

## Understanding Shodan

### BACKGROUND

Recently, in a ploy to attract more followers to PewDiePie's YouTube channel, some grayhat hackers unlawfully played videos on [65,000 ChromeCasts that were exposed to the web](#) (a similar [hack was perpetrated a month earlier using exposed printers](#)). The hack was executed by leveraging exposed ports that ChromeCasts and printers typically use.

[Shodan.io](#) is a search engine available through any web browser and provides a directory of computers connected to the internet (it's a powerful port scanner).

Anyone can go to Shodan and look for machines connected to the internet and apply filters (such as "webcam", "server", city names, etc.). Oftentimes, it is the case that some of these machines can be connected to (and default usernames and passwords may work).

**DO NOT ATTEMPT TO LOGIN TO A DEVICE THAT IS NOT YOURS!  
IN MANY STATES THAT IS ILLEGAL!**

There are some people that believe this is a dangerous tool--CNN, among others, [wrote a scathing article](#) about the tool. However it is a valuable tool not only for penetration testers, but also for responsible security minded cybersecurity enthusiasts.

Shodan functions by a custom port scanner (code made by the developer). Users can get a free account, but for deep dives into Shodan users can pay for an account. You can get a free account too - in fact, you'll need an account to use the filter features.

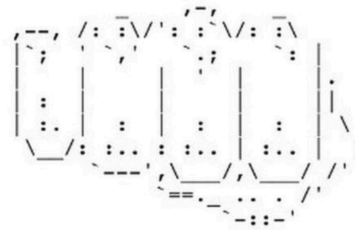
### DESCRIPTION

This lab will introduce you to Shodan and give you a primer on how to use it.

### REQUIREMENTS

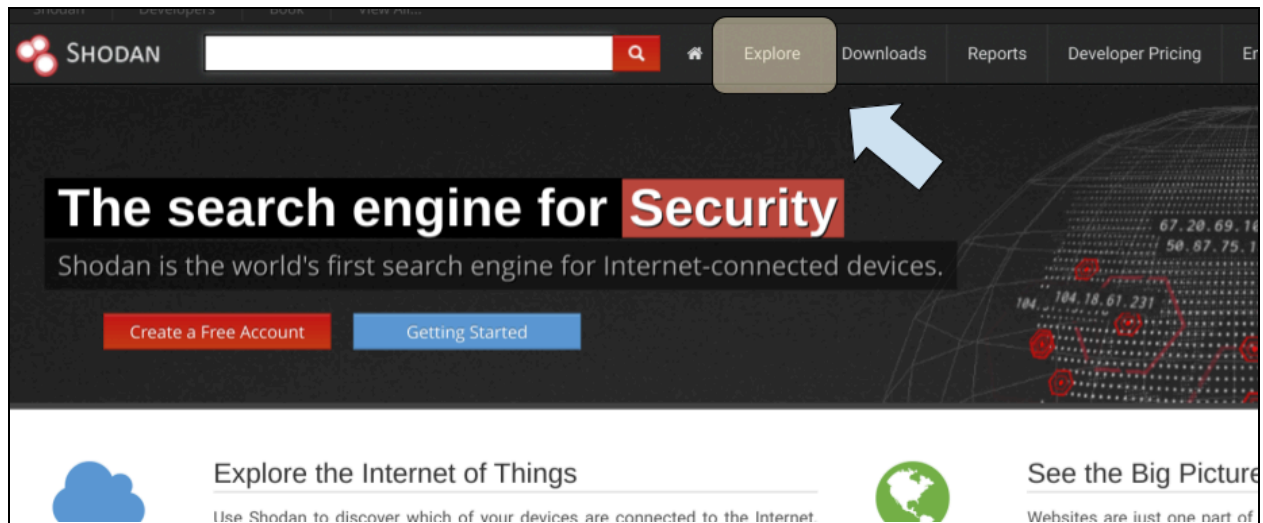
A web browser and an internet connection.

```
--- WHAT TO DO ---
1. Unsubscribe from T-Series
2. Subscribe to PewDiePie
3. Share awareness to this issue
#SavePewDiePie #PrinterHack2
4. Tell everyone you know. Seriously.
5. Fix your printer. It can be abused!
6. BROFIST!
```

