shodan.io

getting tryhackme.com's 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

https://www.ultratools.com/tools/asnInfo

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!

> 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).

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)
