CSCE5580: Computer Networks

Project 1: Network Monitoring Tools

Points: 100 points for full credit

Objective: The objective of the project is to help students to learn some frequently seen network monitoring tools and network moniroting websites. Through the usage of the wiretapping tool such as Wireshark, students can learn about the network packets and how information is encapsulated. In real life, many network administrators and security engineers depend on such tools to capture network activities and then analyze them. The introduction to the webpage Shodan shows how many network devices are online without protection.

Requirements:

(1) References are required in academic format (e.g., APA, MLA, Chicago, etc.). Lack of references will be an automatic loss of points.
(2) All figures and screenshots are required to be labeled per academic format (e.g., Figure 1).
(3) Formatting and consistency matter, make sure to proofread your work.
(4) The submission should be readable with logical flow of information in sections or paragraphs.
(5) The assignment should be approximately ten pages including figures.
(6) Submission must have a title page or header showing date, instructor, student name, and course name at minimum.
(7) Answers to technical questions may be one sentence if appropriate.

Task (1)

(1) Locate and install a wiretapping software tool such as Wireshark. It can eavesdrop on both wired and wireless networks. Make sure that you are downloading from the reliable source such as www.wireshark.org. Do not use third party websites since attackers may embed malware in it.

(2) Use Wireshark to open the packet capture file that we provide. Please note that the file contains some Industrial Control System (ICS) network traffic that we capture. It uses a protocol called Modbus. You can use google to figure out the protocol and port number that Modbus uses.

In this capture file, please answer the following questions:

(a) How many unique MAC addresses were on the network?
(b) How many unique IP addresses were on the network (IPv4 and IPv6)?
(c) What were the two UDP protocols used?

(d) Which Ethernet address was shared between an IPv4 and IPv6 address?
(e) It seems that there is a Human-Machine Interface (HMI) server that interacts with multiple devices in the network through Modbus. What is the IP address of the server?

To accomplish these tasks, you need to use the analysis tools in Wireshark. In the top tool bar, locate the entry called "Statistics". Everything you need should be there. I will recommend you to look at the entries such as "Protocol Hierarchy", "EndPoints", and "Conversations".

Task (2)

(1) Sign up for a free account at www.shodan.io. Note that the registration is free but access to some sensitive information needs payment. You do NOT need to pay the website.

(2) Login to Shodan. Click "explore" at the top. You will see several hot categories. See the attached screenshot.

(3) You can directly type "port:502" in the top explore window. You will then see many items shown on the screen. They are IoT devices that you can access all around the world. You can choose one country or one organization to explore.

(4) Now find one device/IP address returned by shodan that does not show "error" or illegal device type. You can see from the summary what type of device it is. Use google to find out the device type, its manual, and any vulnerabilities associated with the device. This is usually how attackers locate targets and vulnerabilities.