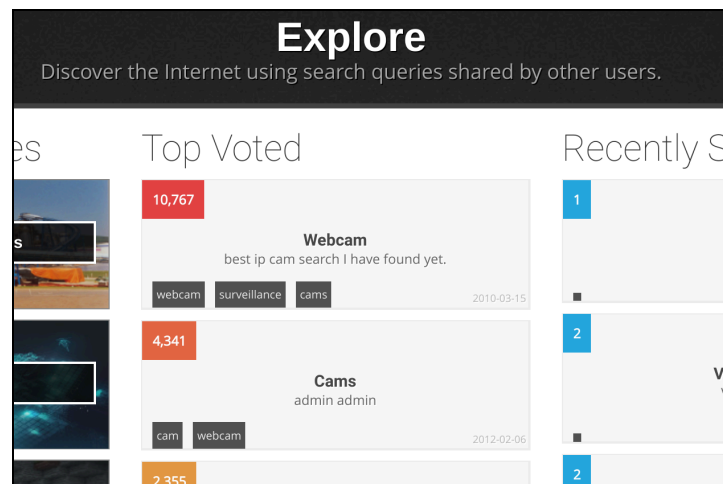


## PART I: Explore with Shodan

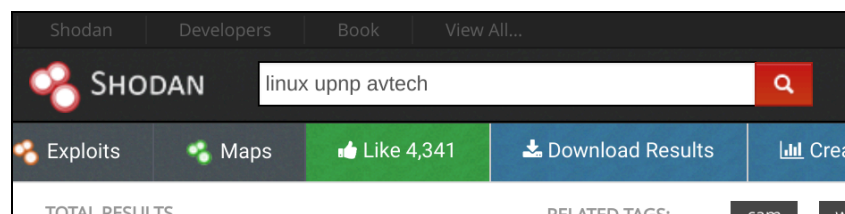
1. Go to [www.shodan.io](http://www.shodan.io) and click on the “Explore” link.



2. Click on a popular search (in my case, I clicked on “Cams”).

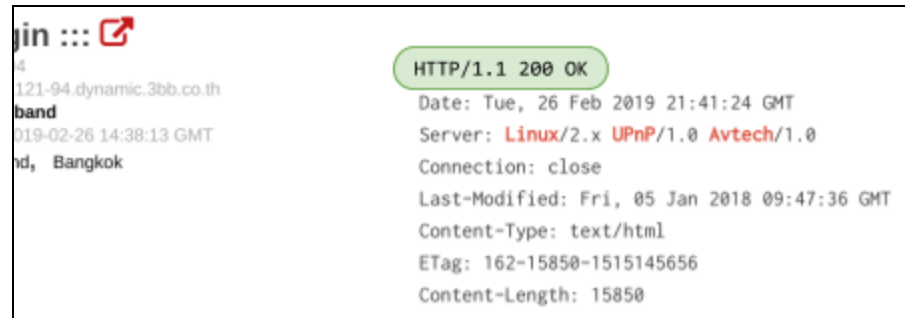


3. Look at the list of devices that are returned. Note two things:
  - a. The term that was applied in the search bar for Shodan. This is important information, as it shows the different search criteria that Shodan can use. If you intend to use Shodan often, it is worth getting a feel for the search scheme.

