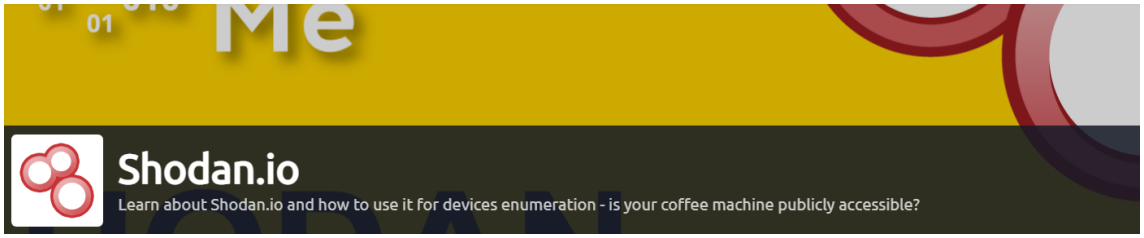
Shodan.io



La máquina es un poco antigua las respuestas pueden cambiar, pero los procesos para llegar a ellas son los mismos

Task 1 Introduction

Follow me on Twitter for more content ✨

Room created by https://twitter.com/bee_sec_san based on this blog post.

Shodan.io is a search engine for the Internet of Things.

Ever wondered how you can find publicly accessible CCTV cameras? What about finding out how many Pi-Holes are publicly accessible?

Or whether your office coffee machine is on the internet?

Shodan.io is the answer!

Shodan scans the whole internet and indexes the services run on each IP address.

Note: if you are following along, you'll need a premium Shodan account.

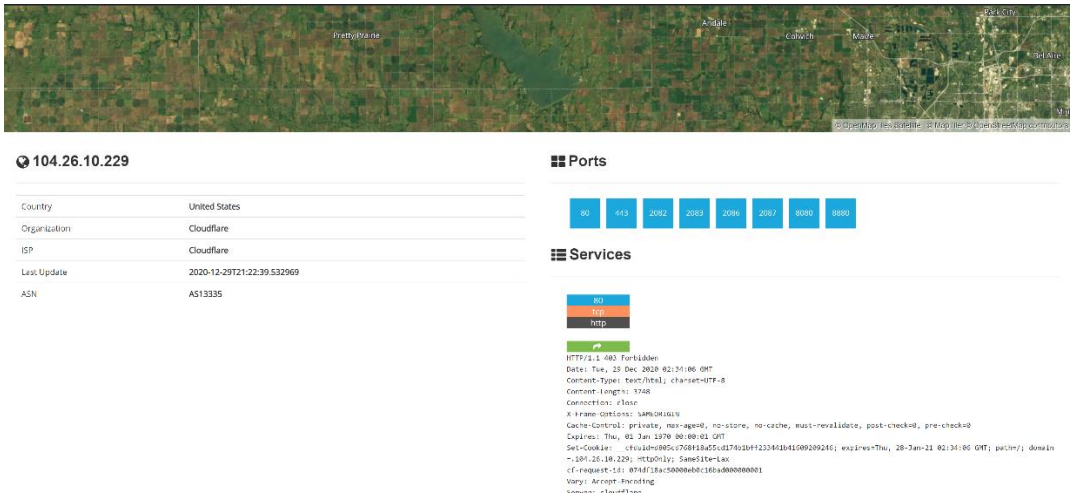
Finding services

Let's say we are performing a pentest on a company, and we want to find out what services one of their servers run.

We need to grab their IP address. We can do this using ping.

We can ping tryhackme.com and the ping response will tell us their IP address.

Then once we do this, we put the IP address into Shodan to get:



We can see that TryHackMe runs on Cloudflare in the United States and they have many ports open.

Cloudflare acts as a proxy between TryHackMe and their real servers. If we were pentesting a large company, this isn't helpful. We need some way to get their IP addresses.

We can do this using Autonomous System Numbers.

Autonomous System Numbers

An autonomous system number (ASN) is a global identifier of a range of IP addresses. If you are an enormous company like Google you will likely have your own ASN for all of the IP addresses you own.

We can put the IP address into an ASN lookup tool such as https://www.ultratools.com/tools/asnInfo ,

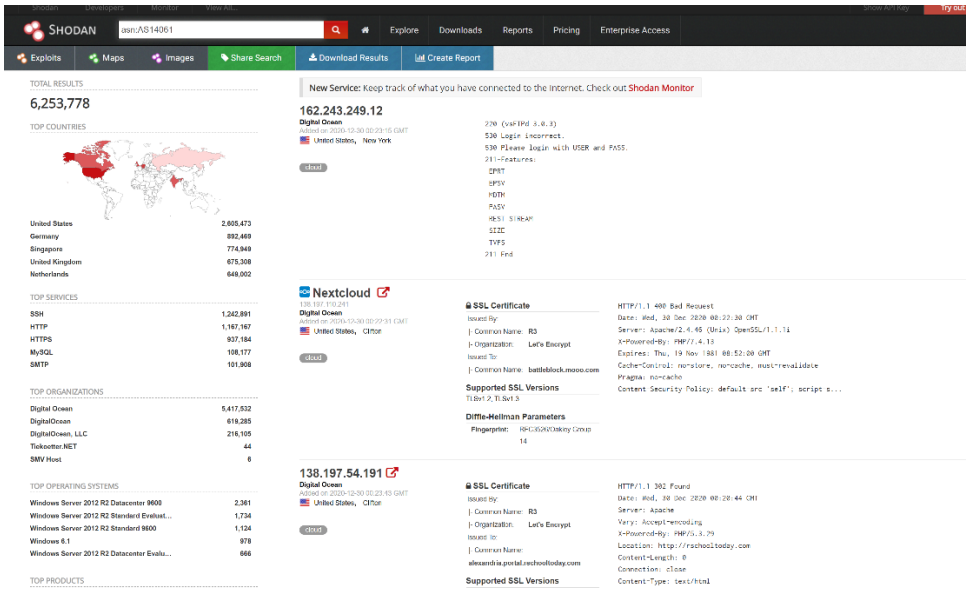
Which tells us they have the ASN AS14061.

