

Network Security Practices

CY5150

Task 6

Submitted By:

Sonam Ghatode(001305171)

Table of Contents

Introduction:	3
Shodan:	3
Censys:	3
Part 1:	4
Shodan:	4
Censys:	4
Part 2:	6
CVE-2017-7529:	6
Shodan:	6
Censys:	7
In Northeastern IP Range:	9
References:	10

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 or 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:

Shodan Developers Monitor View All... Show API Key Try o

SHODAN Cisco port:"22" country:"US" city:"Boston" net:"129.10.0.0/16" Explore Downloads Reports Pricing Enterprise Access

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
1

TOP COUNTRIES
United States 1

TOP CITIES
Boston 1

TOP ORGANIZATIONS
Northeastern University 1

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

129.10.140.77
Northeastern University
Added on 2020-02-07 23:39:20 GMT
United States, Boston

SSH-1.99-Cisco-1.25
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQgQCzCNz9F9Y7uws0GzoJf5bWVAVM+00aFT3zuKCKorme+JyD
xye4mhs+Vv6C3Zxr0JES9PTHF1ZMjrPyrLov9RVpKCugkRtw0W0FK9KTIr1bX1uxjnFb7T++sbU2
jK3KZjmzMPDxvRUq9dvpoNDZZYIJSDr3MhN0k5kt9HAyKQHbw==
Fingerprint: 60:57:15:38:17:ea:d6:cc:31:09:40:0...

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

Q 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

Q 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:

The screenshot shows the Shodan search interface with the query 'nginx product:nginx version:1.13.2'. The results are categorized into several sections:

- TOTAL RESULTS:** 5,768
- TOP COUNTRIES:** A world map showing the distribution of results, with China being the most prominent.
- TOP SERVICES:** A list of services and their counts: HTTPS (2,521), HTTP (2,065), Qconn (947), ntop (67), and HTTP (8080) (30).
- TOP ORGANIZATIONS:** A list of organizations and their counts: Hangzhou Alibaba Advertising Co., Ltd. (2,535), Eastern telecommunication Com... (499), Amazon.com (358), Fibermax S.A. (332), and Google Cloud (128).
- TOP OPERATING SYSTEMS:** A list of operating systems and their counts: Windows (1,099,313), Linux (1,099,313), macOS (1,099,313), and others.

The main results section displays three entries:

- 403 Forbidden:** A 403 Forbidden response from a server running nginx/1.13.2. The response includes headers: Date: Wed, 12 Feb 2020 04:57:58 GMT; Content-Type: text/html; Content-Length: 571; Connection: keep-alive.
- Welcome to nginx!:** A 200 OK response from a server running nginx/1.13.2. The response includes headers: Date: Wed, 12 Feb 2020 04:49:24 GMT; Content-Type: text/html; Content-Length: 612; Last-Modified: Fri, 30 Jun 2017 02:28:18 GMT; Connection: keep-alive; ETag: "5955b742-264"; Accept-Ranges: bytes.
- SSL Certificate:** A 200 OK response from a server running nginx/1.13.2. The response includes headers: Date: Wed, 12 Feb 2020 04:44:56 GMT; Content-Type: text/html; Content-Length: 612; Last-Modified: Fri, 30 Jun 2017 02:28:18 GMT.

The screenshot shows the Shodan search interface with the query 'nginx product:nginx version:1.13.2'. The results are categorized into several sections:

- TOTAL RESULTS:** 1,099,313
- TOP COUNTRIES:** A world map showing the distribution of results, with the United States being the most prominent.
- TOP SERVICES:** A list of services and their counts: HTTPS (2,521), HTTP (2,065), Qconn (947), ntop (67), and HTTP (8080) (30).
- TOP ORGANIZATIONS:** A list of organizations and their counts: Hangzhou Alibaba Advertising Co., Ltd. (2,535), Eastern telecommunication Com... (499), Amazon.com (358), Fibermax S.A. (332), and Google Cloud (128).
- TOP OPERATING SYSTEMS:** A list of operating systems and their counts: Windows (1,099,313), Linux (1,099,313), macOS (1,099,313), and others.

The main results section displays three entries:

- 47.75.143.122:** A 200 OK response from a server running nginx/1.10.3 (Ubuntu). The response includes headers: Date: Wed, 12 Feb 2020 04:55:04 GMT; Content-Type: text/html; charset=UTF-8; Content-Length: 0; Connection: keep-alive; Set-Cookie: JSESSIONID=AAB18732B38E664981B8D17B41FB871B; Path=/; HttpOnly; referer: http://www.xy9q5v.com; host: http://www.4u4....
- 301 Moved Permanently:** A 301 Moved Permanently response from a server running nginx/1.13.2. The response includes headers: Date: Wed, 12 Feb 2020 04:44:56 GMT; Content-Type: text/html; Content-Length: 612; Last-Modified: Fri, 30 Jun 2017 02:28:18 GMT.

