Shodan Workout Instructions

The Big Idea

The Internet is a large, globally distributed network that is divided into layers, governed by protocols, and connects a wide variety of devices.

Through the Shodan application, you will see a current view of the Internet as network protocols providing services across the globe. The machine-readable network, transport, and application protocol layers connect highly diverse devices.

The Internet provides a large attack surface, which offers efficiencies or economies of scale for adversaries.

As you explore these protocols, you will notice how much information is available over the Internet for an adversary and identify the large number of devices currently exposed to cybersecurity vulnerabilities.

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

Shodan is a popular tool that scans the internet for devices that aren't properly or securely configured and returns the information based on 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, go to the URL provided on your Cyber Gym Student landing page in a new tab.

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

  Task 2: Search for devices that still use default passwords in the United States. From the first result, what is the IP for the server? [IP format: 35.1.10.34]

- **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 query and submit a screenshot of your most exciting find!**

You can dig through the raw data by clicking on the view raw data button for more information. This could be anything from more details on CVEs 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.