Tryhackme isn't a mega large corporation, so they don't own their own ASN. When we google AS14061 we can see it is a DigitalOcean ASN number.

On Shodan.io,we can search using the ASN filter. The filter is **ASN:[number]** where number is the number we got from earlier, which is AS14061.

Doing this, we can see a whole range 6.2 million websites, in fact) that are on this one single ASN!

https://www.shodan.io/search?query=asn%3AAS14061



Knowing the ASN is helpful, because we can search Shodan for things such as coffee makers or vulnerable computers within our ASN, which we know (if we are a large company) is on our network.

Getting started

Time to dig in! If you get stuck, look at the previous task for some help! :)

Banners

To get the most out of Shodan, it's important to understand the search query syntax.

Devices run services, and Shodan stores information about them. The information is stored in a *banner*. It's the most fundamental part of Shodan.

An example banner looks like:


```
{
                "data": "Moxa Nport Device",
                "Status": "Authentication disabled",
                "Name": "NP5232I_4728",
                "MAC": "00:90:e8:47:10:2d",
                "ip_str": "46.252.132.235",
                "port": 4800,
                "org": "Starhub Mobile",
                "location": {
                                "country_code": "SG"
                }
 }
```

We're looking at the output of a single port, which includes information about the IP and authentication details.

You don't really see this outside of the API, so we won't delve into it.

Answer the questions below

Go to Shodan.io

Task 2 Filters

Filters

On the Shodan.io homepage, we can click on “explore” to view the most up voted search queries. The most popular one is webcams.

https://www.shodan.io/explore

Note: this is a grey area. It is legal to view a publicly accessible webcam, it is illegal to try to break into a password protected one. Use your brain and research the laws of your country!

One of the other most up voted searches is a search for MYSQL databases.

https://www.shodan.io/search?query=product%3AMySQL

If we look at the search, we can see it is another filter.

product:MySQL

Knowing this, we can actually combine 2 searches into 1.

On TryHackMe’s ASN, let’s try to find some MYSQL servers.

We use this search query

asn:AS14061 product:MySQL

And ta-da! We have MYSQL servers on the TryHackMe ASN (which is really the DigitalOcean ASN).

https://www.shodan.io/search?query=asn%3AAS14061+product%3AMySQL

Shodan has many powerful filters. My favourite one is the vuln filter, which let’s us search for IP addresses vulnerable to an exploit.

Let’s say we want to find IP addresses vulnerable to Eternal Blue:

vuln:ms17-010

However, this is only available for academic or business users, to prevent bad actors from abusing this!

City Country Geo (coordinates) Hostname net (based on IP / CIDR) os (find operating systems) port before/after (timeframes)

API

Shodan.io has an API! It requires an account, so I won't talk about it here.

If you want to explore the Shodan API, I've written a blog post about finding Pi-Holes with it here:

https://github.com/beesecurity/How-I-Hacked-Your-Pi-Hole/blob/master/README.md

The API lets us programmatically search Shodan and receive a list of IP addresses in return. If we are a company, we can write a script to check over our IP addresses to see if any of them are vulnerable.

PS: You can automatically filter on Shodan by clicking the things in the left hand side bar!

Answer the questions below

How do we find Eternal Blue exploits on Shodan?

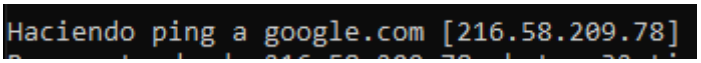
Task 3 Google & Filtering

Learning to filter with Google. **Helpful hint: pay close attention to what the question is asking you!**

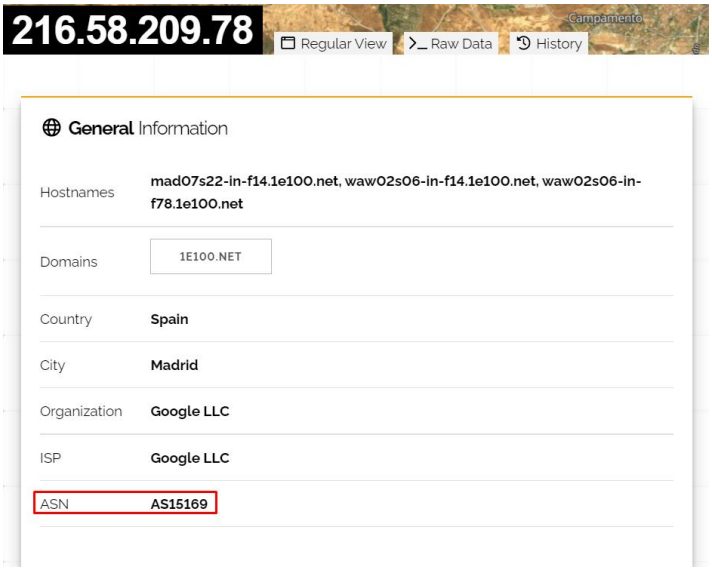
Answer the questions below

What is the top operating system for MYSQL servers in Google's ASN?