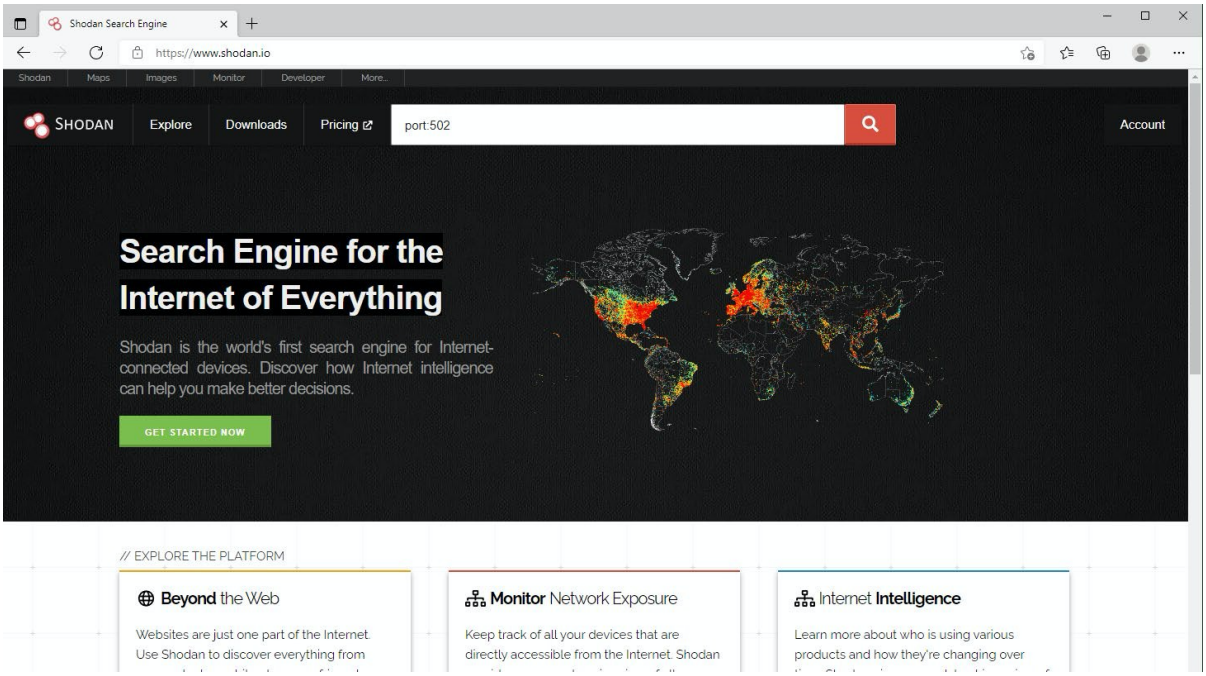
Turn-ins: For task 1, answer all questions and write a paragraph to describe how you figure out the shared MAC address that is associated with multiple IP addresses. Attach at least three screenshots to show how to finish the task. Do not share your screenshots with other students.

For task 2, show the screenshot of the IP address and device type that you find in shodan. Also write a half page report on any vulnerabilities that you can find for this device/chip. If you cannot find any vulnerability report for the device, change to another one.

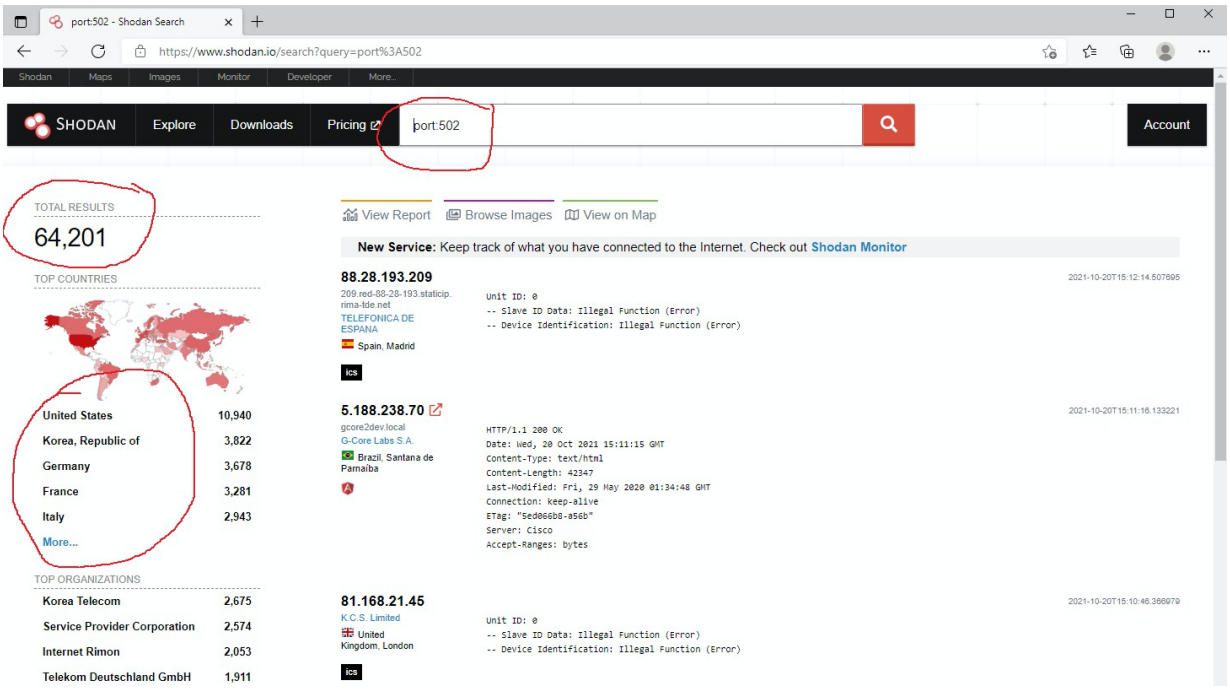
Tip: Wireshark can run on both Windows and Linux machines. I believe there are wiretap tools for Mac as well. In Windows, when you start Wireshark and if you see "no

interface can be found", close the application, right click "WireShark", choose "Run as administrator" and you should be fine.

