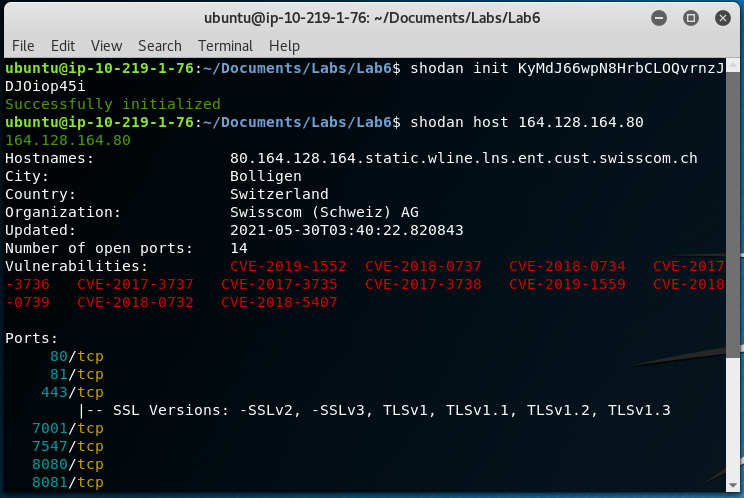
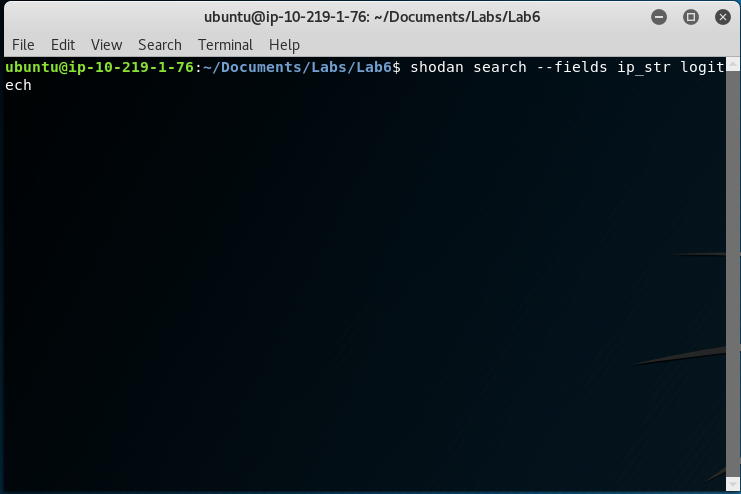
# Lab 6 – IoT Shodan Lab