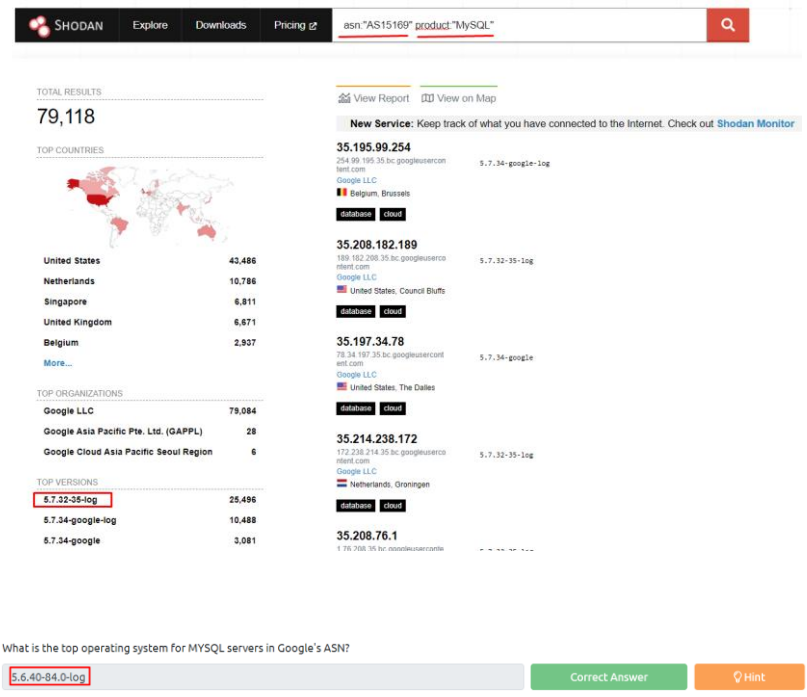
Para conocer la IP de Google hacemos un **ping** y obtendremos la dirección



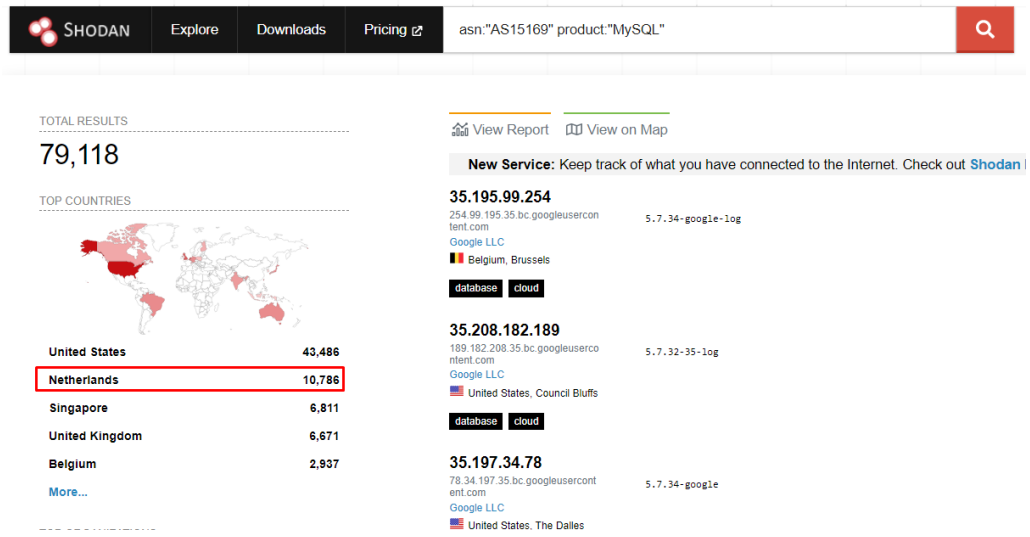
Introducimos la IP en el buscador de Shodan y nos saldrá un apartado con la información del ASN



Usaremos los dorks **asn** y **product**



What is the 2nd most popular country for MYSQL servers in Google's ASN?



