

# 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 monitoring 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](http://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](http://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.

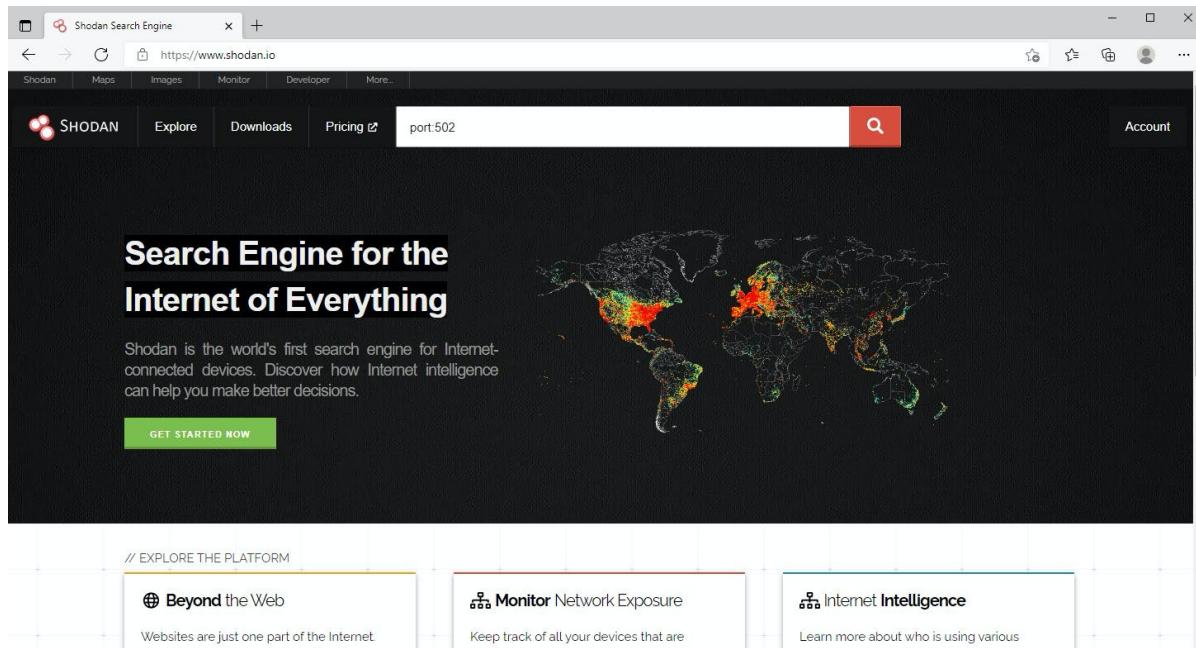
**Turn-ins:** For task 1, answer all questions and write a paragraph to describe how you figure out the shared MAC address that is associated with multiple IP addresses. Attach at least three screenshots to show how to finish the task. Do not share your screenshots with other students.

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**

port:502 - Shodan Search

<https://www.shodan.io/search?query=port%3A502>

Shodan | Maps | Images | Monitor | Developer | More...

**SHODAN** Explore Downloads Pricing port:502 Account

**TOTAL RESULTS**  
**64,201**

**TOP COUNTRIES**

Country	Count
United States	10,940
Korea, Republic of	3,822
Germany	3,678
France	3,281
Italy	2,943
More...	

**TOP ORGANIZATIONS**

Organization	Count
Korea Telecom	2,675
Service Provider Corporation	2,574
Internet Riron	2,053
Telekom Deutschland GmbH	1,911

**88.28.193.209** 209.red-88-28-193.static.ip.irma-ide.net TELEFONICA DE ESPANA Spain, Madrid

Unit ID: 0  
-- Slave ID Data: Illegal Function (Error)  
-- Device Identification: Illegal Function (Error)

**5.188.238.70** gcore2dev.local G-Core Labs S.A. Brazil, Santana de Parnaíba

HTTP/1.1 200 OK  
Date: wed, 28 oct 2021 15:11:15 gmt  
Content-Type: text/html  
Content-Length: 42347  
Last-Modified: fri, 29 may 2020 01:34:48 gmt  
Connection: keep-alive  
ETag: "5ed066b0-a5eb"  
Server: Cisco  
Accept-Ranges: bytes

**81.168.21.45** K.C.S. Limited United Kingdom, London

Unit ID: 0  
-- Slave ID Data: Illegal Function (Error)  
-- Device Identification: Illegal Function (Error)

**52.223.36.125** ab50d6a0d0cc215.awsgl obalaccelerator.com Amazon Technologies Inc. United States, Seattle

No data returned

**66.171.184.4** a7d3098503a0b0e842.aws globalaccelerator.com Amazon Technologies Inc. United States, Seattle

No data returned

**3.33.167.178** a7d3098503a0b0e842.aws globalaccelerator.com Amazon Technologies Inc. United States, Seattle

No data returned

**3.33.194.40** a7f0a22d5ab90780.awsglo balaccelerator.com Amazon Technologies Inc. United States, Seattle

No data returned

**76.223.33.47** a964368a33964eebf.awsgl obalaccelerator.com Amazon.com, Inc. United States, Seattle

No data returned

**149.28.9.121** 149.28.9.121.vulfr.com The Constant Company, LLC United States, Seattle

Unit ID: 1  
-- Slave ID Data: (110101ff)  
-- Device Identification: Siemens SIMATIC 57-200

