**What did you do:**

To conduct the network mapping on a Mac, I followed a similar approach using NMAP. After obtaining permission from the organization, I visited the official NMAP website and downloaded version 7.94 specifically designed for macOS. I then proceeded to install and set up the software on my Mac computer.

Once NMAP was successfully installed, I opened a Terminal window to access the command-line interface. From there, I executed the necessary commands to perform network scanning. Using a combination of scanning techniques and options provided by NMAP, I gathered information about the network infrastructure. This involved conducting host discovery scans, port scanning, and utilizing aggressive scanning options to identify potential vulnerabilities.

To analyze the network and its attack surface, I used a combination of network scanning and enumeration techniques. I started by scanning the IP address range of the specific locations, namely the Amarillo airport (192.168.1.214), Southwest in-flight WIFI (10.188.61.38), and my friend's house in Dallas (192.168.1.49). During the scanning process, I employed various tools and techniques to discover active hosts, open ports, and services running on those hosts.

After the scanning phase, I performed enumeration to gather more detailed information about the identified hosts and services. This involved querying the open ports to determine the specific protocols and applications running on each host. I also gathered information about the operating systems, software versions, and other relevant details to assess the potential vulnerabilities and attack vectors.

**What are the results:**

During the network mapping exercise, I discovered several components and protocols within the organization's network. The components consisted of various devices such as desktop computers, laptops, servers, routers, switches, printers, and IoT devices. I also observed the presence of mobile devices like smartphones and tablets, which were connected to the network.

In terms of protocols, the network utilized common protocols such as TCP/IP, DHCP, DNS, HTTP, HTTPS, SSH, FTP, and SNMP. These protocols facilitated communication and data transfer across the network infrastructure.

The network components and protocols used in the mentioned locations may vary, but they typically include a mix of wired and wireless technologies. Here's an analysis of the components and protocols that might be present: **Amarillo airport** **(192.168.1.214)**: The airport is likely to have a combination of wired infrastructure, such as routers, switches, and firewalls, to manage the network traffic. Wireless access points (APs) provide connectivity for passengers. The protocols used may include TCP/IP for data transmission, DHCP for IP address allocation, DNS for domain name resolution, and HTTP/HTTPS for web browsing. **Southwest flight WIFI (10.188.61.38)**: In-flight WIFI services on airplanes often utilize satellite-based communication to connect to the internet. Passengers may connect through onboard wireless networks, and the network protocols used are like those in other WIFI environments. **My friend's house in Dallas (192.168.1.49)**: Residential networks typically consist of a router connected to an internet service provider (ISP). WIFI access points allow wireless connectivity within the house. Common protocols include TCP/IP, DHCP, DNS, and various application-layer protocols for online services.

Analyzing the attack surface of the network, I considered different areas that could be vulnerable to cybersecurity attacks. This included mobile devices, which could be targeted through malicious apps or network exploits. Bluetooth connections posed risks of unauthorized access or device impersonation if not properly secured. IoT devices, if not adequately protected, could serve as entry points for attackers to gain access to the network. Wireless networks, if not encrypted or with weak security configurations, could be susceptible to unauthorized access and eavesdropping. Additionally, cloud components and protocols could introduce security challenges if not effectively managed, potentially leading to data breaches or unauthorized access.

The attack surface of the network is the total number of potential entry points or vulnerabilities that could be exploited by a cyber attacker. In the mentioned locations, the attack surface may include the following components: **WIFI networks**: Unsecured or weakly secured WIFI networks are vulnerable to attacks like man-in-the-middle (MITM), rogue access points, and eavesdropping. Attackers may attempt to intercept sensitive data or inject malicious content into the network. **Network devices**: Routers, switches, and firewalls could be targeted for exploitation if they have known vulnerabilities or default credentials. Unauthorized access to these devices may enable attackers to manipulate network traffic or gain control over the network. **Internet-connected devices**: If any IoT devices are present, they may be susceptible to cyber-attacks if not properly secured. IoT devices are notorious for having weak security measures, making them attractive targets for attackers. **Cloud services**: If any cloud services are used in the network, misconfigurations or weak authentication measures could expose sensitive data to unauthorized access.

**What did you learn:**

This assignment provided valuable insights into the intricacies of digital networks and the concept of the attack surface. I learned how to effectively use NMAP to map and analyze networks, allowing me to understand the network topology, identify devices, and assess potential security risks.

One significant lesson learned was the importance of considering all aspects of the network when assessing the attack surface. This involved not only traditional wired components but also mobile, Bluetooth, IoT, wireless, and cloud components. Each of these areas presented unique security challenges that required careful consideration and appropriate security measures.

Furthermore, I realized the significance of continuous monitoring and regular security assessments to ensure the network remains protected against evolving cybersecurity threats. By identifying vulnerabilities and implementing necessary security measures, organizations can enhance their overall security posture and mitigate potential risks.

In the future, the knowledge gained from this assignment can be applied to strengthen network security practices. By identifying and addressing vulnerabilities, organizations can proactively protect their networks and sensitive data. Additionally, understanding the attack surface allows for better resource allocation and prioritization of security efforts to maximize protection.

For the organization, the insights from this network mapping exercise can guide their cybersecurity strategy. By understanding the components, protocols, and potential vulnerabilities, they can implement appropriate security controls and measures to mitigate risks. This will help in safeguarding their network infrastructure, maintaining data confidentiality, and ensuring the integrity and availability of critical systems and information.