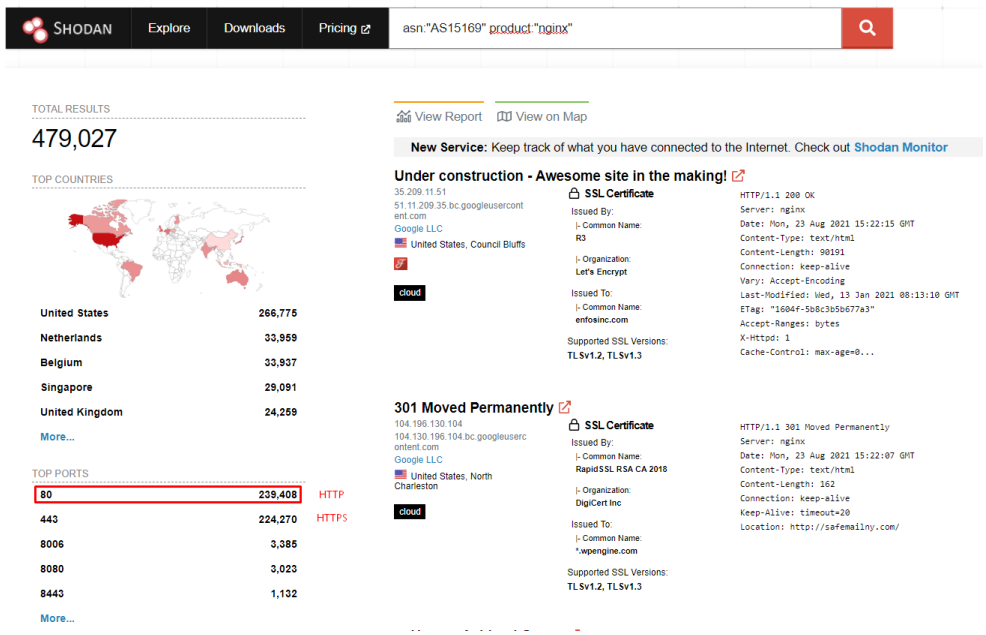
What is the 2nd most popular country for MYSQL servers in Google's ASN?

Netherlands

Correct Answer

Hint

Under Google's ASN, which is more popular for nginx, Hypertext Transfer Protocol or Hypertext Transfer Protocol with SSL?



Under Google's ASN, which is more popular for nginx, Hypertext Transfer Protocol or Hypertext Transfer Protocol with SSL?

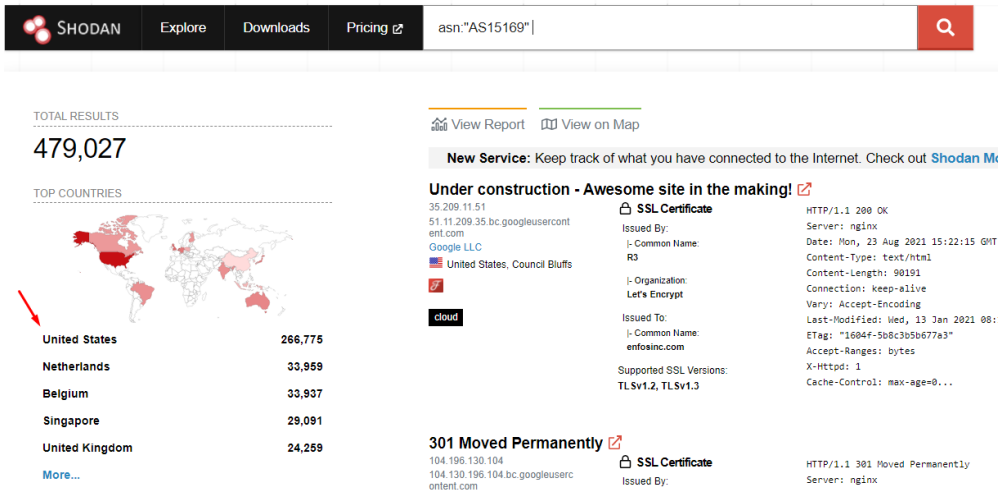
Hypertext Transfer Protocol

Correct Answer

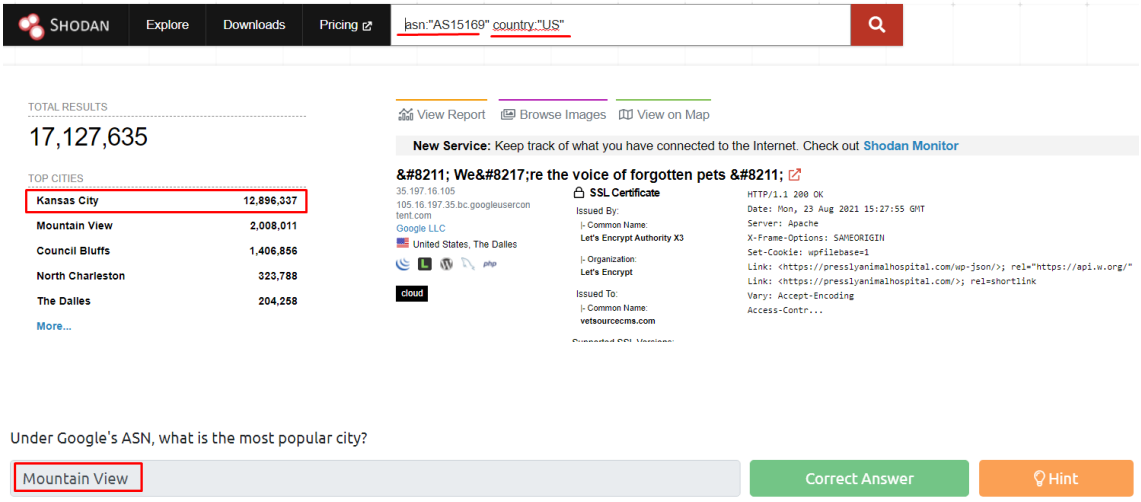
Hint

Under Google's ASN, what is the most popular city?