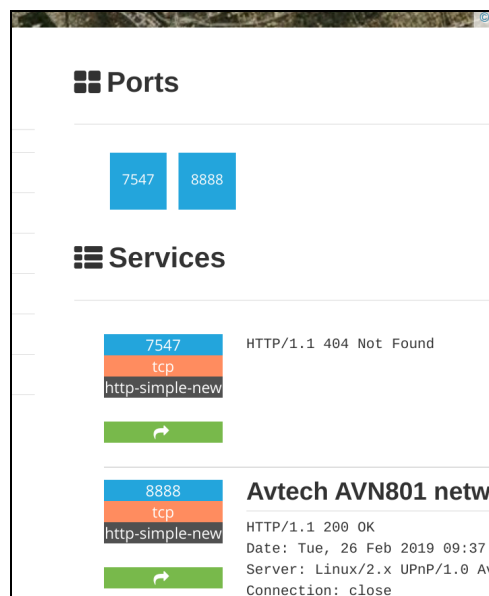


- b. The *protocol status code* (for instance, HTTP/1.1 200). Any code that is 404 or 401 is not of particular interest as they won't be accessible. However, 200 means

that the machine can be communicated with. It does *not* mean that visitors have unfettered access to the device (there may be a login screen); it just means that the machine is up, running, and ready to connect.



4. You should also gain familiarity with important ports on these machines. For example, port 80 and port 443 are reserved for serving web pages. Other ports, like 21 and 22 are reserved for connections (FTP and SSH, respectively). Ports 0-1,023 are *well known* ports and have very specific purposes. Ports 1,024-49,151 are *registered* ports, which mean they have an official use, but can be overridden. For instance, port 1,194 is registered to OpenVPN, but a user could override it if needed. The last range, 49,152-65,535 are *ephemeral* ports, which are temporary and can be used whenever needed. Look at the open ports for a machine:

