Network Security Practices
CY5150
Task 6

Submitted By:
Sonam Ghatode(001305171)

Table of Contents

Introduction:

In this task, we were asked to do two tasks, finding all IP addresses in Northeastern University IP range that has Cisco in banner and search for the vulnerable devices that runs on nginx servers with vulnerability CVE-2017-7529. To do these tasks, we had to use either Shodan or Censys. I used them both to get my hands on them and see which tool is easier to use.

Shodan:

Shodan is a search engine like **Google** but the only difference in both is that Shodan allows the user to search everything on the internet, be it web camera or a printer or something like refrigerator. It can be a very useful tool for reconnaissance since it can list all the devices running on a vulnerable version of server of service in an IP range, making it extremely useful for hackers to decide on the targets in an environment.

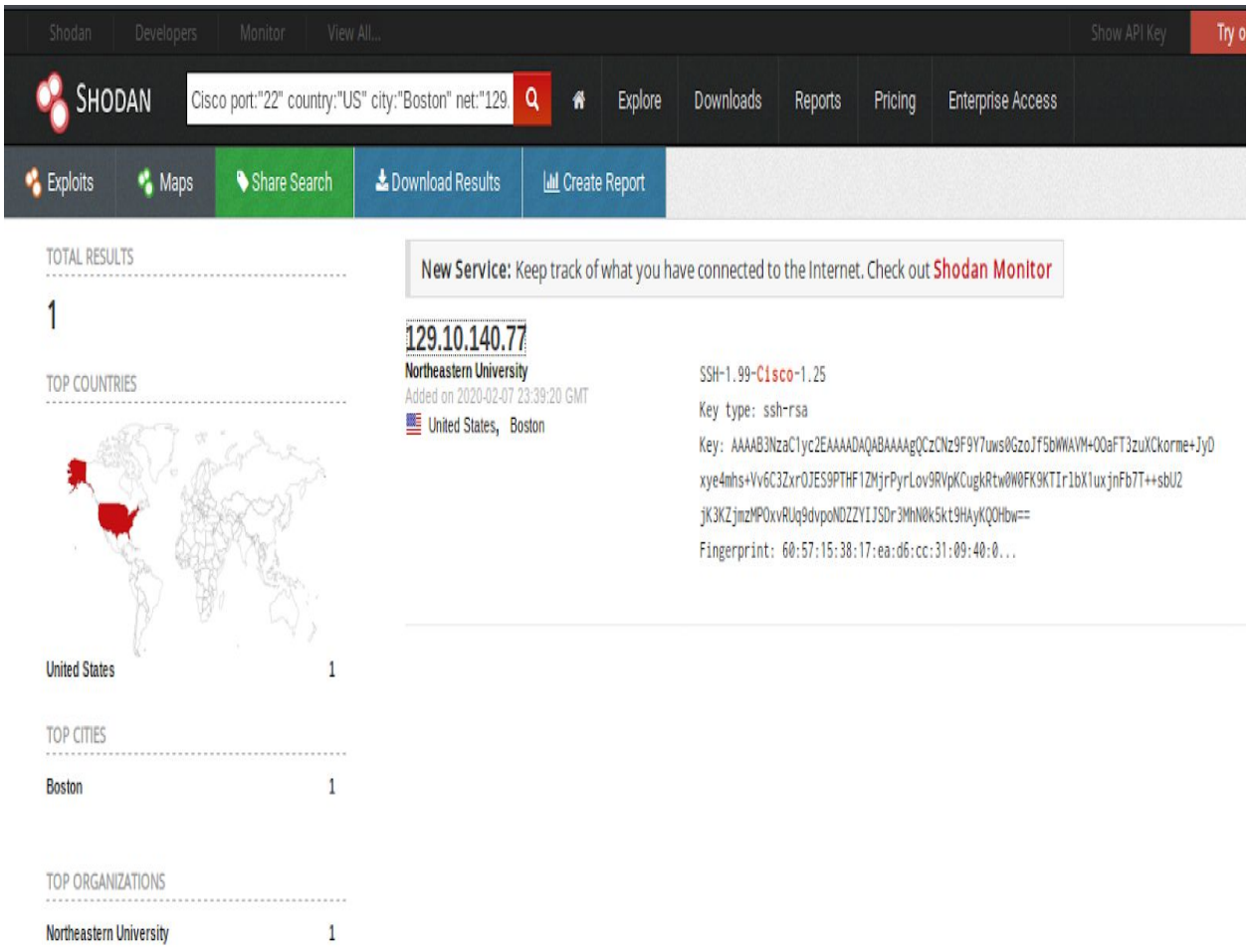
Censys:

Censys is a search engine similar to **Shodan** which searches for all types of devices exposed on the internet. It is a free search engine that was originally released in October by researchers from the University of Michigan and is currently powered by Google. It scans the internet searching for devices and returns aggregate reports on how resources (i.e. devices, websites, and certificates) are configured and deployed.

Part 1:

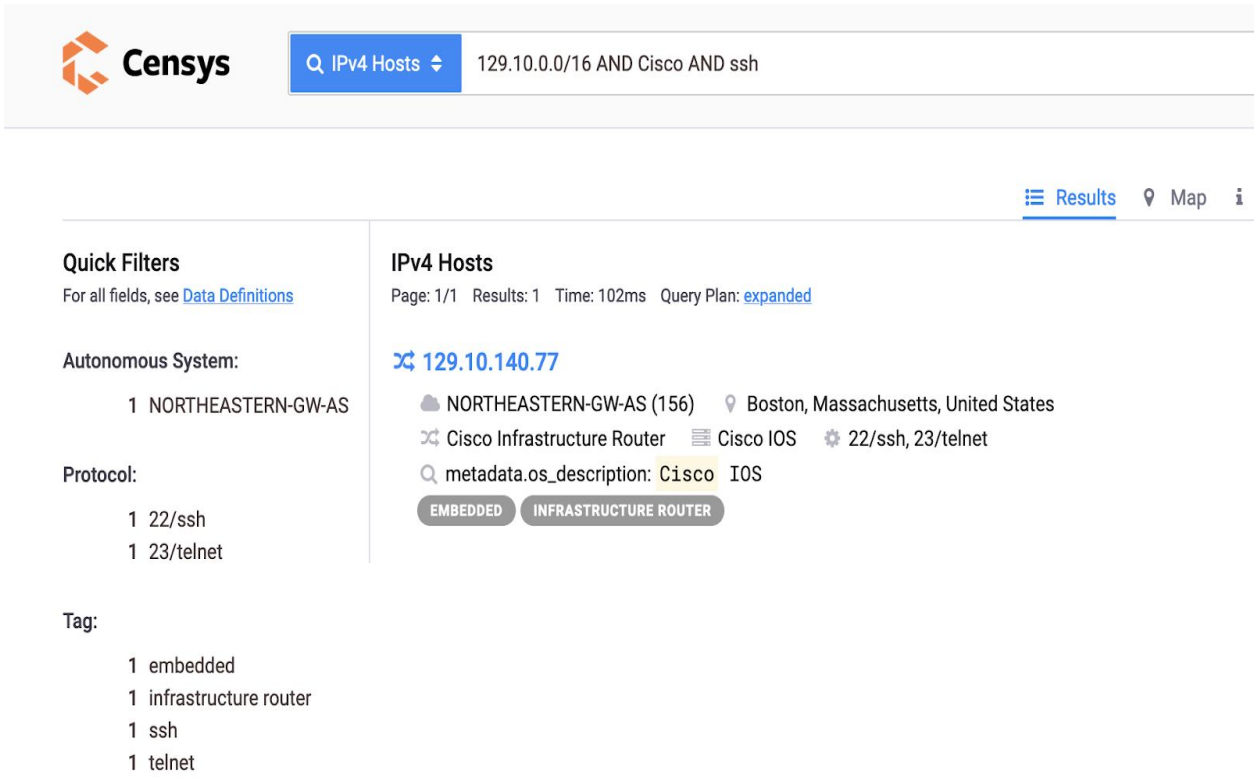
Shodan:

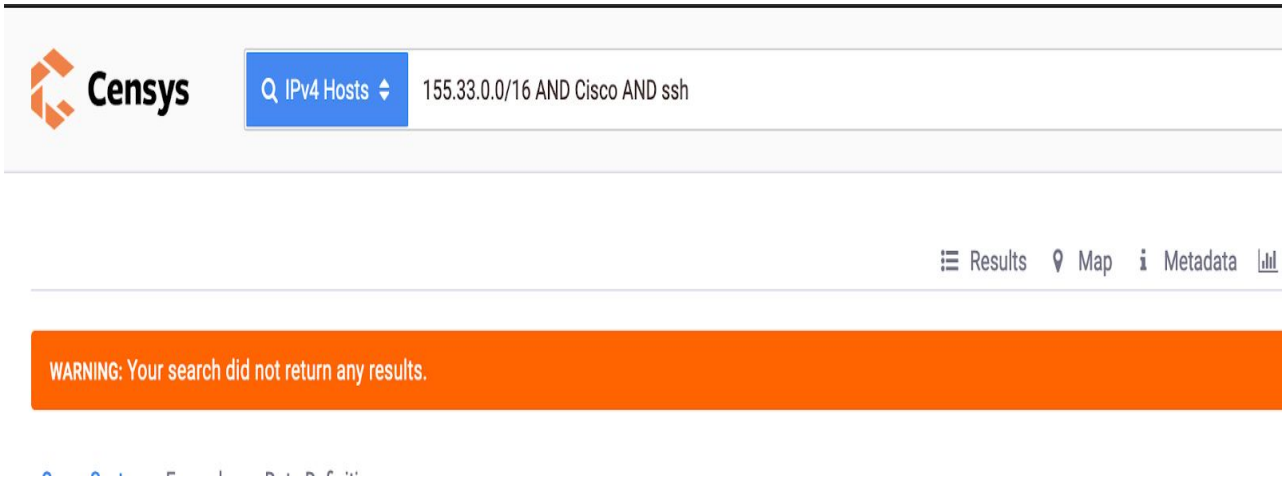
In this part, all the IP addresses that are running on SSH server and had Cisco in banner in the IP range of Northeastern University are to be searched. I used the queries ***Cisco port:"22" country:"US" city:"Boston" net:"129.10.0.0/16" and Cisco port:"22" country:"US" city:"Boston" net:"155.33.0.0/16",*** which gave just one IP address that is running on SSH service and has Cisco in banner: 129.10.140.77:



Censys:

To search all the IP addresses that are running on SSH server and had Cisco in banner in the IP range of Northeastern University using Censys, I used the queries ***129.10.0.0/16 AND Cisco AND ssh*** **and** ***155.33.0.0/16 AND Cisco AND ssh,*** which again gave just one IP address that is running on SSH service and has Cisco in banner: 129.10.140.77:


Censys
IPv4 Hosts
129.10.0.0/16 AND Cisco AND ssh
Results
Map
Quick Filters
For all fields, see Data Definitions
Autonomous System:
1 NORTHEASTERN-GW-AS
Protocol:
1 22/ssh
1 23/telnet
Tag:
1 embedded
1 infrastructure router
1 ssh
1 telnet
IPv4 Hosts
Page: 1/1 Results: 1 Time: 102ms Query Plan: expanded
129.10.140.77
NORTHEASTERN-GW-AS (156)
Boston, Massachusetts, United States
Cisco Infrastructure Router
Cisco IOS
22/ssh, 23/telnet
metadata.os_description: Cisco IOS
EMBEDDED
INFRASTRUCTURE ROUTER


Censys
IPv4 Hosts
155.33.0.0/16 AND Cisco AND ssh
Results
Map
Metadata
WARNING: Your search did not return any results.