Hacemos clic sobre Estados Unidos ya que es el estado más popular



Y podemos observar que la ciudad más popular es Kansas City

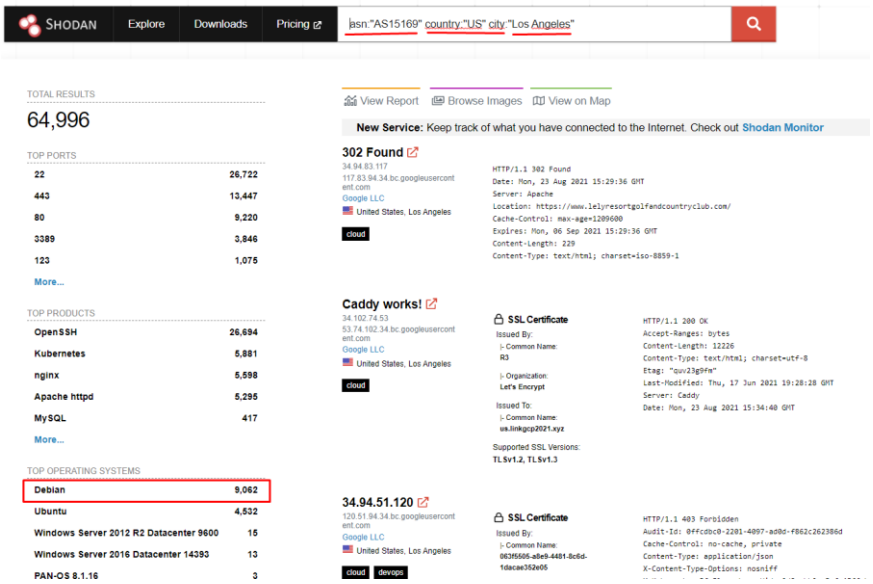


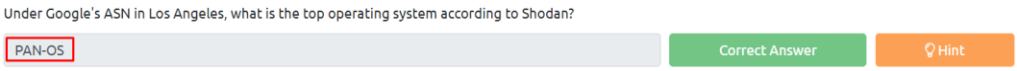
Under Google's ASN, what is the most popular city?

Mountain View | Correct Answer | Hint

Under Google's ASN in Los Angeles, what is the top operating system according to Shodan?

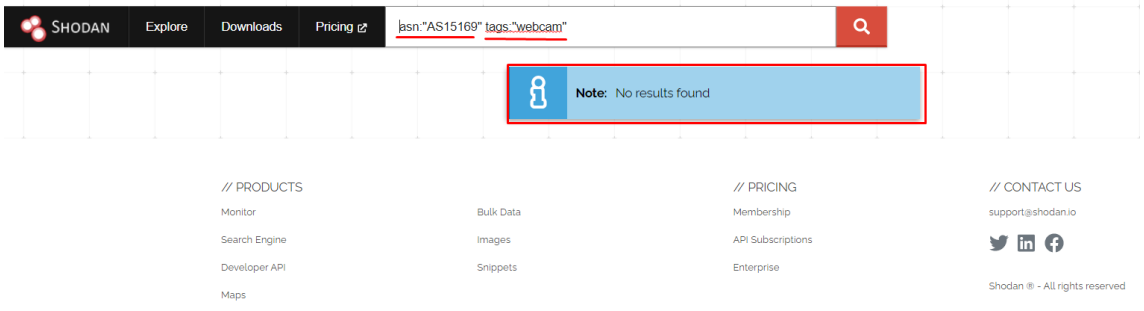
Para la siguiente pregunta solo tendremos que añadir el dork **city** y nos aparecerá que el Sistema Operativo más usado es Debian



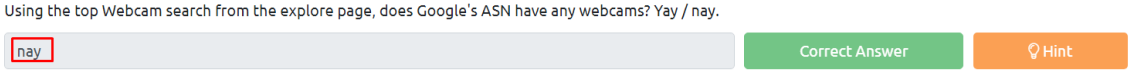


Using the top Webcam search from the explore page, does Google's ASN have any webcams? Yay / nay.

Para ver el top web cam debemos usar los dorks **asn** y **tags:"webcam"**



En este caso no hay resultados



Task 4 Shodan Monitor

Shodan Monitor is an application for monitoring your devices in your own network. In their words:

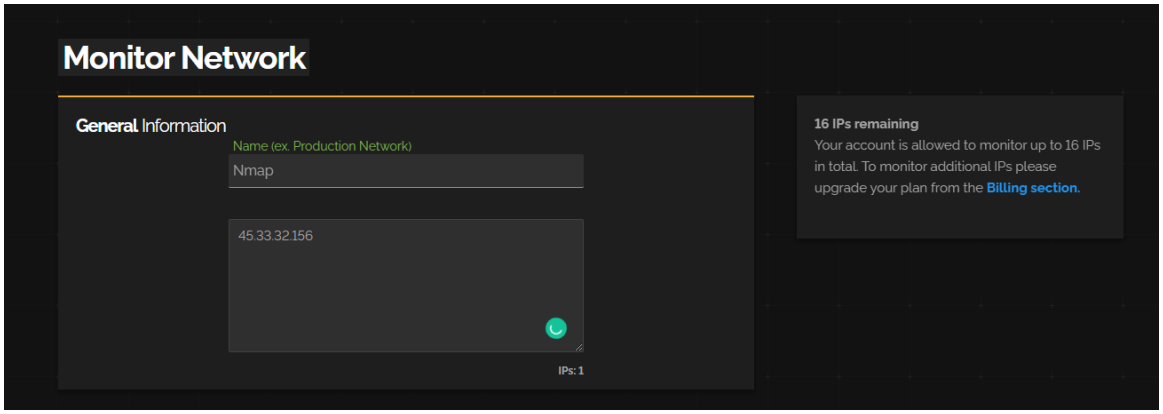
Keep track of the devices that you have exposed to the Internet. Setup notifications, launch scans and gain complete visibility into what you have connected.

