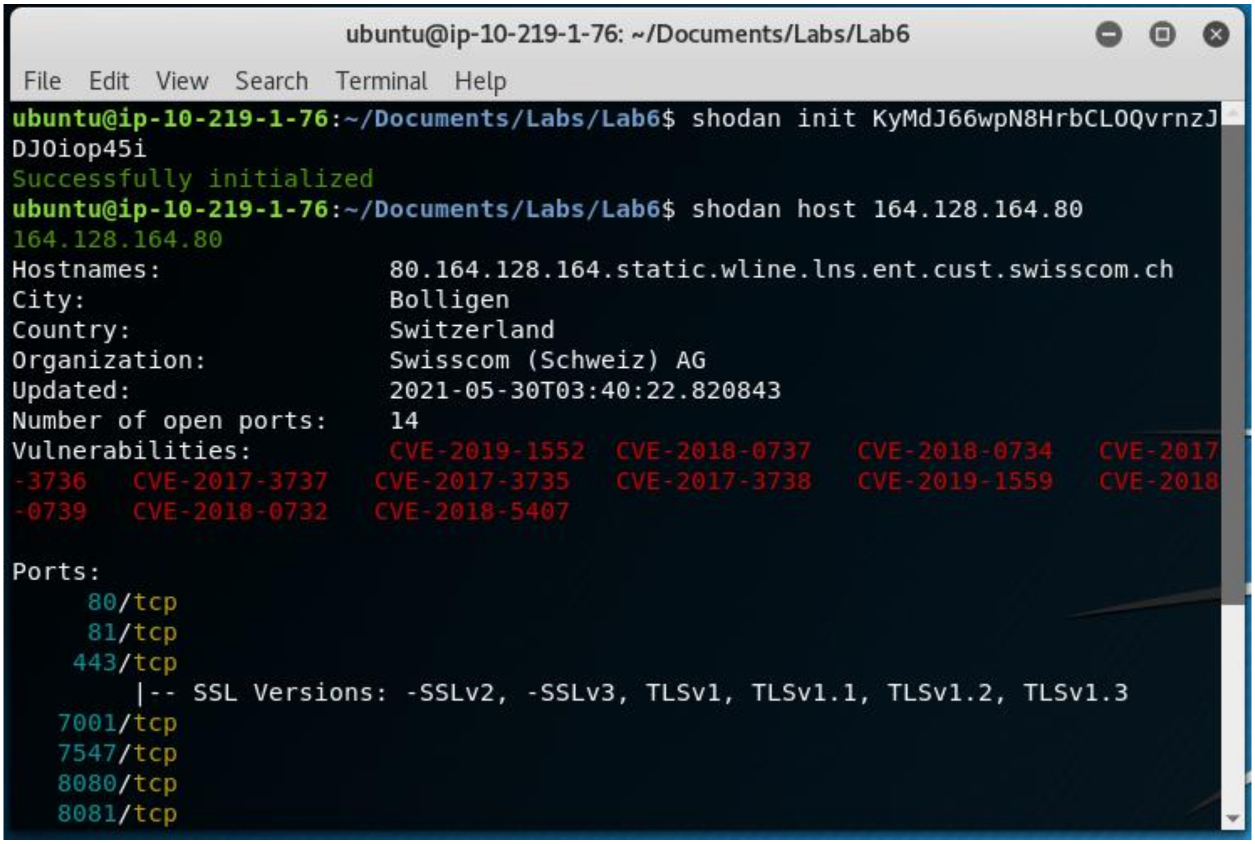
Lab 6 – IoT Shodan Lab

Section 0: Setup

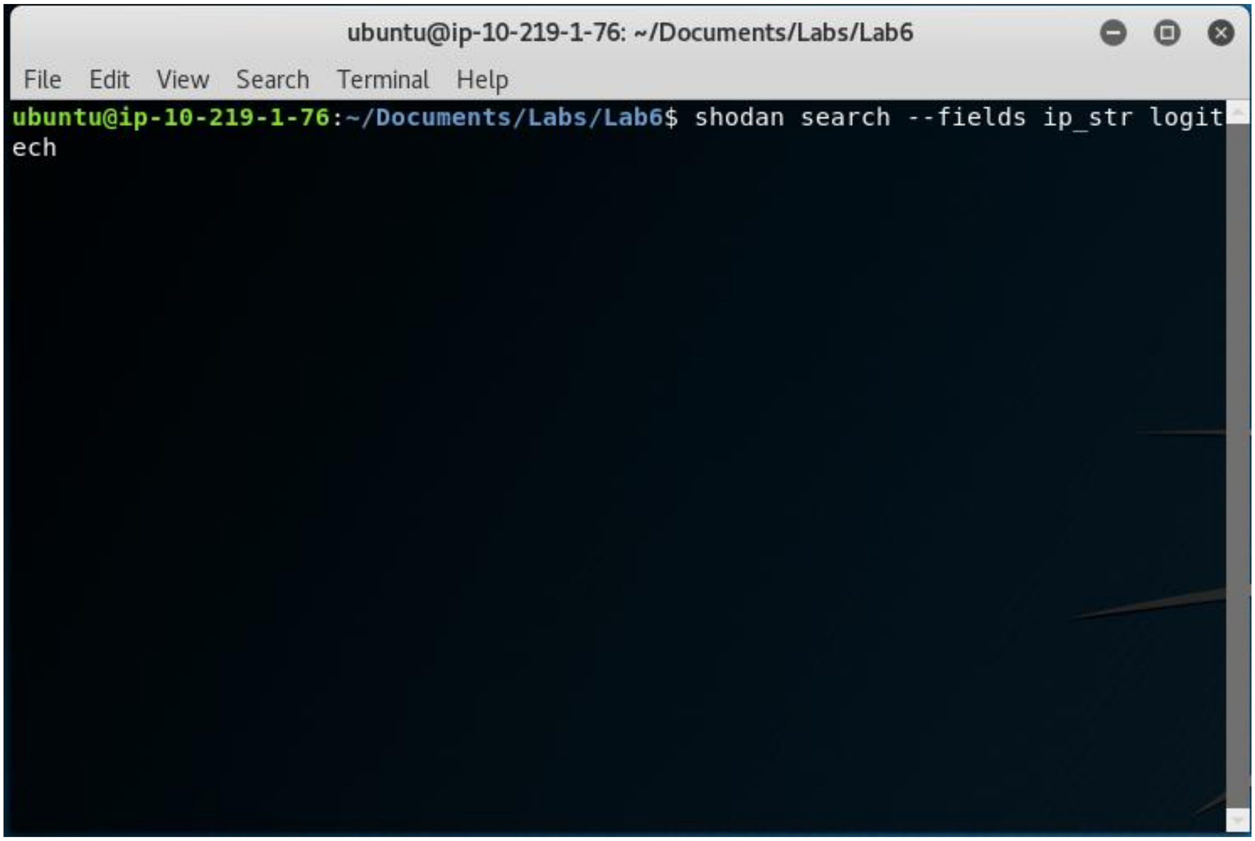


ubuntu@ip-10-219-1-76: ~/Documents/Labs/Lab6
File Edit View Search Terminal Help

```
ubuntu@ip-10-219-1-76:~/Documents/Labs/Lab6$ shodan init KyMdJ66wpN8HrbCLOQvrnzJ
DJOiop45i
Successfully initialized
ubuntu@ip-10-219-1-76:~/Documents/Labs/Lab6$ shodan host 164.128.164.80
164.128.164.80
Hostnames:                80.164.128.164.static.wline.lns.ent.cust.swisscom.ch
City:                     Bolligen
Country:                  Switzerland
Organization:             Swisscom (Schweiz) AG
Updated:                  2021-05-30T03:40:22.820843
Number of open ports:     14
Vulnerabilities:          CVE-2019-1552  CVE-2018-0737   CVE-2018-0734   CVE-2017
-3736   CVE-2017-3737   CVE-2017-3735   CVE-2017-3738   CVE-2019-1559   CVE-2018
-0739   CVE-2018-0732   CVE-2018-5407

Ports:
     80/tcp
     81/tcp
    443/tcp
        |-- SSL Versions: -SSLv2, -SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3
   7001/tcp
   7547/tcp
   8080/tcp
   8081/tcp
```