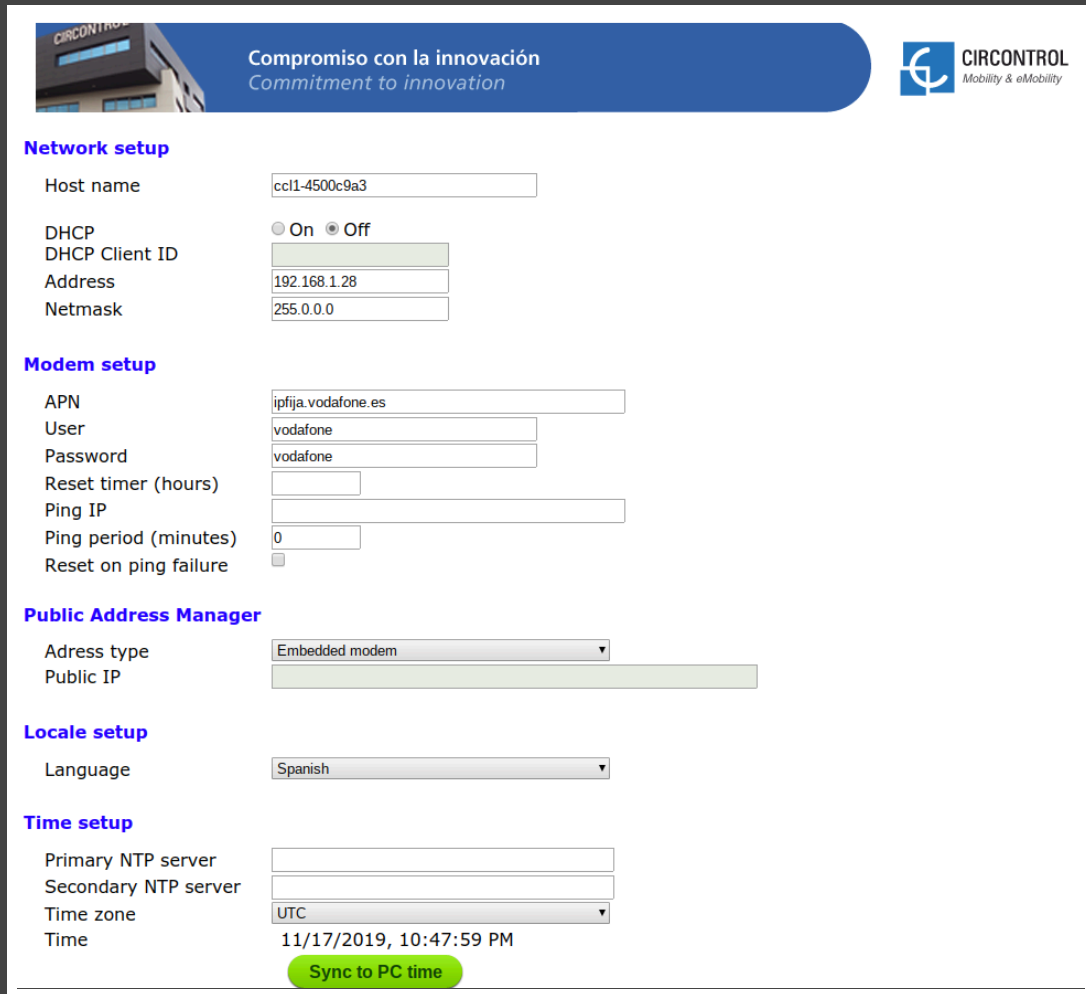


If you are curious, look up port numbers at [this Wikipedia entry](#). Note that if a green box with a white arrow is listed in your Shodan results, you can click on it to investigate more.

## PART II: Use Shodan to find some interesting things

1. Dork around in Shodan (dig a little bit deeper with the “Explore” feature if you want). Find something interesting or exciting. I happened to search for “SCADA” and check out what I found:

# EVIDENCE #1



The screenshot displays the CIRCONTROL web interface, which includes a header with the company logo and tagline "Compromiso con la innovación / Commitment to innovation". The interface is organized into several sections for configuration:

- Network setup:** Includes fields for Host name (cc11-4500c9a3), DHCP status (On/Off), DHCP Client ID, Address (192.168.1.28), and Netmask (255.0.0.0).
- Modem setup:** Includes fields for APN (ipfija.vodafone.es), User (vodafone), Password (vodafone), Reset timer (hours), Ping IP, Ping period (minutes), and a checkbox for Reset on ping failure.
- Public Address Manager:** Includes a dropdown for Address type (set to Embedded modem) and a field for Public IP.
- Locale setup:** Includes a dropdown for Language (set to Spanish).
- Time setup:** Includes fields for Primary NTP server, Secondary NTP server, a dropdown for Time zone (set to UTC), and a timestamp (11/17/2019, 10:47:59 PM). A green button labeled "Sync to PC time" is located at the bottom of this section.

INSERT A SCREENSHOT OF AN INTERESTING RESULT.

Note that you can search for specific manufacturers or models, too (like avtech, AVN901, cisco, ngnix, etc.).

## PART III: Use Shodan to Look for a Webcam that is Open

1. In the Shodan search bar, search for any webcam in Rochester.

**webcam city:"rochester"**

2. Follow a link (if any) and see if you can access a webcam. If there are no available webcams, change your search and poke around until you find one. Try your home town or a city you like. I happened to find one--the Global Cybersecurity Institute construction cam (this building is under construction at RIT).

# EVIDENCE #2



**INSERT AN IMAGE OF YOUR FINDINGS**

## CONCLUSION

One of the main hackers, TheHackerGiraffe, said they used Shodan to look for printers. Shodan is a tool that can be used for good, too.

And how to prevent this from happening to you? An [article at nakedSecurity suggests](#):

- Turn off UPnP on your router. It's been a recipe for trouble for many years, and you almost certainly neither want nor need to open it up to the outside world.
- Check what network ports are opened up on your router. If you see 8008, 8009 and 8443 open, then any Chromecasts you own are probably exposed. But any open port could spell needless danger, so close any port that you aren't 100% sure you need to keep open. You can also run a Shodan interrogation on your own public IP address. If you don't know the IP address, go to [whatismyip.com](http://whatismyip.com).

If you are interested in learning more about Shodan, you can buy the book [The Complete Guide to Shodan: Collect. Analyze. Visualize. Make Internet Intelligence Work For You.](#) by John Matherly (the creator of Shodan). It's a quick read; it's actually more like an instructional manual.

You can also read a [quick-start entry here](#).