Previously we had to do this using their API, but now we have this fancy application.

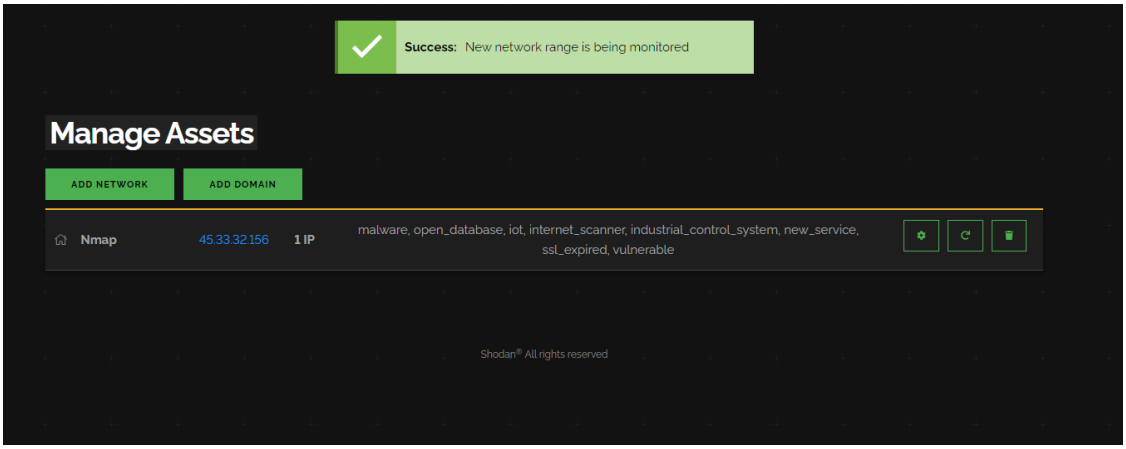
Access the dashboard via this link:

https://monitor.shodan.io/dashboard

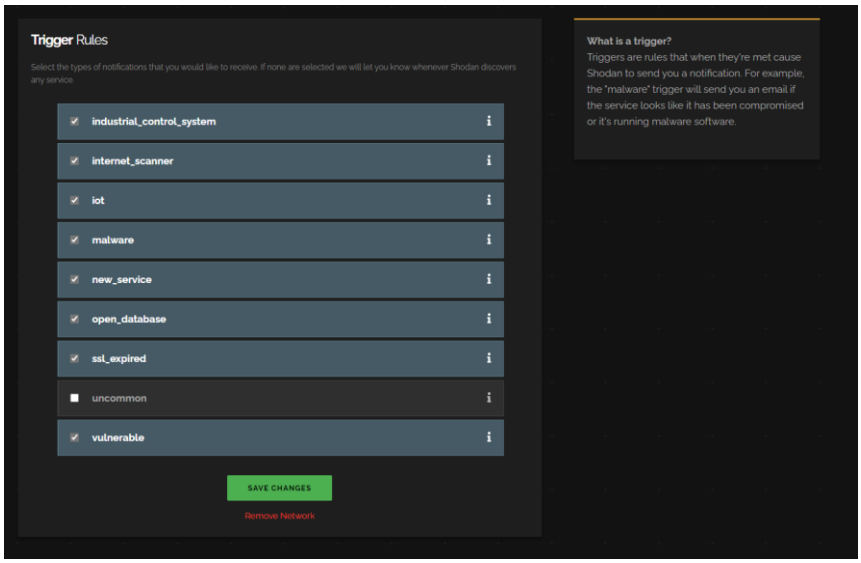
You'll see it's asking for an IP range.



Once we add a network, we can see it in our dashboard.