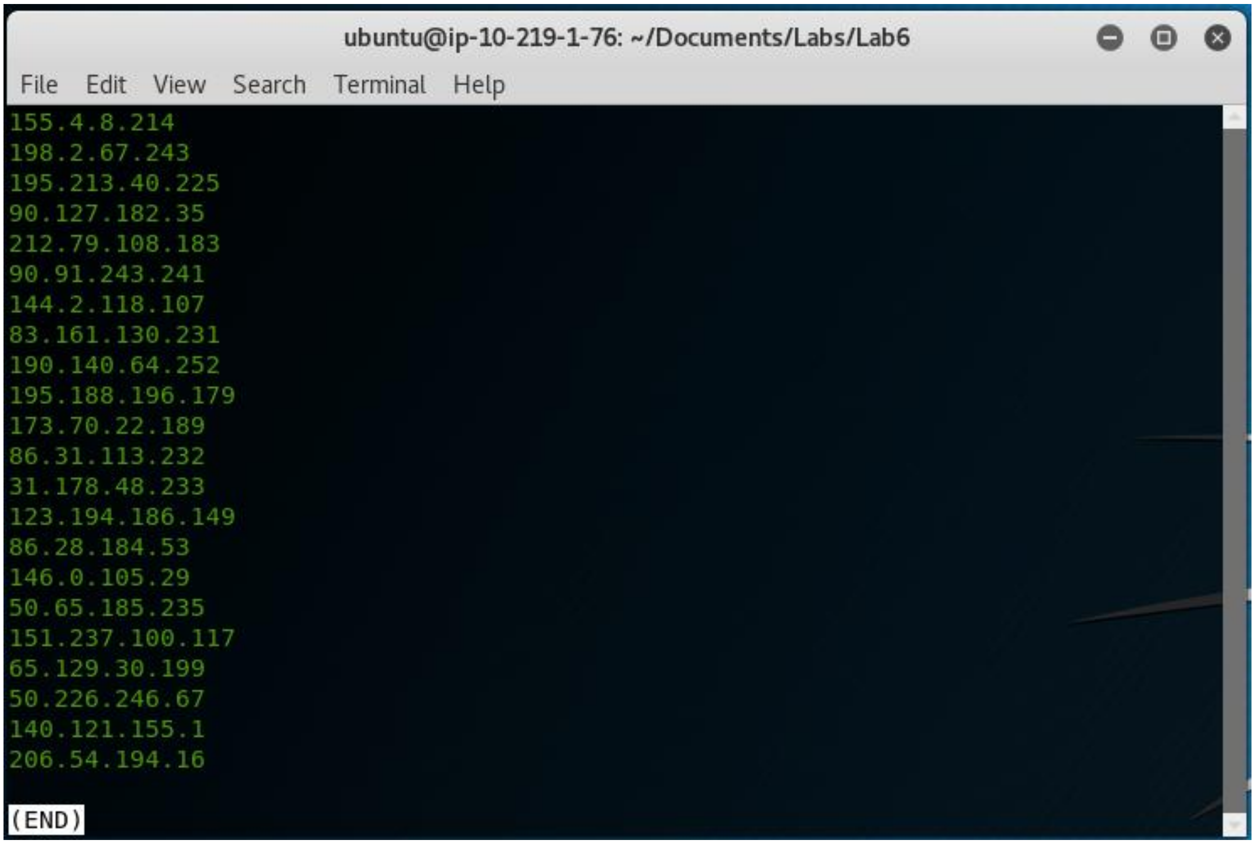
Section 1 Questions

Device 1

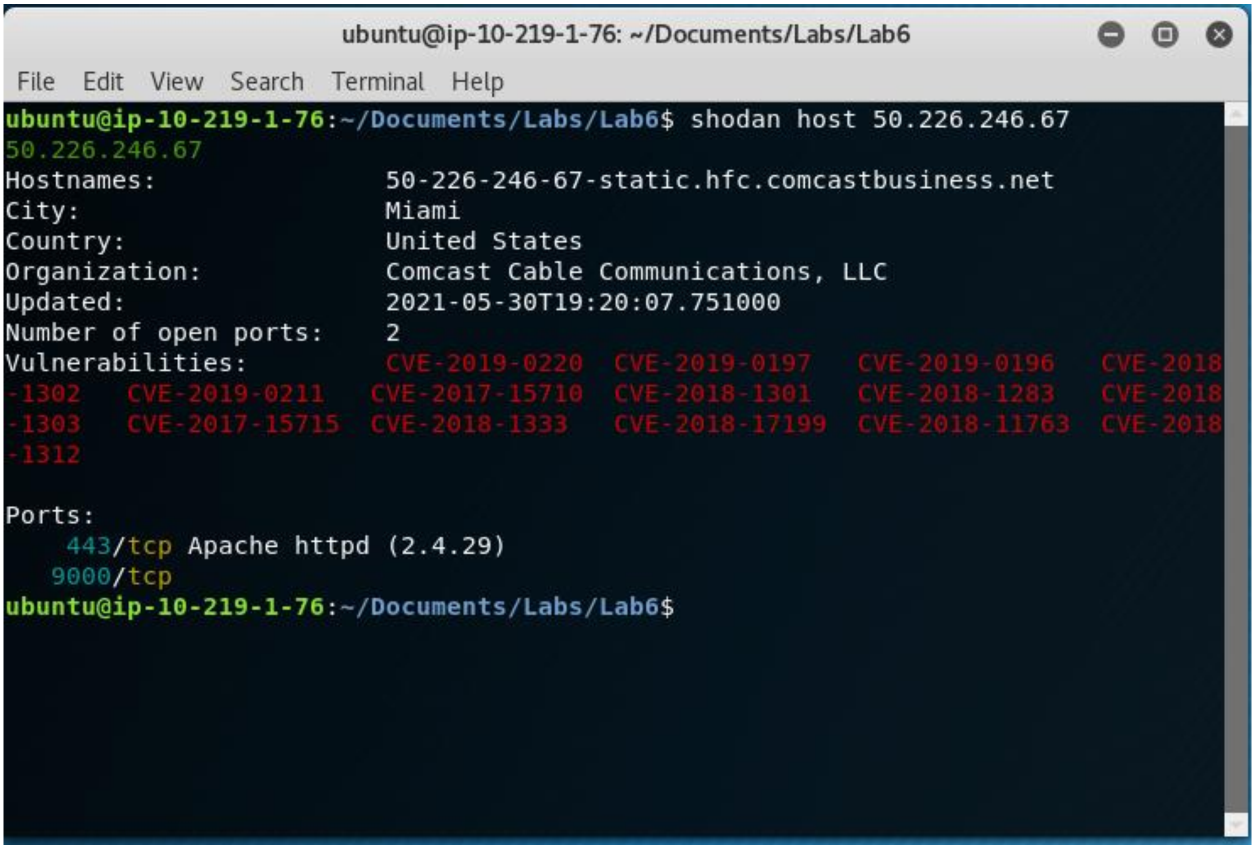


ubuntu@ip-10-219-1-76: ~/Documents/Labs/Lab6
File Edit View Search Terminal Help

```
ubuntu@ip-10-219-1-76:~/Documents/Labs/Lab6$ shodan search --fields ip_str logit
ech
```