Part 2:

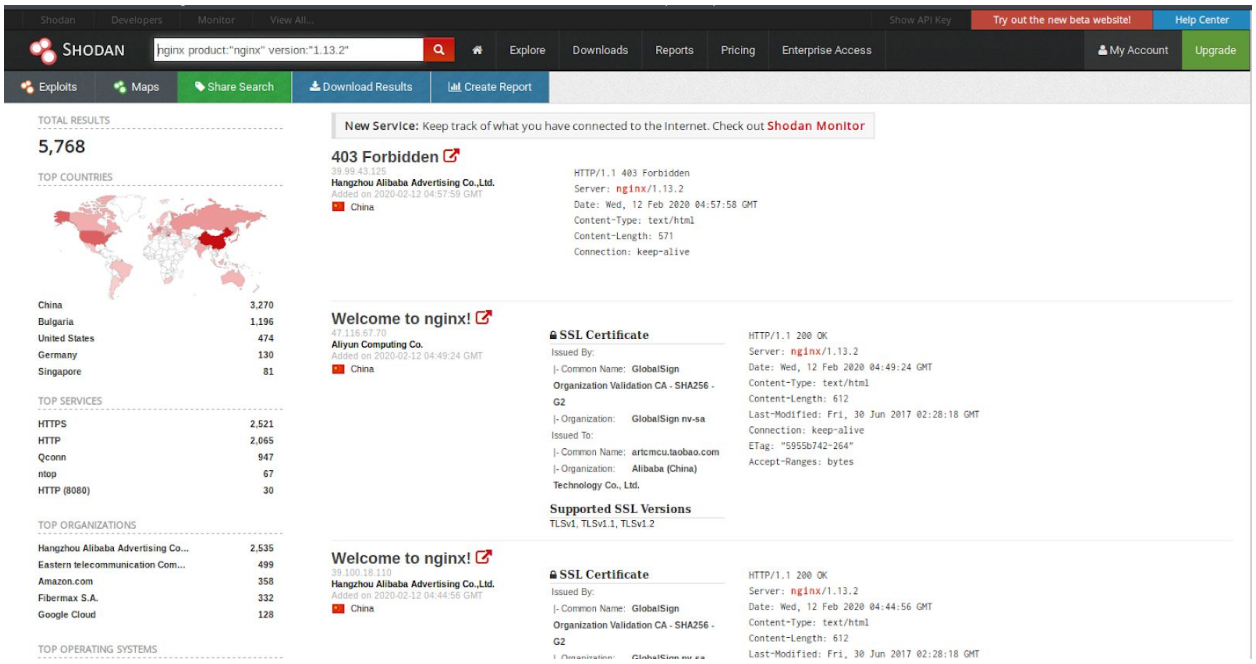
CVE-2017-7529:

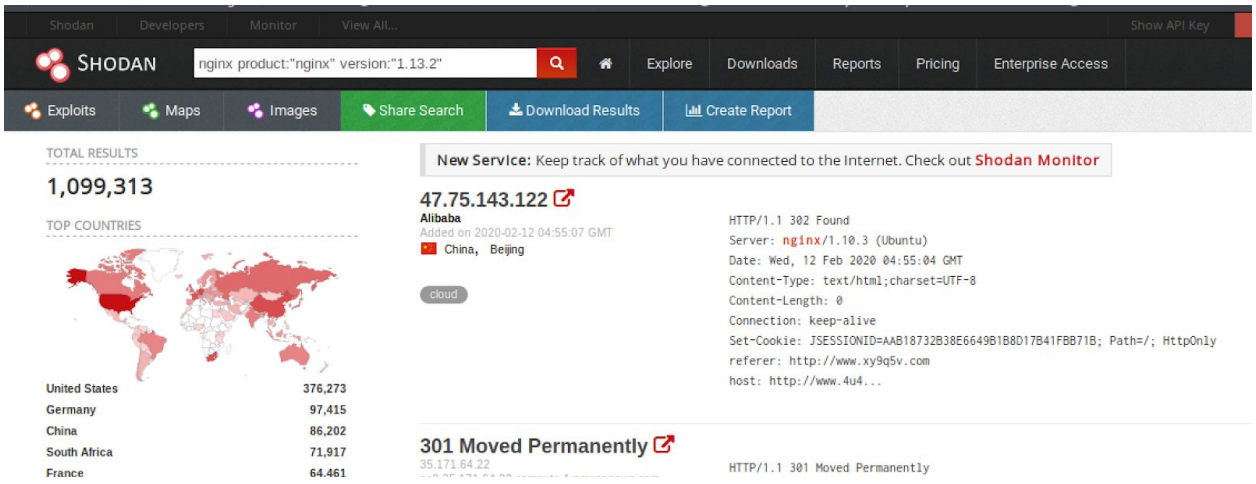
Description of this CVE is that Nginx server versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.