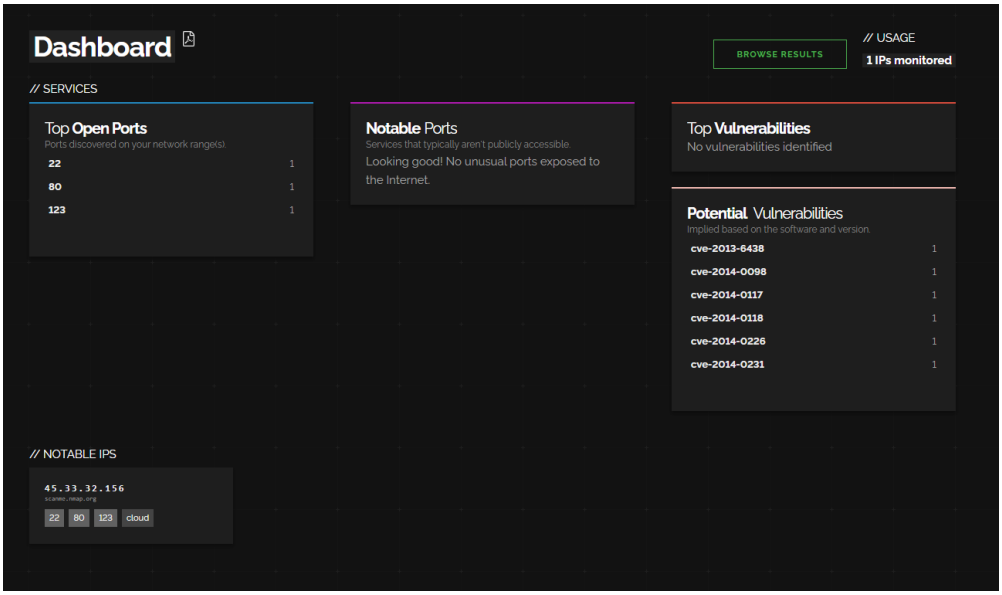


If we click on the settings cog, we can see that we have a range of “scans” Shodan performs against our network.



Anytime Shodan detects a security vulnrability in one of these categories, it will email us.

If we go to the dashboard again we can see it lays some things out for us.



Most notably:

- Top Open Ports (most common)
- Top Vulnerabilities (stuff we need to deal with right away)
- Notable Ports (unusual ports that are open)
- Potential Vulenrabilites
- Notable IPs (things we should investigate in more depth).

The interesting part is that you can actually monitor other peoples networks using this. For bug bounties you can save a list of IPs and Shodan will email you if it finds any problems.

Note: This is a premium product, but you can often get $1 Shodan accounts on their Black Friday deals.

Answer the questions below

What URL takes you to Shodan Monitor?

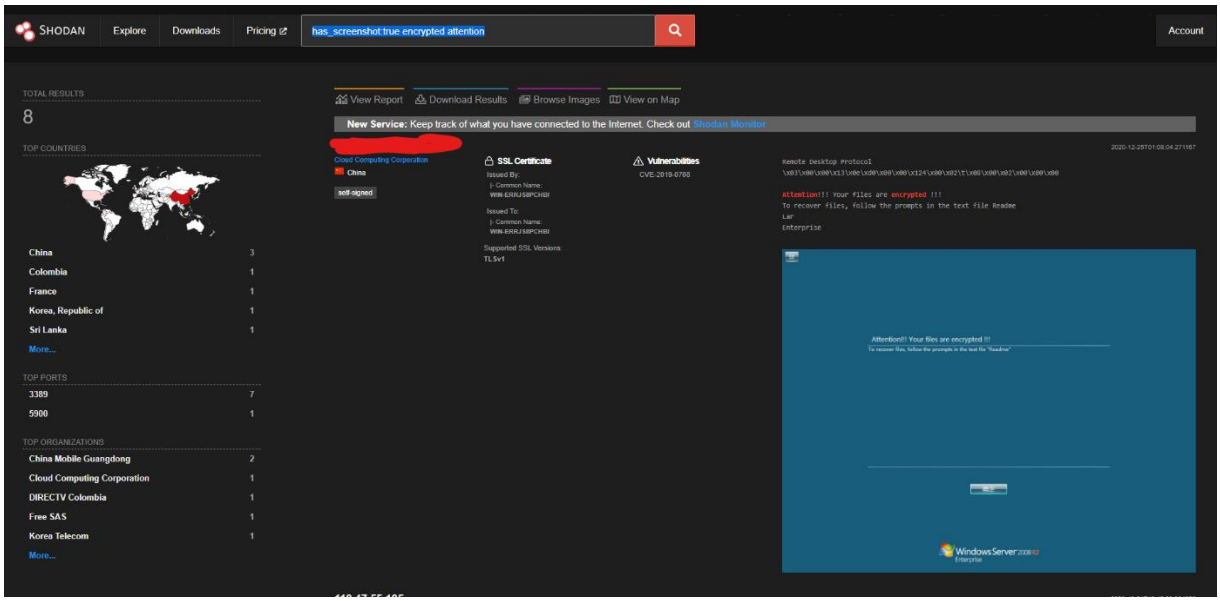
Task 5 Shodan Dorking

Shodan has some lovely webpages with Dorks that allow us to find things. Their search example webpages feature some.