ubuntu@ip-10-219-1-76: ~/Documents/Labs/Lab6
File Edit View Search Terminal Help

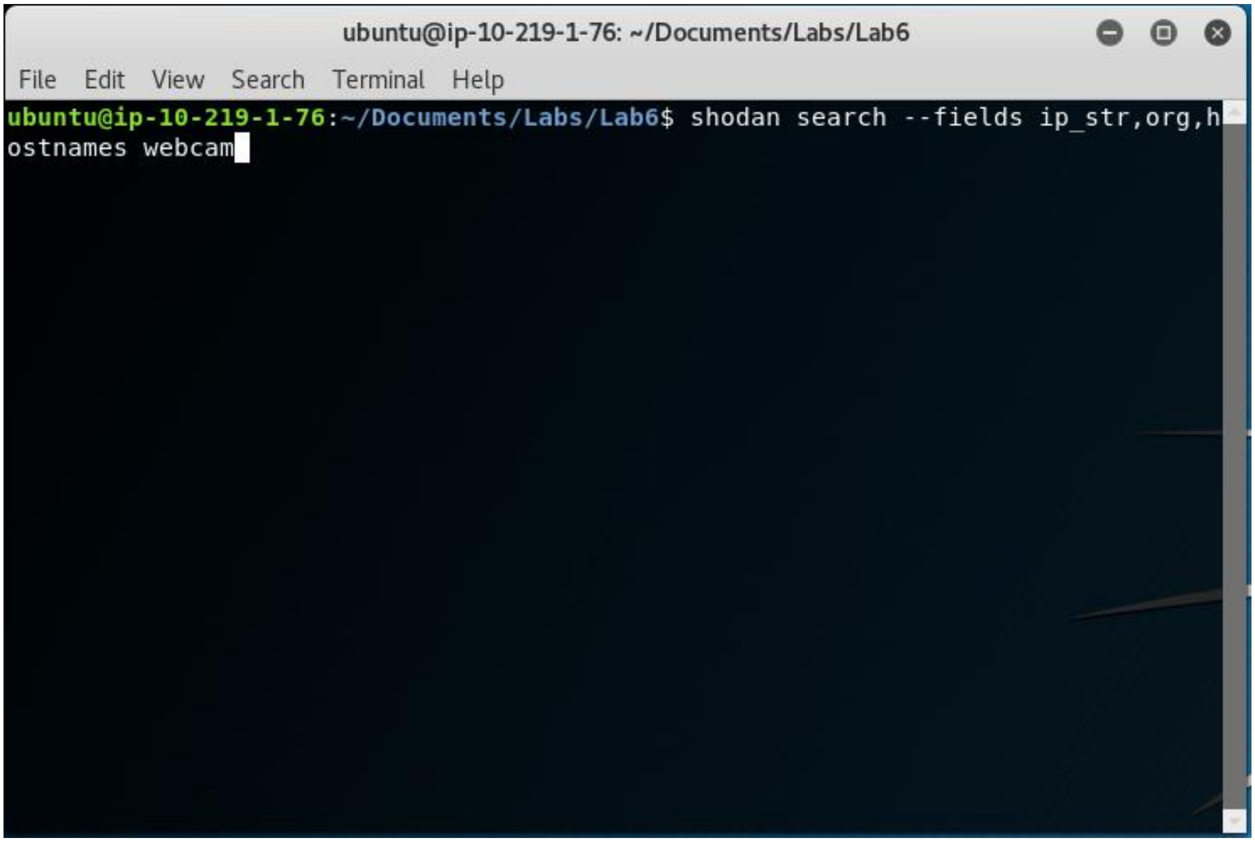
```
155.4.8.214
198.2.67.243
195.213.40.225
90.127.182.35
212.79.108.183
90.91.243.241
144.2.118.107
83.161.130.231
190.140.64.252
195.188.196.179
173.70.22.189
86.31.113.232
31.178.48.233
123.194.186.149
86.28.184.53
146.0.105.29
50.65.185.235
151.237.100.117
65.129.30.199
50.226.246.67
140.121.155.1
206.54.194.16

(END)
```


ubuntu@ip-10-219-1-76: ~/Documents/Labs/Lab6
File Edit View Search Terminal Help

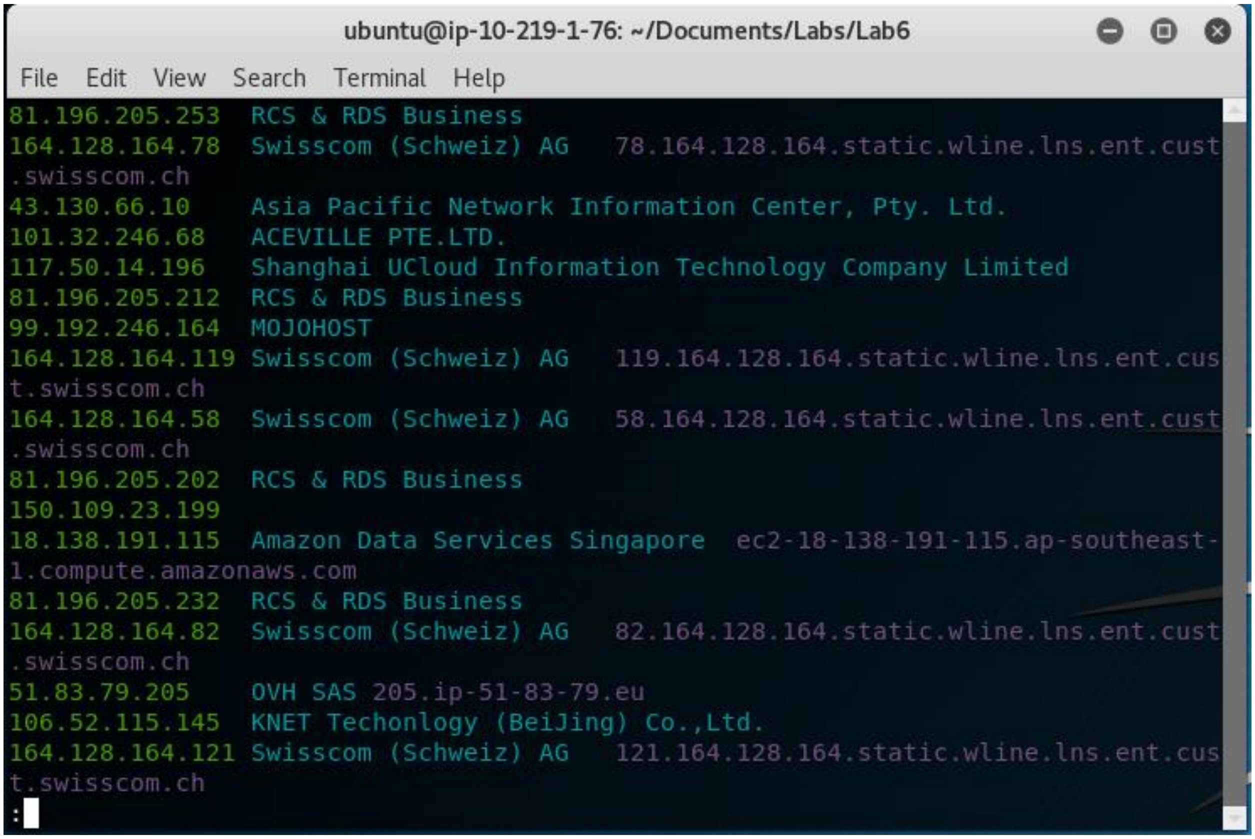
```
ubuntu@ip-10-219-1-76:~/Documents/Labs/Lab6$ shodan host 50.226.246.67
50.226.246.67
Hostnames:                 50-226-246-67-static.hfc.comcastbusiness.net
City:                      Miami
Country:                   United States
Organization:              Comcast Cable Communications, LLC
Updated:                   2021-05-30T19:20:07.751000
Number of open ports:      2
Vulnerabilities:           CVE-2019-0220  CVE-2019-0197  CVE-2019-0196  CVE-2018
-1302   CVE-2019-0211  CVE-2017-15710  CVE-2018-1301  CVE-2018-1283  CVE-2018
-1303   CVE-2017-15715  CVE-2018-1333  CVE-2018-17199  CVE-2018-11763  CVE-2018
-1312

Ports:
    443/tcp Apache httpd (2.4.29)
   9000/tcp
ubuntu@ip-10-219-1-76:~/Documents/Labs/Lab6$
```

