Question 1

[REDACTED], so I just went there after hours to log onto [REDACTED] computer. Unfortunately, the agency moved locations recently and all employees are now using Macs. This would cause some problems for me when trying to figure out how to run the scan because I ran some test scans at home, but I use Windows and am not really used to macOS.

Moving on, I just downloaded nmap 7.95 for Mac and tried to run Zenmap. The problem is, Zenmap would not run when clicking on it in the location where it is installed. It showed that it was running on the taskbar, but it would simply not show the interface of Zenmap. I found that this is apparently a common problem when trying to run Zenmap on a Mac in the way I did. Regardless, I thought the only way I could complete the scan was through the terminal using the sudo command. While running the scan through the terminal, I found out that you *can* reliably open Zenmap on a Mac. All I had to do was use the terminal and enter the file path of Zenmap to run it. This did work for me, at this point I could run the scan on the network.

In the beginning, I chose to do the TCP SYN scan, I added in the -O to get the operating systems, and the network range, which was just the [REDACTED]. The scan took around 45 minutes, which was a bit strange to me. The agency is not a huge business by any means, and the same scan on my home network was super quick. Either way, just for comparison, I ran the -T4 -F scan while still using the same network range and OS retrieval commands. This scan only took 39.4 seconds, and from looking at the results, it accomplished the same things as the more thorough scan. At this point, I was far more inclined to use the result of the quick scan because after running the -sS one, I tried to put Zenmap into full-screen to copy my results and take

screenshots of everything else, and the program crashed. Now knowing that Zenmap does not work well with full-screen and how the results between the two scans I did are seemingly negligible, I just opened up Zenmap again and ran the quick scan.

Now, I will talk about how my nmap command and scan worked. -T4 sets the speed of the scan to aggressive. This specific speed setting is best in my opinion as it does not sacrifice much accuracy and still speeds up scan times exponentially. -F puts the scan in fast mode that tells nmap to scan fewer ports than default. Instead of all the 1,000 most common ports, it just scans the top 100. -O enables operating system detection that tells nmap to send a series of TCP and UDP packets to the target and analyzes the responses to hopefully determine the OS running on any device. Finally, [REDACTED].

Question 2

Scan Details

- **Command Used**: nmap -T4 -O -F [REDACTED]
- **Start Time**: Sun Jul 21 20:17:20 2024
- **Nmap Version**: 7.95
- **Scan Type**: SYN scan on TCP ports

Hosts Scanned

1. Router [REDACTED]

- **Host Status**: Up
- **Latency**: 0.0041s
- **Open Ports**:
    - 53/tcp (domain)
    - 80/tcp (http)
    - 111/tcp (rpcbind)

    - 443/tcp (https)
    - 2049/tcp (nfs)
    - 5000/tcp (upnp)
- **MAC Address**: [REDACTED]
- **OS Details**: OpenWrt 21.02 (Linux 5.4)

2. Xerox Printer [REDACTED]

- **Host Status**: Up
- **Latency**: 0.0047s
- **Open Ports**:
    - 80/tcp (http)
    - 443/tcp (https)
    - 515/tcp (printer)
    - 631/tcp (ipp)
    - 9100/tcp (jetdirect)
- **MAC Address**: [REDACTED]

(Xerox)

- **OS Details**: No exact match; various Linux versions and embedded systems detected

3. [REDACTED] iMac [REDACTED]

- **Host Status**: Up
- **Latency**: 0.099s
- **Open Ports**: None (all ports filtered)
- **MAC Address**: [REDACTED]

(Apple)

- **OS Details**: Possible embedded systems like Dell PowerConnect switch or Grandstream VoIP phones

4. iMac-2 [REDACTED]

- **Host Status**: Up
- **Latency**: 0.099s
- **Open Ports**: None (all ports filtered)
- **MAC Address**: [REDACTED]

(Apple)

- **OS Details**: Like [REDACTED] iMac, embedded systems detected

5. iMac [REDACTED]

- **Host Status**: Up
- **Latency**: 0.0066s
- **Open Ports**:
    - 88/tcp (kerberos-sec)
    - 445/tcp (microsoft-ds)
    - 5000/tcp (upnp)
- **MAC Address**: [REDACTED]
- **OS Details**: Apple macOS 11 (Big Sur) - 13 (Ventura)

6. iMac-3 [REDACTED]

- **Host Status**: Up
- **Latency**: 0.00012s
- **Open Ports**:
    - 5000/tcp (upnp)
- **MAC Address**: Not listed
- **OS Details**: Apple macOS 12 (Monterey)

Topology View

[REDACTED]

Summary

The nmap scan identified 6 hosts on the network with varying levels of detail:

- The router is running OpenWrt and has several open ports including HTTP, HTTPS, and NFS.
- A Xerox printer with open ports for web interfaces and printing services.
- Multiple iMacs with some having filtered ports and others showing specific open ports like Kerberos, Microsoft DS, and UPnP.

Usage

The nmap scan I did can be used to enhance network security by:

- Closing ports that are unnecessary.
- Restricting access through firewalls.
- Ensuring ports are configured securely.
- Ensuring there are no unauthorized devices on the network.
- Updating outdated software.

Question 3

Before performing the nmap scan and using Zenmap in general, the most networking experience I had was changing some settings on my router at home. After all the scans I did in Zenmap and specifically, the one I did in a workplace, I learned a multitude of things. I learned how networks are structured, how devices and services on a network are connected, and a little bit about how to identify possible weak points in a network. The hands-on experience with Zenmap provided me with a deeper understanding of network scanning tools. Additionally, I learned to how configure and execute different types of scans and how to interpret those results. The topology view in Zenmap was especially useful for learning about how devices are

connected and the purpose of each one by using the legend to see what all the symbols represent. Finally, I learned about different network protocols (mostly TCP and UDP), along with their roles in communication between devices. Understanding how different protocols operate along with the ports they use has helped me recognize the services running on the network. As with most things, learning about and getting experience with networking feels like something that the more you know about it, the more you know that you do not know.