Shodan.io

Shodan.io

Learn about Shodan.io and how to use it for devices enumeration - is your coffee machine publicly accessible?

[Task 1] Introduction

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!

What is the TryHackMe.com IP address?

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

```
Pinging tryhackme.com [142.93.194.248] with 32 bytes of data:
```

What is their autonomous system number?
An autonomous system number (ASN) is a global identifier of a range of IP addresses. If you are a very, very large 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 (2.8 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.

IMPORTANT: The answers in this room change all the time, due to the nature of Shodan and their scanning services. If you get an incorrect answer, try the 2nd most likely answer or wait a day.
More errors? Tag me @Bee on Discord in channel #bugs.

#1
Go to Shodan.io

No answer needed

[Task 2] Getting Started

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

click me

What is Google's ASN number?

AS15169

click me

When was it allocated? Give the year only.

2000

click me

Where are most of the machines on this ASN number, physically in the world?

United States

click me

What is Google's top service across all their devices on this ASN?

SSH

click me

What SSH product does Google use?

openssh

#6

What is Google's most used Google product, according to this search? Ignore the word "Google" in front of it.

cloud

[Task 3] 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 script kiddies from abusing this!

Here are some nice filters we can use on Shodan:

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

#1
Wow, that's nifty!

No answer needed

[Task 4] Google & Filtering

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

#1
What is the top operating system for MYSQL servers in Google's ASN?

windows server 2008

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

singapore

#3
Under Google's ASN, which is more popular for nginx, Hypertext Transfer Protocol or Hypertext Transfer Protocol(s)?

Hypertext Transfer Protocol

#4
Under Google's ASN, what is the most popular city?

mountain view

#5
Under Google's ASN in Los Angeles, what is the top operating system according to Shodan?

linux 3.x

#6
Using the top Webcam search from the explore page, does Google's ASN have any webcams? Yay / nay

nay

[Task 5] 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!

#1

Read the blog post above!

No answer needed