1. How did you find the device?
    a. Using the shodan search command to list ip addresses for the search query "Logitech".
2. What are the superficial vulnerabilities?
    a. Unsecured Apache server on port 443.
3. List and explain two other vulnerabilities.
    a. The server could have been crashed by a maliciously created request (CVE-2018-1301).
    b. Maliciously created requests could cause request handlers to allocate for longer than usual, causing server overload (CVE-2018-1333).
4. What mitigation techniques are available, if any?
    a. Update Apache server version to the latest version.
5. Explain one of the CVEs in detail.
    a. A client could constantly send large SETTINGS frames to the server, which in older versions of Apache, would allow the client to keep a connection open for longer than allowed and lock up a server thread. (Only affects HTTP/2 connections)

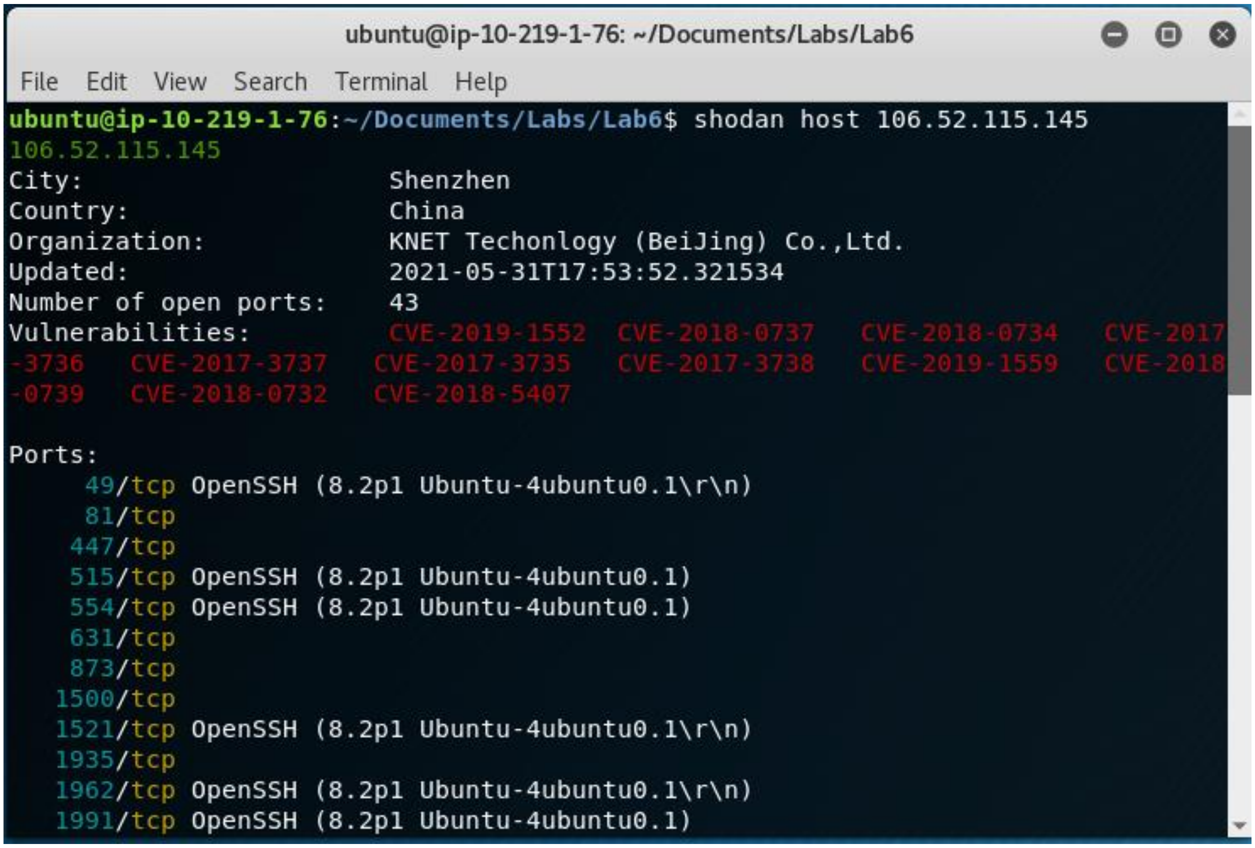
Device 2


ubuntu@ip-10-219-1-76: ~/Documents/Labs/Lab6
File Edit View Search Terminal Help

```
ubuntu@ip-10-219-1-76:~/Documents/Labs/Lab6$ shodan search --fields ip_str,org,hostnames webcam
```