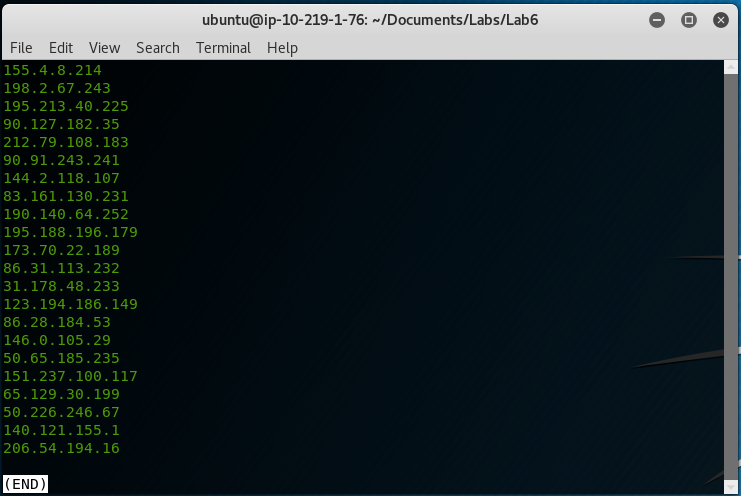
## Section 0: Setup

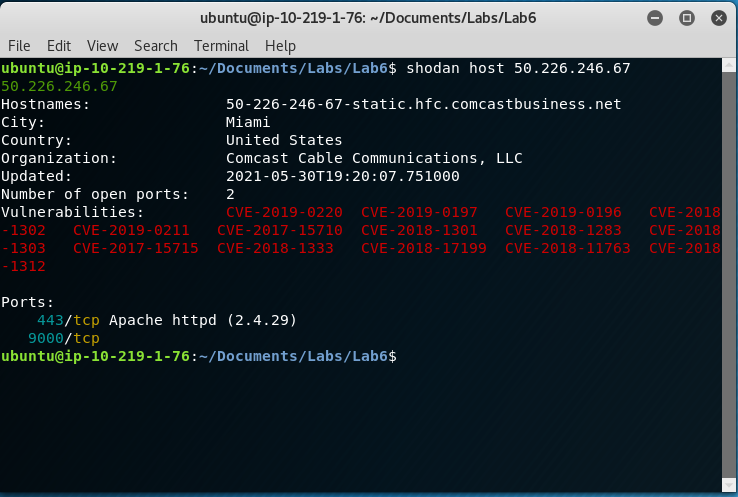


## Section 1 Questions

### Device 1

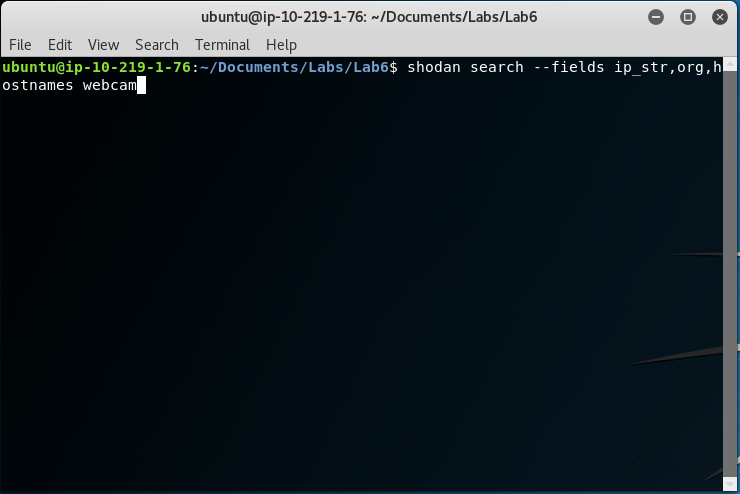


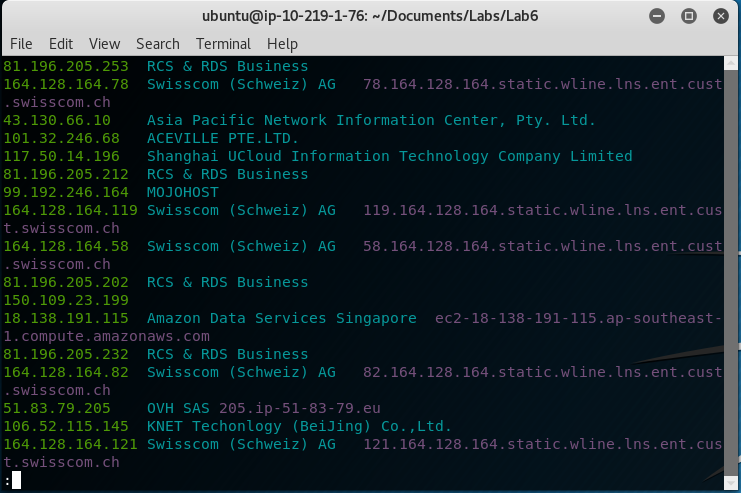


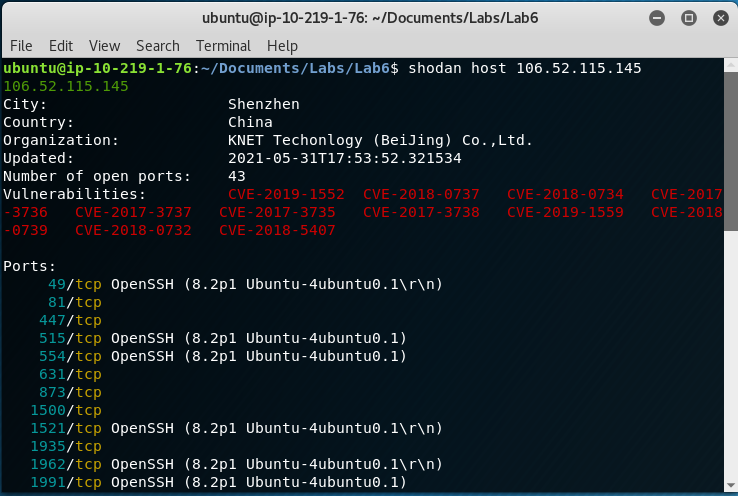


1. How did you find the device?
   1. Using the shodan search command to list ip addresses for the search query “Logitech”.
2. What are the superficial vulnerabilities?
   1. Unsecured Apache server on port 443.
3. List and explain two other vulnerabilities.
   1. The server could have been crashed by a maliciously created request (CVE-2018-1301).
   2. 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?
   1. Update Apache server version to the latest version.
5. Explain one of the CVEs in detail.
   1. 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