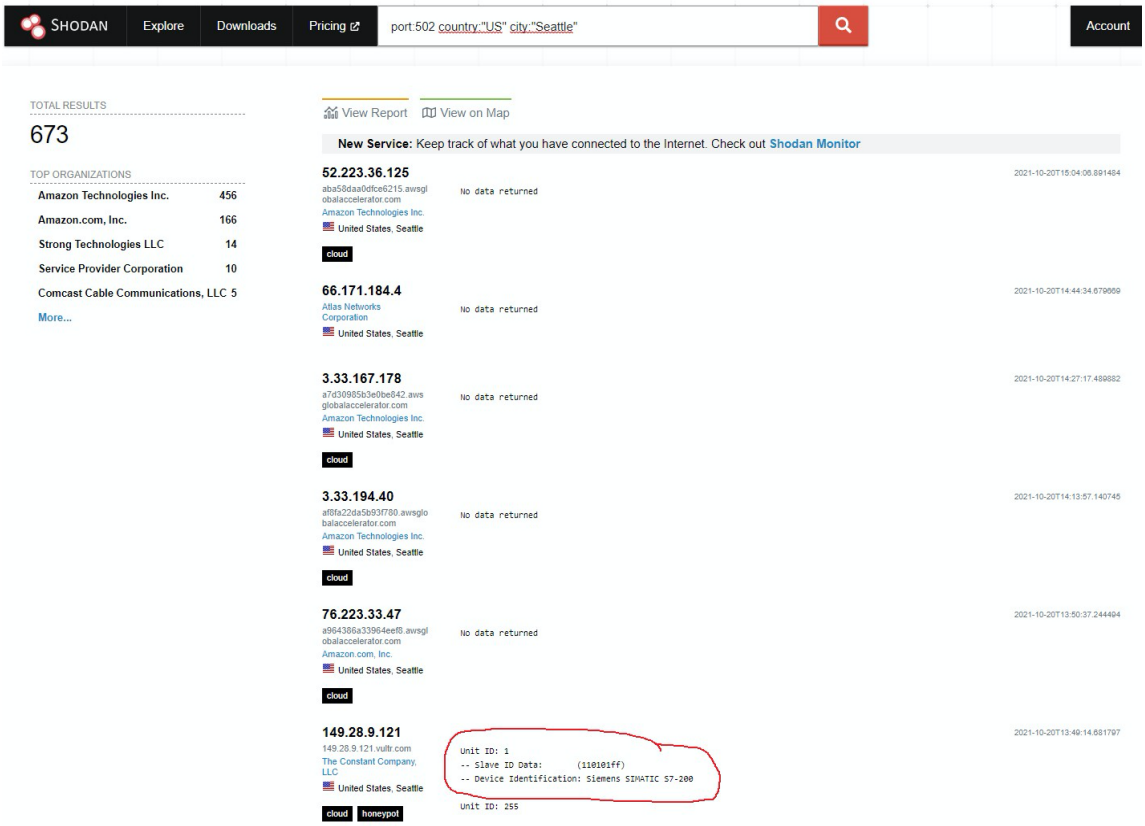
The following figure shows a screenshot from Shodan. At the IP address 149.28.9.121, you can find many open ports. The device type is Siemens SIMATIC S7-200. Through google, you can find that it is a Siemens Programmable Controller that uses Modbus protocol. You can then find any vulnerabilities associated with the device or protocol. Note that Shodan also shows the physical zone (Seattle area). We also provide a few screenshots for locating the devices in Shodan.