ubuntu@ip-10-219-1-76: ~/Documents/Labs/Lab6
File Edit View Search Terminal Help

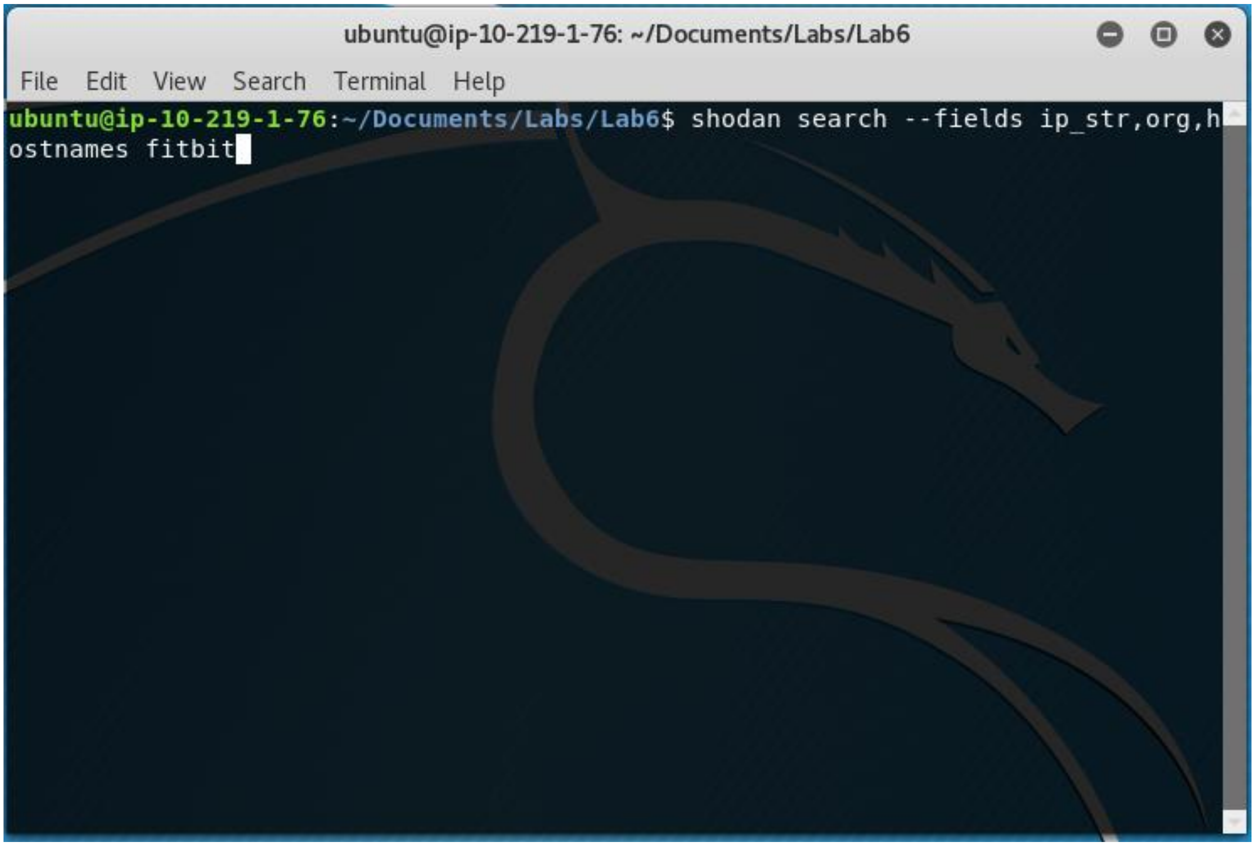
```
81.196.205.253  RCS & RDS Business
164.128.164.78  Swisscom (Schweiz) AG   78.164.128.164.static.wline.lns.ent.cust
.swisscom.ch
43.130.66.10    Asia Pacific Network Information Center, Pty. Ltd.
101.32.246.68   ACEVILLE PTE.LTD.
117.50.14.196   Shanghai UCloud Information Technology Company Limited
81.196.205.212  RCS & RDS Business
99.192.246.164  MOJOHOST
164.128.164.119 Swisscom (Schweiz) AG   119.164.128.164.static.wline.lns.ent.cus
t.swisscom.ch
164.128.164.58  Swisscom (Schweiz) AG   58.164.128.164.static.wline.lns.ent.cust
.swisscom.ch
81.196.205.202  RCS & RDS Business
150.109.23.199
18.138.191.115  Amazon Data Services Singapore  ec2-18-138-191-115.ap-southeast-
1.compute.amazonaws.com
81.196.205.232  RCS & RDS Business
164.128.164.82  Swisscom (Schweiz) AG   82.164.128.164.static.wline.lns.ent.cust
.swisscom.ch
51.83.79.205    OVH SAS 205.ip-51-83-79.eu
106.52.115.145  KNET Techonlogy (BeiJing) Co.,Ltd.
164.128.164.121 Swisscom (Schweiz) AG   121.164.128.164.static.wline.lns.ent.cus
t.swisscom.ch
:
```