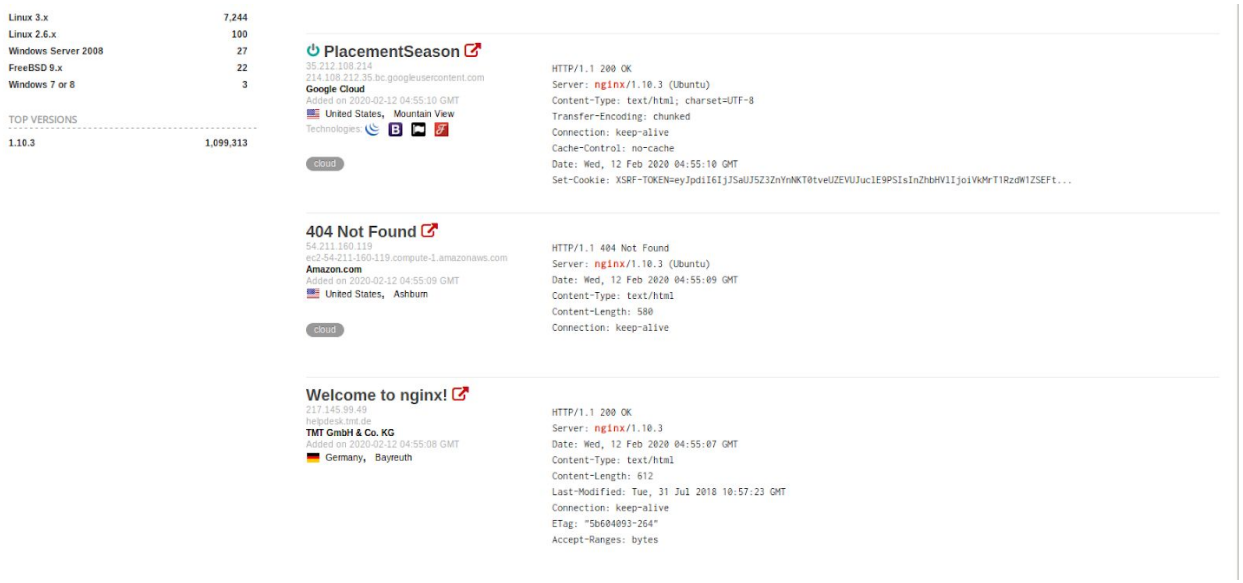
In this part we had to search for the targets running on the vulnerable version of service.

Shodan:

To search these devices in Shodan, ***vuln*** filter had to be used which is a paid feature, so I used the version number instead to search for the targets still running on vulnerable nginx version:

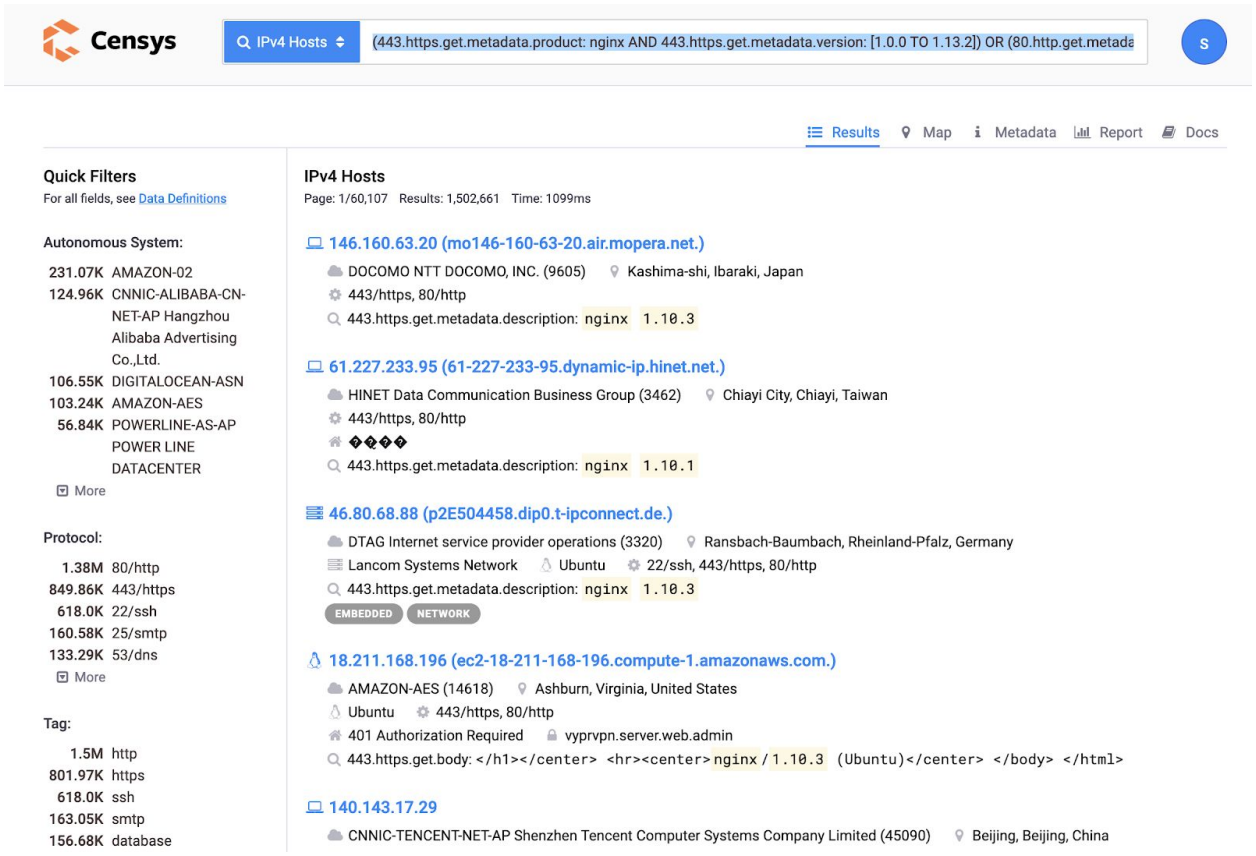




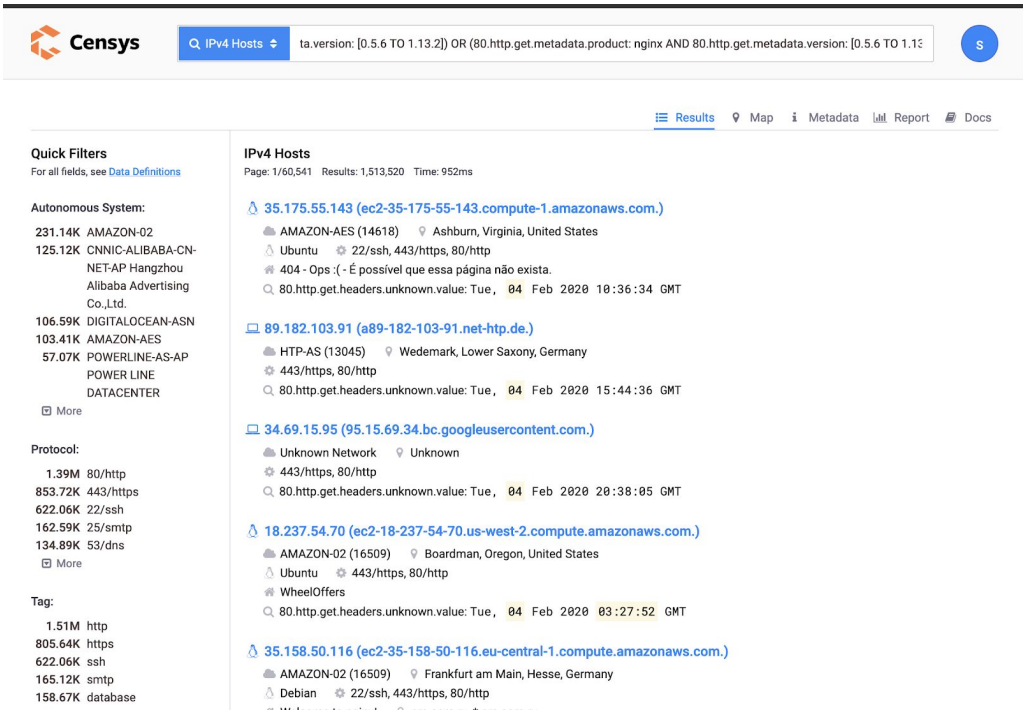


Censys:

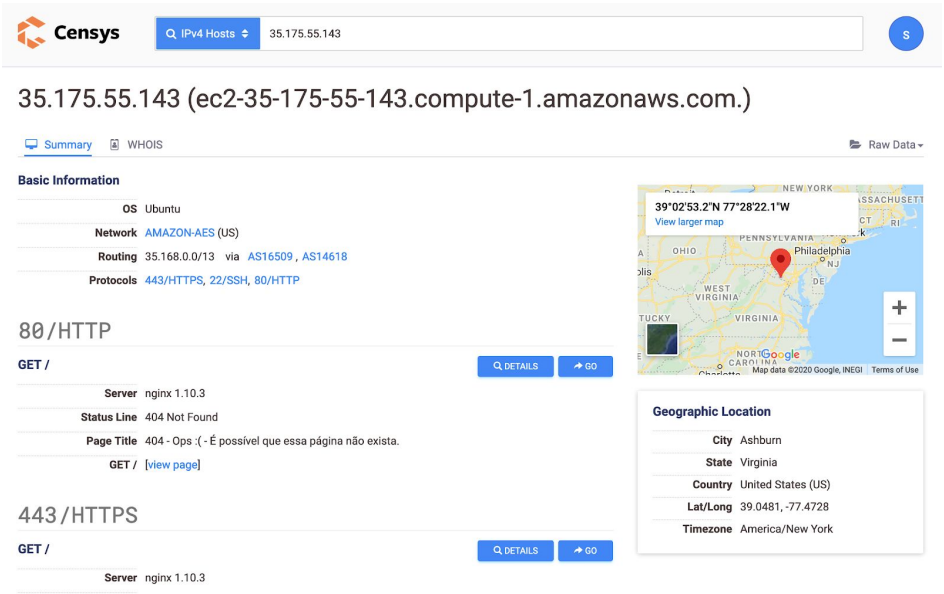
In Censys, to search for these targets, I used the query: ***(443.https.get.metadata.product: nginx AND 443.https.get.metadata.version: [1.0.0 TO 1.13.2]) OR (80.http.get.metadata.product: nginx AND 80.http.get.metadata.version: [1.0.0 TO 1.13.2])*** which returned the following result:



Tried searching from version 0.5.6 too, but it was not showing version in Banner, so searched from 1.0.0 version on nginx: ***(443.https.get.metadata.product: nginx AND 443.https.get.metadata.version: [0.5.6 TO 1.13.2]) OR (80.http.get.metadata.product: nginx AND 80.http.get.metadata.version: [0.5.6 TO 1.13.2])***. Results if searched from 0.5.6 gave the results if the results are opened individually, but did not show it in banner itself:

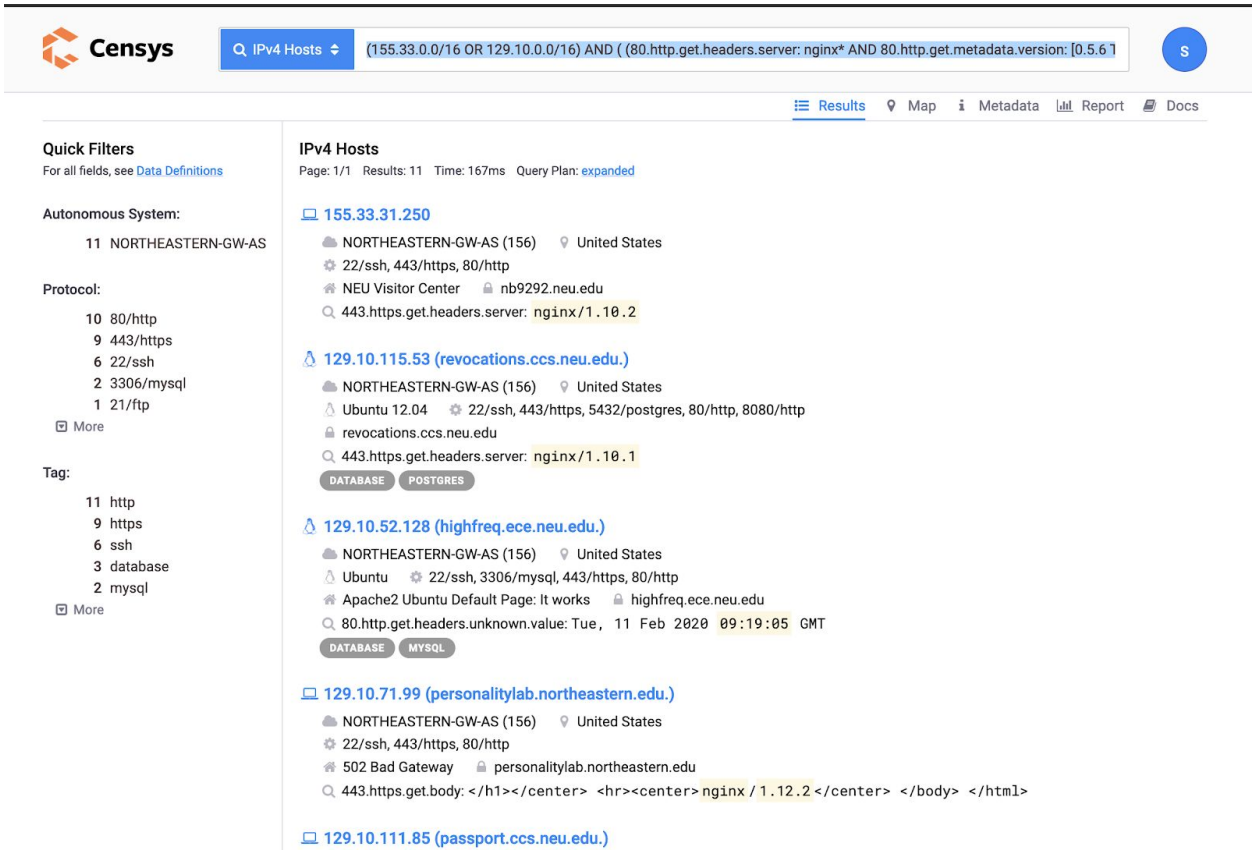


For example, if the first search result is expanded, it shows the actual version of nginx, which is vulnerable one:



In Northeastern IP Range:

The command used to search this was: ***(155.33.0.0/16 OR 129.10.0.0/16) AND ((80.http.get.headers.server: nginx* AND 80.http.get.metadata.version: [0.5.6 TO 1.13.2]) OR (443.https.get.headers.server: nginx* AND 443.https.get.metadata.version: [0.5.6 TO 1.13.2]))***, which gave following results:



References:

[1] https://en.wikipedia.org/wiki/Shodan_(website)
[2] https://securityaffairs.co/wordpress/42725/hacking/censys-search-engine.html
[3] https://nvd.nist.gov/vuln/detail/CVE-2017-7529