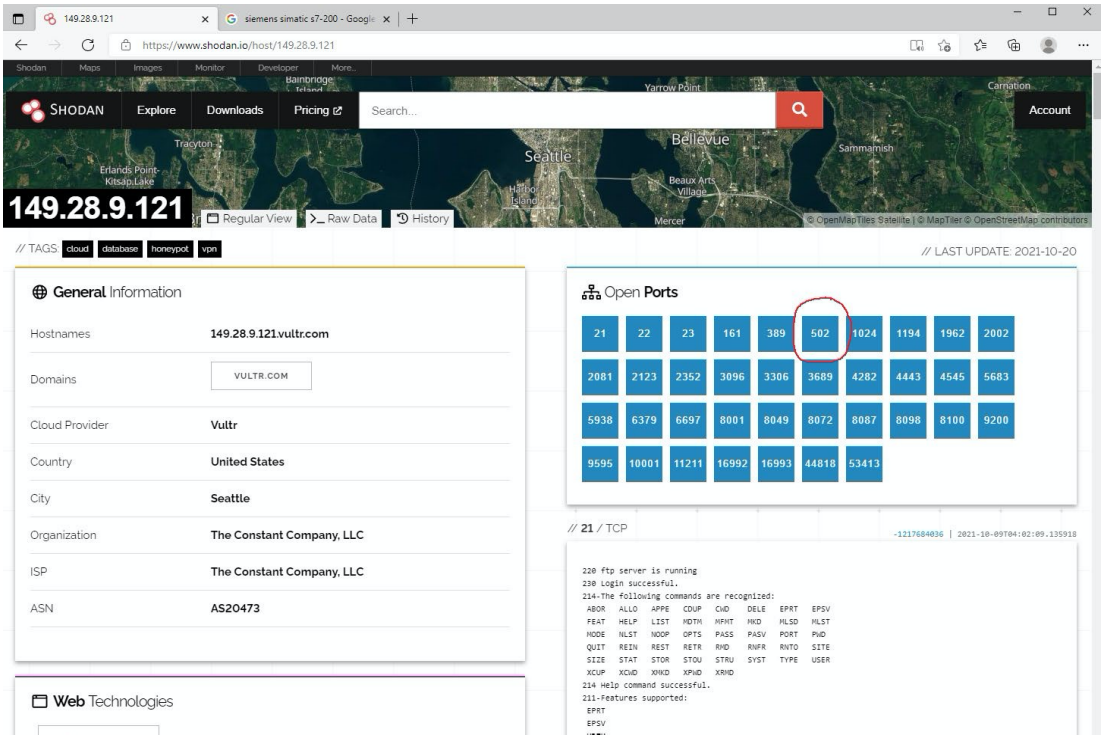


Login page of Shodan

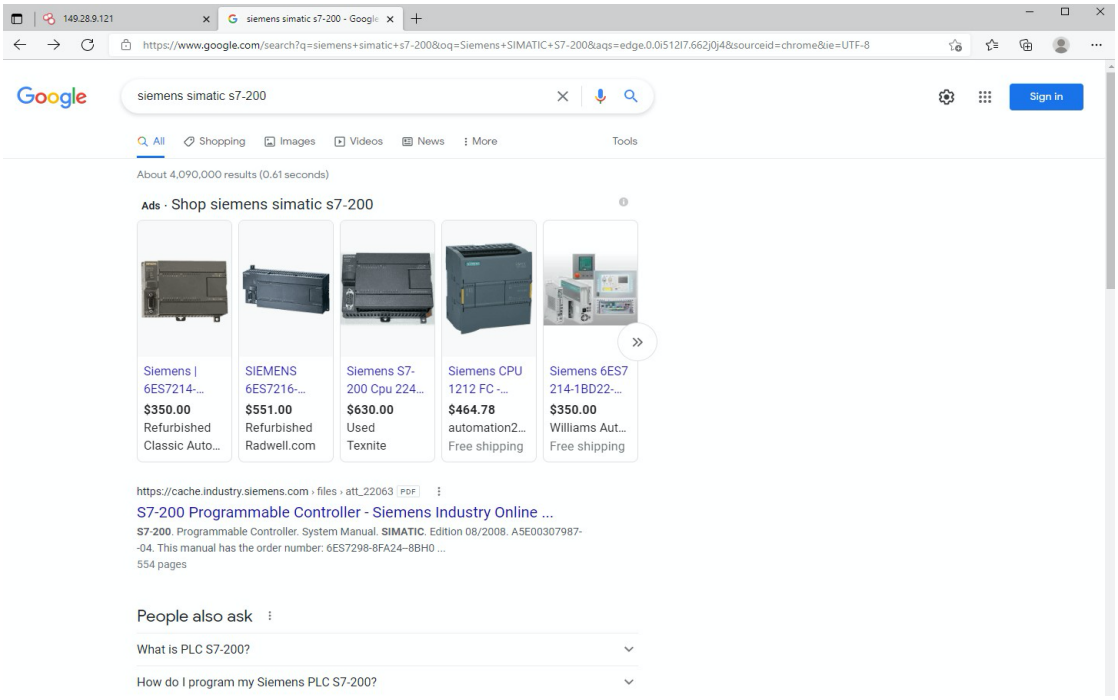


