not be. It can also allow them to find possible rogue or unauthorized devices that have been added to the company network.

**Task 0: Shodan Website**



**Task 1: Find Apache servers in New York**



1. ***Colon :*** require
2. ***Double quotes:*** optional
3. ***Space between city and name of the city***: none

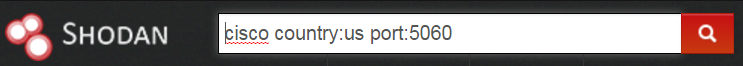
**Task 2: Find Apache servers in the United States**



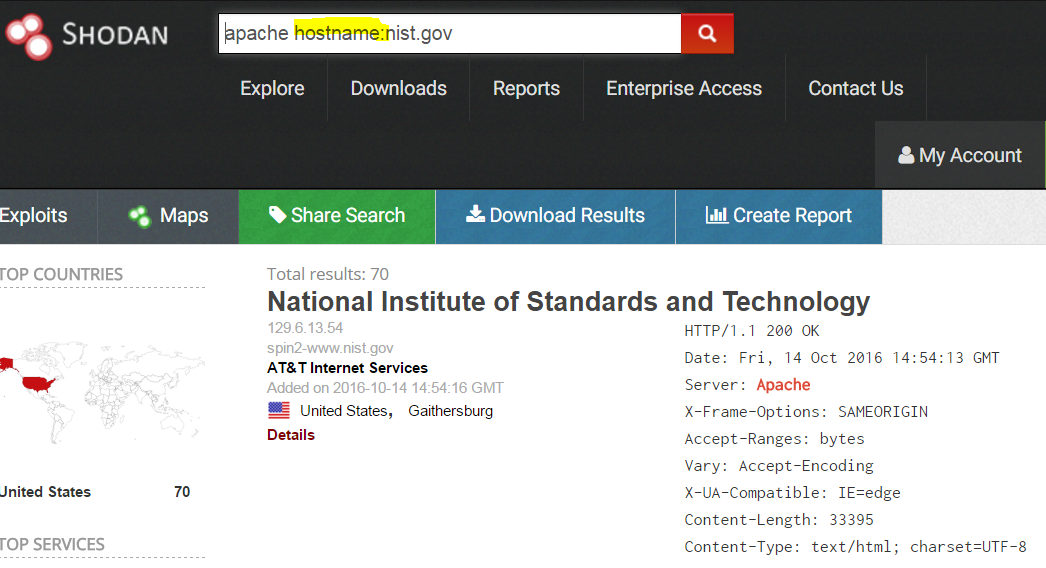
Note: Two-letter country code of United States is **US**. Note the colon (:) between the keyword country and the two-letter country code.

**Task 3: Find Cisco devices Apache servers in the United States**

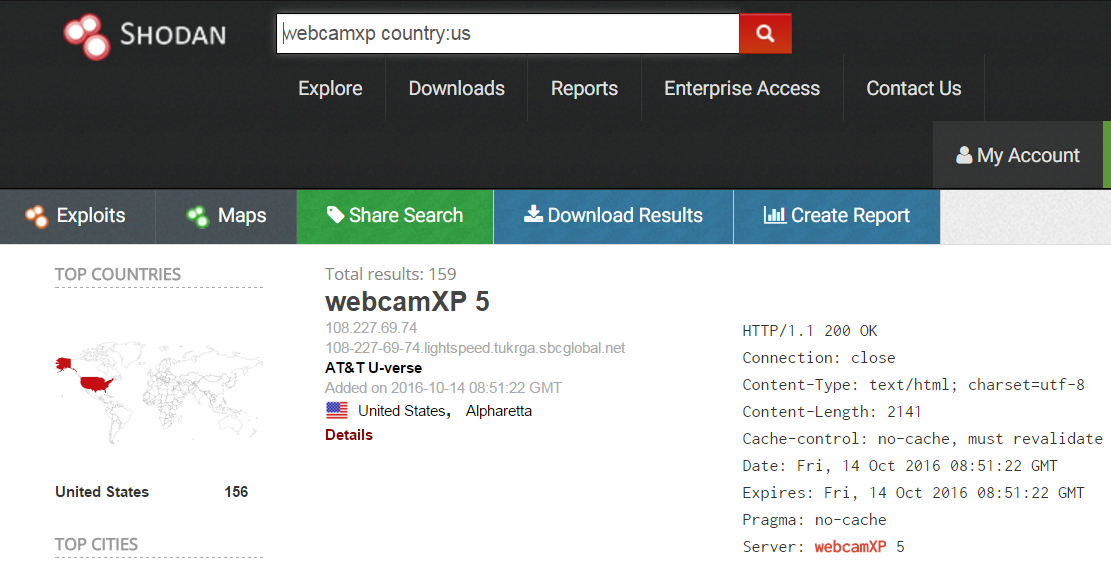
Search for Cisco routers that enable VOIP in US. VOIP uses the SIP protocol and the SIP protocol uses port 5060.