ubuntu@ip-10-219-1-76: ~/Documents/Labs/Lab6
File Edit View Search Terminal Help

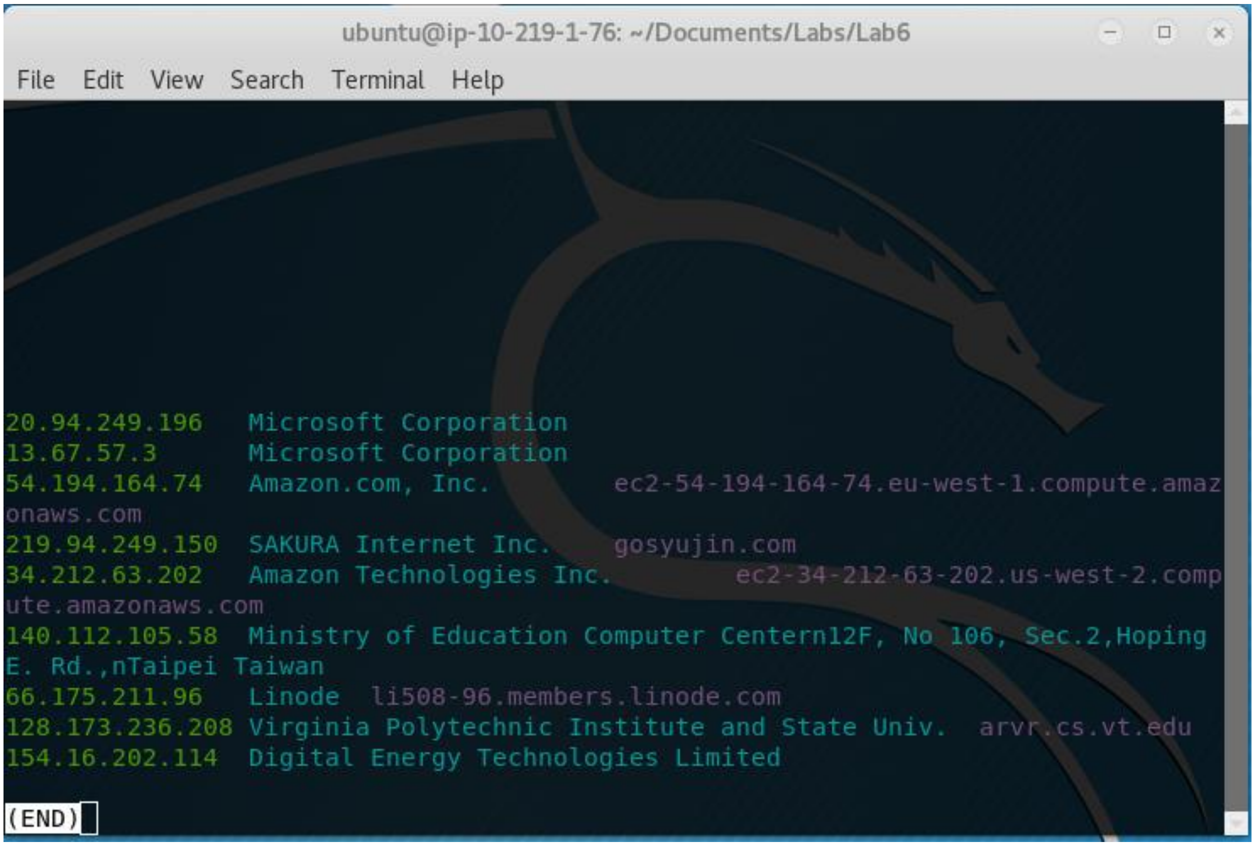
```
ubuntu@ip-10-219-1-76:~/Documents/Labs/Lab6$ shodan host 106.52.115.145
106.52.115.145
City:                    Shenzhen
Country:                 China
Organization:            KNET Techonlogy (BeiJing) Co.,Ltd.
Updated:                 2021-05-31T17:53:52.321534
Number of open ports:    43
Vulnerabilities:         CVE-2019-1552   CVE-2018-0737   CVE-2018-0734   CVE-2017
-3736   CVE-2017-3737   CVE-2017-3735   CVE-2017-3738   CVE-2019-1559   CVE-2018
-0739   CVE-2018-0732   CVE-2018-5407

Ports:
     49/tcp OpenSSH (8.2p1 Ubuntu-4ubuntu0.1\r\n)
     81/tcp
    447/tcp
    515/tcp OpenSSH (8.2p1 Ubuntu-4ubuntu0.1)
    554/tcp OpenSSH (8.2p1 Ubuntu-4ubuntu0.1)
    631/tcp
    873/tcp
   1500/tcp
   1521/tcp OpenSSH (8.2p1 Ubuntu-4ubuntu0.1\r\n)
   1935/tcp
   1962/tcp OpenSSH (8.2p1 Ubuntu-4ubuntu0.1\r\n)
   1991/tcp OpenSSH (8.2p1 Ubuntu-4ubuntu0.1)
```

1. How did you find the device?
    a. Search query using shodan showing ip, org, hostname, for keyword “webcam”.
2. What are the superficial vulnerabilities?
    a. Unsecured SSL/TLS connections on multiple open ports.
3. List and explain two other vulnerabilities.
    a. Private keys for an older version of SSL can be obtained through a cache timing attack (CVE-2018-0737)
    b. An error state feature added in 1.0.2, meant to prevent further handshake steps if an error occurred, was not being properly called for a handful of SSL commands. The handshake would then allow data to pass through regardless rather than restricting it. (CVE-2017-3737)
4. What mitigation techniques are available, if any?
    a. Upgrade to newer version of OpenSSL that patched these vulnerabilities.
5. Explain one of the CVEs in detail.
    a. In OpenSSL version 1.1.0 and 1.1.1, the default configuration file for Windows was located in C:\Users\usr\local, which was externally writable although not a problem for the Unix environment, and allowed for SSL connections on a Windows machine to have its configuration file and certificates maliciously tampered with by unauthorized users.

