Shodan Student Workout Instructions

Introduction:

For this workout you will be using the Shodan API to view data on unprotected devices connected to the internet.

Shodan is a popular tool used that scans the internet for devices that aren't properly or securely configured and returns the information based upon the header response. While all of these devices could be found with a regular search on Google, a user might have to search through thousands of results to find one instance whereas Shodan makes this access easily accessible. Some security professionals use Shodan to help discover any vulnerable devices or servers that can be used to provide access to the client they are performing a security analysis for.

> When using Shodan, it is important to know that unless you have *explicit written consent from the owner of the device,* it is considered illegal *to act* upon any information found.

Your Mission

To get started, in a new tab, go to the URL provided on your Cyber Gym Student landing page

- **Task 1: Search for Minecraft servers in Dallas. What is the organization that owns the server of the 2nd result?**

  Task 2: Search for companies that could be running pfSense in the United States. From the first result, what is the IP for the server? [IP format: 35.1.10.34]
  - What is pfSense?
- **Task 3: How many vulnerable Apache servers are there in Phoenix?**
- **Task 4: How many servers are still vulnerable to Heartbleed? [*Hint: What is Heartbleed?]***
- **Task 5: Build your own query and submit a screenshot of your most interesting find!**

For even more information, you can dig through the raw data by clicking on the *vie w raw data* button. This could be anything from more details on CVE's found on the page to HTML responses from the server to Shodan. Dig around in the raw data. See what else you can learn!

Do not go to any URL’s or IP addresses that were found from the Shodan results as some of these pages could contain malware.