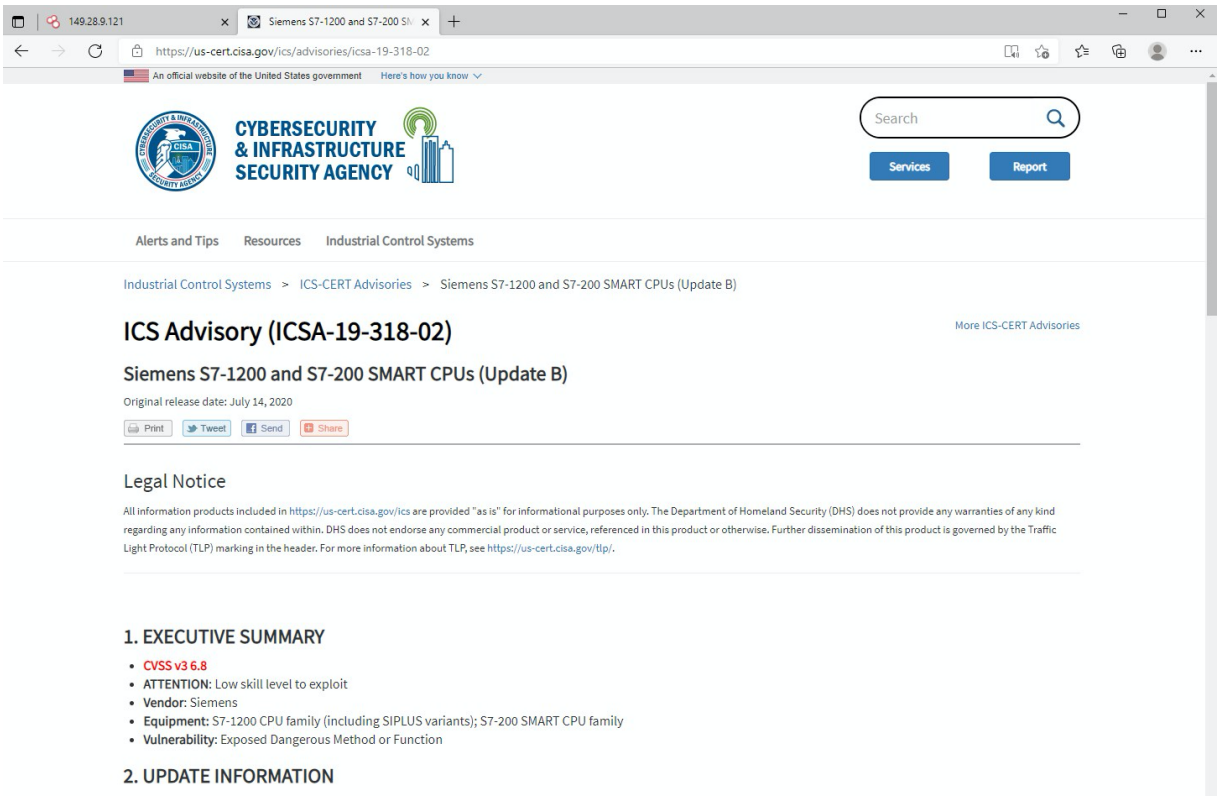
Search for Port 502





Locate a device of interest





Search for specific devices and vulnerabilities