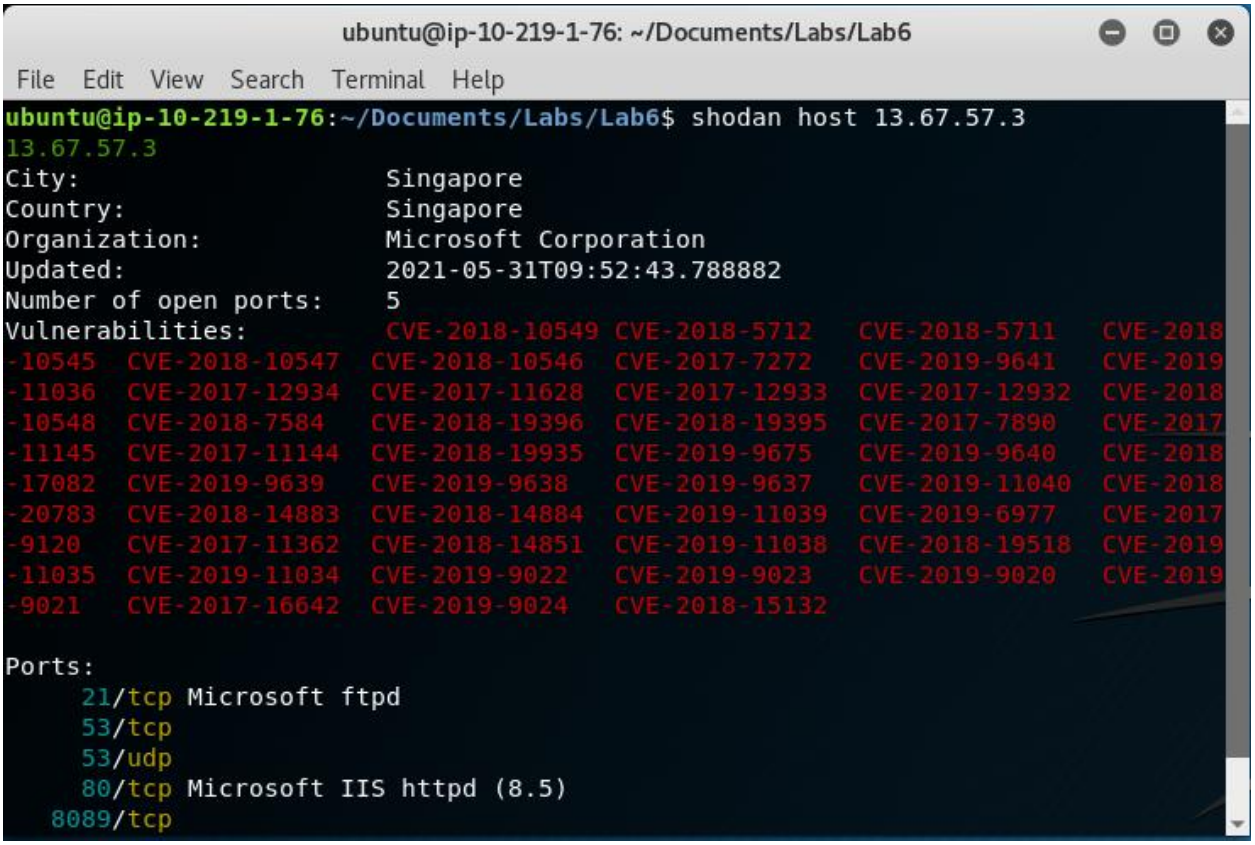
Device 3


ubuntu@ip-10-219-1-76: ~/Documents/Labs/Lab6
File Edit View Search Terminal Help

```
ubuntu@ip-10-219-1-76:~/Documents/Labs/Lab6$ shodan search --fields ip_str,org,h
ostnames fitbit
```


ubuntu@ip-10-219-1-76: ~/Documents/Labs/Lab6
File Edit View Search Terminal Help

```
20.94.249.196   Microsoft Corporation
13.67.57.3      Microsoft Corporation
54.194.164.74   Amazon.com, Inc.        ec2-54-194-164-74.eu-west-1.compute.amaz
onaws.com
219.94.249.150  SAKURA Internet Inc.    gosyujin.com
34.212.63.202   Amazon Technologies Inc.        ec2-34-212-63-202.us-west-2.comp
ute.amazonaws.com
140.112.105.58  Ministry of Education Computer Centern12F, No 106, Sec.2,Hoping
E. Rd.,nTaipei Taiwan
66.175.211.96   Linode  li508-96.members.linode.com
128.173.236.208 Virginia Polytechnic Institute and State Univ.  arvr.cs.vt.edu
154.16.202.114  Digital Energy Technologies Limited

(END)
```


ubuntu@ip-10-219-1-76: ~/Documents/Labs/Lab6
File Edit View Search Terminal Help

```
ubuntu@ip-10-219-1-76:~/Documents/Labs/Lab6$ shodan host 13.67.57.3
13.67.57.3
City:                    Singapore
Country:                 Singapore
Organization:            Microsoft Corporation
Updated:                 2021-05-31T09:52:43.788882
Number of open ports:    5
Vulnerabilities:         CVE-2018-10549 CVE-2018-5712   CVE-2018-5711   CVE-2018
-10545  CVE-2018-10547  CVE-2018-10546  CVE-2017-7272   CVE-2019-9641   CVE-2019
-11036  CVE-2017-12934  CVE-2017-11628  CVE-2017-12933  CVE-2017-12932  CVE-2018
-10548  CVE-2018-7584   CVE-2018-19396  CVE-2018-19395  CVE-2017-7890   CVE-2017
-11145  CVE-2017-11144  CVE-2018-19935  CVE-2019-9675   CVE-2019-9640   CVE-2018
-17082  CVE-2019-9639   CVE-2019-9638   CVE-2019-9637   CVE-2019-11040  CVE-2018
-20783  CVE-2018-14883  CVE-2018-14884  CVE-2019-11039  CVE-2019-6977   CVE-2017
-9120   CVE-2017-11362  CVE-2018-14851  CVE-2019-11038  CVE-2018-19518  CVE-2019
-11035  CVE-2019-11034  CVE-2019-9022   CVE-2019-9023   CVE-2019-9020   CVE-2019
-9021   CVE-2017-16642  CVE-2019-9024   CVE-2018-15132

Ports:
     21/tcp Microsoft ftpd
     53/tcp
     53/udp
     80/tcp Microsoft IIS httpd (8.5)
   8089/tcp
```

1. How did you find the device?
    a. Search query using shodan showing IP, org, hostname, using keyword “fitbit”
2. What are the superficial vulnerabilities?
    a. Unsecured open FTP connection on port 21, IIS connection on port 80
3. List and explain two other vulnerabilities.
    a. PHP issue allowed bypassing opcache access controls to allow a user to get sensitive information about another user (CVE-2018-10545)
    b. Possible information leak caused by an extension reading past the buffer limit when reading information (CVE-2019-11036)
4. What mitigation techniques are available, if any?
    a. Update PHP to the latest version.
5. Explain one of the CVEs in detail.
    a. In previous version of PHP on Windows, the linkinfo function doesn’t correctly support the check open_basedir. The lack of this check can be used to find files and information outside what is allowed, since the system does not know otherwise to disallow it.