Linux 3.x	7,244
Linux 2.6.x	100
Windows Server 2008	27
FreeBSD 9.x	22
Windows 7 or 8	3

TOP VERSIONS	
1.10.3	1,099,313

PlacementSeason
 95.212.108.214
 214.108.212.35.bc.googleusercontent.com
 Google Cloud
 Added on 2020-02-12 04:55:10 GMT
 United States, Mountain View
 Technologies

HTTP/1.1 200 OK
 Server: **nginx/1.10.3** (Ubuntu)
 Content-Type: text/html; charset=UTF-8
 Transfer-Encoding: chunked
 Connection: keep-alive
 Cache-Control: no-cache
 Date: Wed, 12 Feb 2020 04:55:10 GMT
 Set-Cookie: XSRF-TOKEN=eyJpdjI6Ij5salU5Z3Z3ZnRKT0tveUZEUVJuc1E9PSIsInZhbnV1Ijo1VWMrT1RzdW1ZSEft...

404 Not Found
 54.211.160.119
 ec2-54-211-160-119.compute-1.amazonaws.com
 Amazon.com
 Added on 2020-02-12 04:55:09 GMT
 United States, Ashburn

HTTP/1.1 404 Not Found
 Server: **nginx/1.10.3** (Ubuntu)
 Date: Wed, 12 Feb 2020 04:55:09 GMT
 Content-Type: text/html
 Content-Length: 580
 Connection: keep-alive

Welcome to nginx!
 217.145.89.49
 webdisk.mn.de
 TMT GmbH & Co. KG
 Added on 2020-02-12 04:55:08 GMT
 Germany, Bayreuth

HTTP/1.1 200 OK
 Server: **nginx/1.10.3**
 Date: Wed, 12 Feb 2020 04:55:07 GMT
 Content-Type: text/html
 Content-Length: 612
 Last-Modified: Tue, 31 Jul 2018 10:57:23 GMT
 Connection: keep-alive
 ETag: "5b604093-264"
 Accept-Ranges: bytes

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:

Quick Filters
 For all fields, see [Data Definitions](#)

Autonomous System:
 231.07K AMAZON-02
 124.96K CNNIC-ALIBABA-CN-
 NET-AP Hangzhou
 Alibaba Advertising
 Co.,Ltd.
 106.55K DIGITALOCEAN-ASN
 103.24K AMAZON-AES
 56.84K POWERLINE-AS-AP
 POWER LINE
 DATACENTER
[More](#)

Protocol:
 1.38M 80/http
 849.86K 443/https
 618.0K 22/ssh
 160.58K 25/smtp
 133.29K 53/dns
[More](#)

Tag:
 1.5M http
 801.97K https
 618.0K ssh
 163.05K smtp
 156.68K database

IPv4 Hosts
 Page: 1/60,107 Results: 1,502,661 Time: 1099ms

[146.160.63.20 \(mo146-160-63-20.air.mopera.net.\)](#)

DOCOMO NTT DOCOMO, INC. (9605) Kashima-shi, Ibaraki, Japan

443/https, 80/http

443.https.get.metadata.description: **nginx 1.10.3**

[61.227.233.95 \(61-227-233-95.dynamic-ip.hinet.net.\)](#)

HINET Data Communication Business Group (3462) Chiayi City, Chiayi, Taiwan

443/https, 80/http

443.https.get.metadata.description: **nginx 1.10.1**

[46.80.68.88 \(p2E504458.dip0.t-ipconnect.de.\)](#)

DTAG Internet service provider operations (3320) Ransbach-Baumbach, Rheinland-Pfalz, Germany

Lancom Systems Network Ubuntu 22/ssh, 443/https, 80/http

443.https.get.metadata.description: **nginx 1.10.3**

[18.211.168.196 \(ec2-18-211-168-196.compute-1.amazonaws.com.\)](#)

AMAZON-AES (14618) Ashburn, Virginia, United States

Ubuntu 443/https, 80/http

401 Authorization Required vyprvpn.server.web.admin

443.https.get.body: </h1></center> <hr><center>**nginx / 1.10.3** (Ubuntu)</center> </body> </html>

[140.143.17.29](#)

CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited (45090) Beijing, Beijing, China

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:

Censys Search: `ta.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])`

Quick Filters
For all fields, see [Data Definitions](#)

Autonomous System:
231.14K AMAZON-02
125.12K CNIC-ALIBABA-CN-
NET-AP Hangzhou
Alibaba Advertising
Co., Ltd.
106.59K DIGITALOCEAN-ASN
103.41K AMAZON-AES
57.07K POWERLINE-AS-AP
POWER LINE
DATACENTER
[More](#)