**Task 4: Task 2: Find Apache servers in the .nist.gov domain**



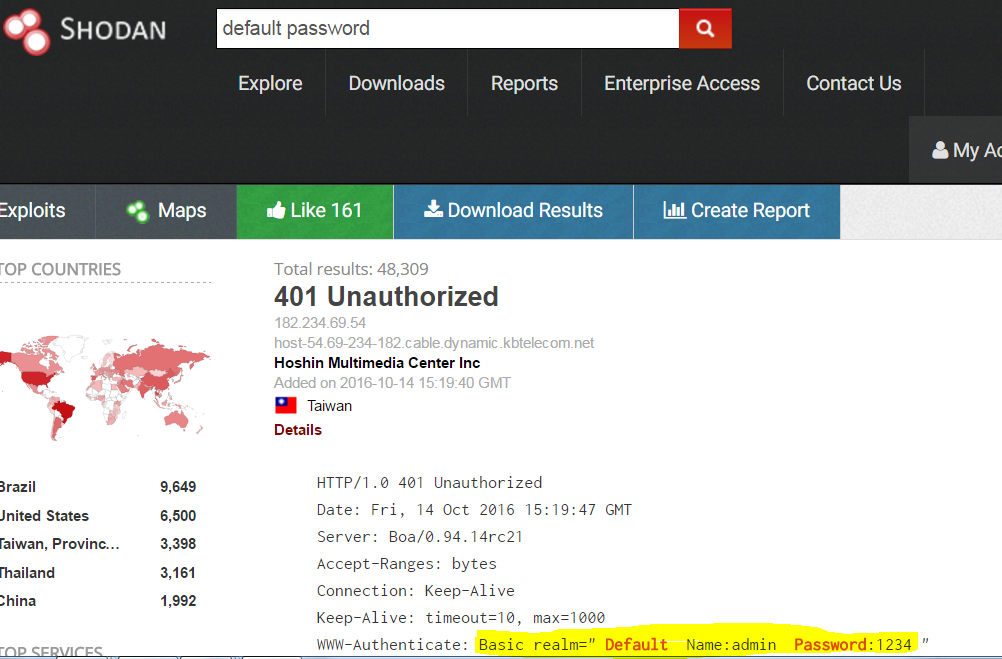
**Task 5: Search for Webcams in US**



**Default username and passwords of some of the most widely used webcams below.**

* **ACTi**: *admin/123456* or *Admin/123456*
* **Axis (traditional)**: *root/pass*,
* **Axis (new)**: requires password creation during first login
* **Cisco**: No default password, requires creation during first login
* **Grandstream**: *admin/admin*
* **IQinVision**: *root/system*
* **Mobotix**: *admin/meinsm*
* **Panasonic**: *admin/12345*
* **Samsung Electronics**: *root/root* or *admin/4321*
* **Samsung Techwin (old)**: *admin/1111111*
* **Samsung Techwin (new)**: *admin/4321*
* **Sony**: *admin/admin*
* **TRENDnet**: *admin/admin*
* **Toshiba**: *root/ikwd*
* **Vivotek**: *root/<blank>*
* **WebcamXP**: *admin/ <blank>*

**Task 6: Penetration Testing: Search for default password**



**How It Works?**

**Basic search filters:**

**city**: find devices in a particular city

**country**: find devices in a particular country

**geo**: you can pass it coordinates

**hostname**: find values that match the hostname

**net**: search based on an IP or /x CIDR

**os**: search based on operating system

**port**: find particular ports that are open

**before/after**: find results within a timeframe - Read more at: http://scl.io/F9h7hl9e#gs.EC7B5jc

Reference

* <https://www.youtube.com/watch?v=Db5TPYTgy9c>
* <https://en.wikipedia.org/wiki/Shodan_(website)>
* Daniel W. Dieterle, Basic Security Testing with Kali Linux 2 Paperback – March 24, 2016