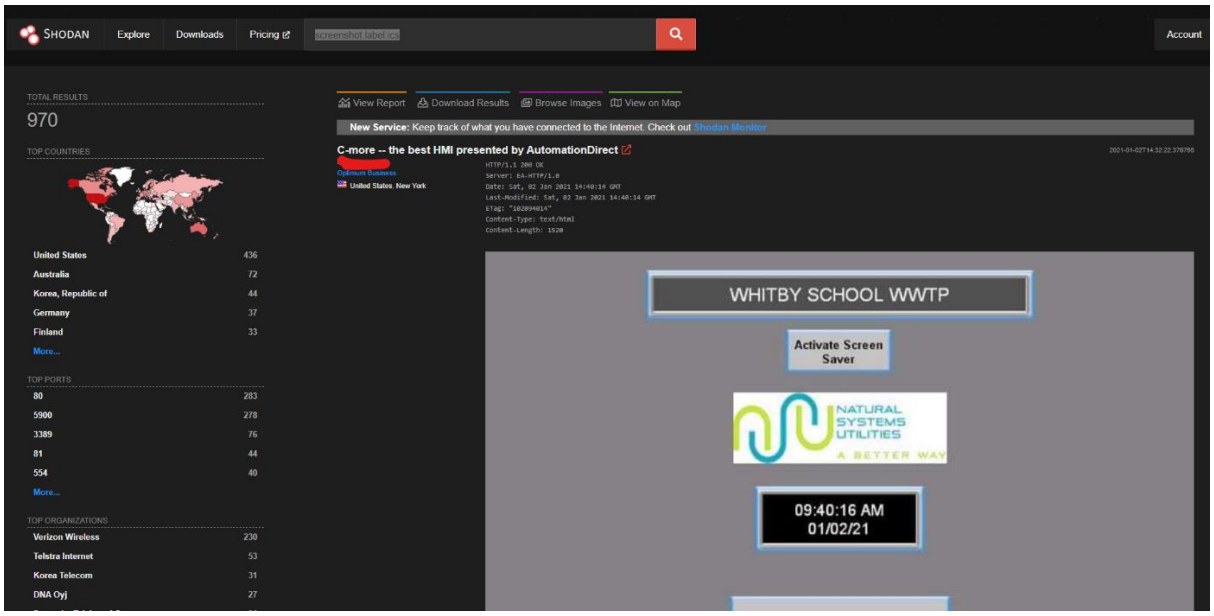
Some fun ones include:

has_screenshot:true encrypted attention

Which uses optical character recognition and remote desktop to find machines compromised by ransomware on the internet.



screenshot.label:ics



vuln:CVE-2014-0160 Internet connected machines vulenrable to heartbleed. Note: CVE search is only allowed to academic or business subscribers.

Solar Winds Supply Chain Attack by using Favicons:

http.favicon.hash:-1776962843

You can find more Shodan Dorks on GitHub.

Answer the questions below

What dork lets us find PCs infected by Ransomware?

El dork que usaríamos para encontrar PCs infectadeos con ransomware sería

has_screenshot:true encrypted attention

Task 6 Shodan Extension

Shodan Extension

Shodan also has an extension.

https://chrome.google.com/webstore/detail/shodan/jjalcfnidlmpjhdfepjhjbhnhkbgleap

When installed, you can click on it and it'll tell you the IP address of the webserver running, what ports are open, where it's based and if it has any security issues.

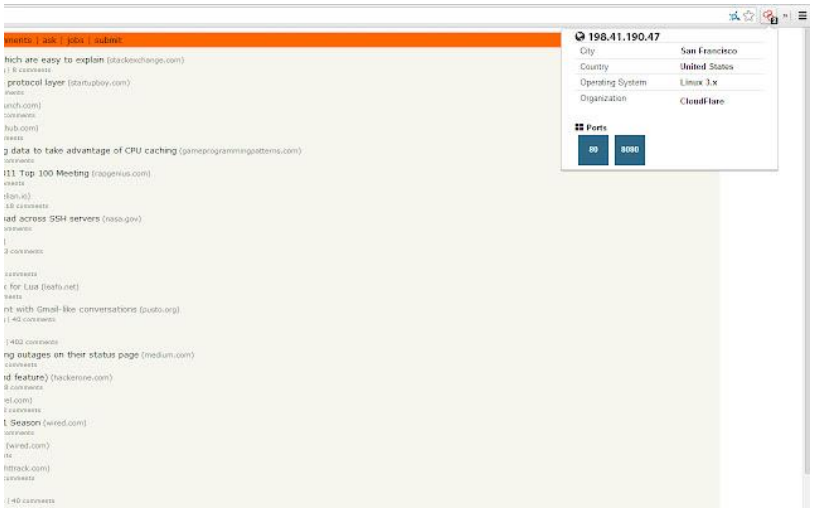
I imagine this is a good extension for any people interested in bug bounties, being quickly able to tell if a system looks vulnerable or not based on the Shodan output.

Shodan also has an extension.

https://chrome.google.com/webstore/detail/shodan/jjalcfnidlmpjhdfepjhjbhnhkbgleap

When installed, you can click on it and it'll tell you the IP address of the webserver running, what ports are open, where it's based and if it has any security issues.

I imagine this is a good extension for any people interested in bug bounties, being quickly able to tell if a system looks vulnerable or not based on the Shodan output.



PS: That's the official image for the extension. Sorry it's so blurry!

Answer the questions below

This will be nice for bug bounties!

This will be nice for bug bounties!

No answer needed

Correct Answer

Task 7 Exploring the API & Conclusion

Shodan.io has an API! It requires an account, so I won't talk about it here.

If you want to explore the Shodan API, I've written a blog post about finding Pi-Holes with it here:

https://github.com/beesecurity/How-I-Hacked-Your-Pi-Hole/blob/master/README.md

The API lets us programmatically search Shodan and receive a list of IP addresses in return. If we are a company, we can write a script to check over our IP addresses to see if any of them are vulnerable.

PS: You can automatically filter on Shodan by clicking the things in the left hand side bar!

Answer the questions below

Read the blog post above!