Protocol:
1.39M 80/http
853.72K 443/https
622.06K 22/ssh
162.59K 25/smtp
134.89K 53/dns
[More](#)

Tag:
1.51M http
805.64K https
622.06K ssh
165.12K smtp
158.67K database

IPv4 Hosts
Page: 1/60,541 Results: 1,513,520 Time: 952ms

35.175.55.143 (ec2-35-175-55-143.compute-1.amazonaws.com.)
AMAZON-AES (14618) Ashburn, Virginia, United States
Ubuntu 22/ssh, 443/https, 80/http
404 - Ops {- É possível que essa página não exista.
80.http.get.headers.unknown.value: Tue, 04 Feb 2020 10:36:34 GMT

89.182.103.91 (a89-182-103-91.net-http.de.)
HTP-AS (13045) Wedemark, Lower Saxony, Germany
443/https, 80/http
80.http.get.headers.unknown.value: Tue, 04 Feb 2020 15:44:36 GMT

34.69.15.95 (95.15.69.34.bc.googleusercontent.com.)
Unknown Network Unknown
443/https, 80/http
80.http.get.headers.unknown.value: Tue, 04 Feb 2020 20:38:05 GMT

18.237.54.70 (ec2-18-237-54-70.us-west-2.compute.amazonaws.com.)
AMAZON-02 (16509) Boardman, Oregon, United States
Ubuntu 443/https, 80/http
WheelOffers
80.http.get.headers.unknown.value: Tue, 04 Feb 2020 03:27:52 GMT

35.158.50.116 (ec2-35-158-50-116.eu-central-1.compute.amazonaws.com.)
AMAZON-02 (16509) Frankfurt am Main, Hesse, Germany
Debian 22/ssh, 443/https, 80/http

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

Censys Search: `35.175.55.143`

35.175.55.143 (ec2-35-175-55-143.compute-1.amazonaws.com.)

[Summary](#) [WHOIS](#) [Raw Data](#)

Basic Information
OS Ubuntu
Network AMAZON-AES (US)
Routing 35.168.0.0/13 via AS16509, AS14618
Protocols 443/HTTPS, 22/SSH, 80/HTTP

Geographic Location
City Ashburn
State Virginia
Country United States (US)
Lat/Long 39.0481, -77.4728
Timezone America/New York

80/HTTP
[GET /](#) [DETAILS](#) [GO](#)
Server nginx 1.10.3
Status Line 404 Not Found
Page Title 404 - Ops {- É possível que essa página não exista.
GET / [view page](#)

443/HTTPS
[GET /](#) [DETAILS](#) [GO](#)
Server nginx 1.10.3

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:

Censys

[Results](#) [Map](#) [Metadata](#) [Report](#) [Docs](#)

Quick Filters
For all fields, see [Data Definitions](#)

Autonomous System:

- 11 NORTHEASTERN-GW-AS

Protocol:

- 10 80/http
- 9 443/https
- 6 22/ssh
- 2 3306/mysql
- 1 21/ftp

☐ More

Tag:

- 11 http
- 9 https
- 6 ssh
- 3 database
- 2 mysql

☐ More

IPv4 Hosts
Page: 1/1 Results: 11 Time: 167ms Query Plan: [expanded](#)

[155.33.31.250](#)

- NORTHEASTERN-GW-AS (156) United States
- 22/ssh, 443/https, 80/http
- NEU Visitor Center nb9292.neu.edu
- 443.https.get.headers.server: nginx/1.10.2

[129.10.115.53 \(revocations.ccs.neu.edu.\)](#)

- NORTHEASTERN-GW-AS (156) United States
- Ubuntu 12.04 22/ssh, 443/https, 5432/postgres, 80/http, 8080/http
- revocations.ccs.neu.edu
- 443.https.get.headers.server: nginx/1.10.1

[129.10.52.128 \(highfreq.ece.neu.edu.\)](#)

- NORTHEASTERN-GW-AS (156) United States
- Ubuntu 22/ssh, 3306/mysql, 443/https, 80/http
- Apache2 Ubuntu Default Page: It works highfreq.ece.neu.edu
- 80.http.get.headers.unknown.value: Tue, 11 Feb 2020 09:19:05 GMT

[129.10.71.99 \(personalitylab.northeastern.edu.\)](#)

- NORTHEASTERN-GW-AS (156) United States
- 22/ssh, 443/https, 80/http
- 502 Bad Gateway personalitylab.northeastern.edu
- 443.https.get.body: </h1></center> <hr><center>nginx / 1.12.2</center> </body> </html>

[129.10.111.85 \(passport.ccs.neu.edu.\)](#)

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>