Unit ID: 255

cloud honeypot

## Search for Port 502

SHODAN | Explore | Downloads | Pricing | port:502 country:"US" city:"Seattle" Account

**TOTAL RESULTS**  
**673**

**TOP ORGANIZATIONS**

Organization	Count
Amazon Technologies Inc.	456
Amazon.com, Inc.	166
Strong Technologies LLC	14
Service Provider Corporation	10
Comcast Cable Communications, LLC	5
More...	

**52.223.36.125** ab50d6a0d0cc215.awsgl obalaccelerator.com Amazon Technologies Inc. United States, Seattle

No data returned

**66.171.184.4** a7d3098503a0b0e842.aws globalaccelerator.com Amazon Technologies Inc. United States, Seattle

No data returned

**3.33.167.178** a7d3098503a0b0e842.aws globalaccelerator.com Amazon Technologies Inc. United States, Seattle

No data returned

**3.33.194.40** a7f0a22d5ab90780.awsglo balaccelerator.com Amazon Technologies Inc. United States, Seattle

No data returned

**76.223.33.47** a964368a33964eebf.awsgl obalaccelerator.com Amazon.com, Inc. United States, Seattle

No data returned

**149.28.9.121** 149.28.9.121.vulfr.com The Constant Company, LLC United States, Seattle

Unit ID: 1  
-- Slave ID Data: (110101ff)  
-- Device Identification: Siemens SIMATIC 57-200

Unit ID: 255

cloud honeypot

**General Information**

Hostnames	149.28.9.121.vultr.com
Domains	VULTR.COM
Cloud Provider	Vultr
Country	United States
City	Seattle
Organization	The Constant Company, LLC
ISP	The Constant Company, LLC
ASN	AS20473

**Open Ports**

21	22	23	161	389	502	1024	1194	1962	2002
2081	2123	2352	3096	3306	3689	4282	4443	4545	5683
5938	6379	6697	8001	8049	8072	8087	8098	8100	9200
9595	10001	11211	16992	16993	44818	53413			

**Web Technologies**

```

220 ftp server is running
230 Login successful.
214 The following commands are recognized:
ABOR ALLO APPE CWD PWD DELE EPRT EPSV
FEAT HELP LIST MDTM MFMT MKD MLSD MLST
MODE NLST NOOP OPTS PASS PASV PORT PWD
QUIT REIN REST RETR RMD SITE TDE
SITE SMC2 STOU STRU SYST TYPE USER
XCUP XRD XWD XWD
214 Help command successful.
211 Features supported:
EPRT
EPSV
...

```

## Locate a device of interest

**Ads - Shop siemens simatic s7-200**

Siemens   6ES7214-... <b>\$350.00</b> Refurbished Classic Auto...	SIEMENS 6ES7216-... <b>\$551.00</b> Refurbished Radwell.com	Siemens S7- 200 Cpu 224... <b>\$630.00</b> Used Texnite	Siemens CPU 1212 FC ... <b>\$464.78</b> automation2... Free shipping	Siemens 6ES7 214-1BD22-... <b>\$350.00</b> Williams Aut... Free shipping

[https://cache.industry.siemens.com/files/att\\_22063.pdf](https://cache.industry.siemens.com/files/att_22063.pdf)

**S7-200 Programmable Controller - Siemens Industry Online ...**

S7-200. Programmable Controller. System Manual. SIMATIC. Edition 08/2008. A5E00307987-04. This manual has the order number: 6ES7298-8FA24-8BH0 ...  
554 pages

**People also ask :**

- What is PLC S7-200?
- How do I program my Siemens PLC S7-200?

The screenshot shows a web browser window with the URL <https://us-cert.cisa.gov/ics/advisories/icfa-19-318-02>. The page is titled "Siemens S7-1200 and S7-200 SMART CPUs (Update B)". It features the CISA logo and navigation links for Alerts and Tips, Resources, and Industrial Control Systems. A search bar and "Services" and "Report" buttons are also present. The main content area includes a "Legal Notice" section and two sections of executive summary and update information.

**Legal Notice**

All information products included in <https://us-cert.cisa.gov/ics> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <https://us-cert.cisa.gov/tlp>.

**1. EXECUTIVE SUMMARY**

- **CVSS v3 6.8**
- **ATTENTION:** Low skill level to exploit
- **Vendor:** Siemens
- **Equipment:** S7-1200 CPU family (including SIMATIC variants); S7-200 SMART CPU family
- **Vulnerability:** Exposed Dangerous Method or Function

**2. UPDATE INFORMATION**

## Search for specific devices and vulnerabilities