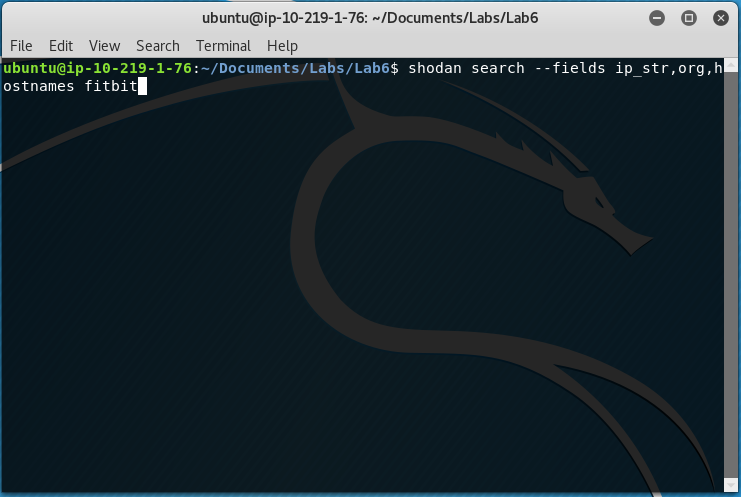


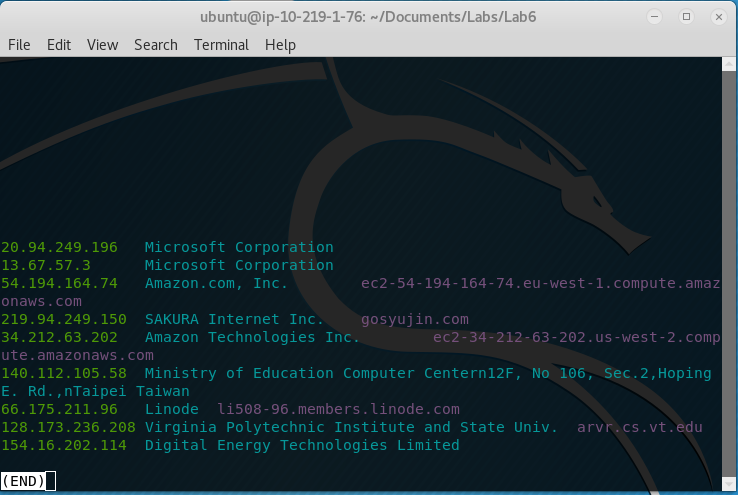


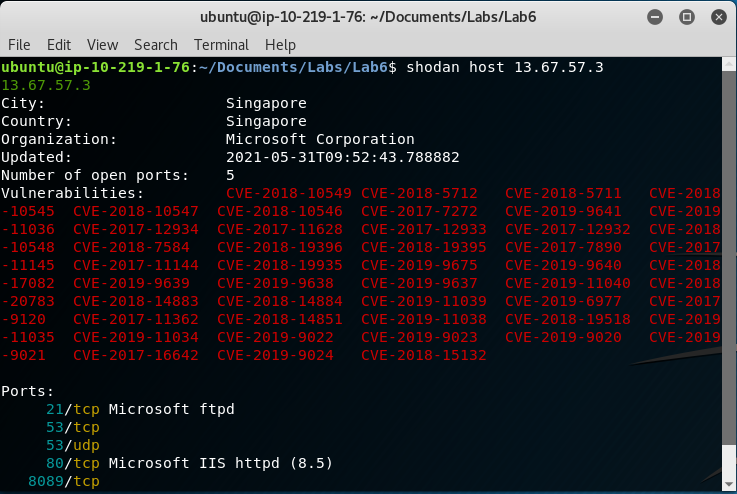


1. How did you find the device?
   1. Search query using shodan showing ip, org, hostname, for keyword “webcam”.
2. What are the superficial vulnerabilities?
   1. Unsecured SSL/TLS connections on multiple open ports.
3. List and explain two other vulnerabilities.
   1. Private keys for an older version of SSL can be obtained through a cache timing attack (CVE-2018-0737)
   2. 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?
   1. Upgrade to newer version of OpenSSL that patched these vulnerabilities.
5. Explain one of the CVEs in detail.
   1. 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







1. How did you find the device?
   1. Search query using shodan showing IP, org, hostname, using keyword “fitbit”
2. What are the superficial vulnerabilities?
   1. Unsecured open FTP connection on port 21, IIS connection on port 80
3. List and explain two other vulnerabilities.
   1. PHP issue allowed bypassing opcache access controls to allow a user to get sensitive information about another user (CVE-2018-10545)
   2. 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?
   1. Update PHP to the latest version.
5. Explain one of the CVEs in detail.
   1. 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.