**What did you do?**

For this assignment, I conducted vulnerability scans on my network using two web software tools: Shields Up and Nessus.

a) Shields Up:

I visited the Shields Up website (https://www.grc.com/x/ne.dll?bh0bkyd2) and ran a vulnerability scan on my home network. I clicked on "Proceed" and selected both the "Common Ports" and "All Service Ports" options to perform two port scans. Shields Up scanned my network's IP address for open ports and provided the results.

b) Nessus:

I downloaded the Nessus Essentials, a free limited-capability version for students, from the official Tenable website (https://www.tenable.com/products/nessus/nessus-essentials). After installing Nessus, I obtained permission from my organization to use it for vulnerability scanning. I ran Nessus to scan up to 16 IP addresses, including my home network's IP address. The scan performed a comprehensive vulnerability assessment on the selected IP addresses.

After completing both scans, I collected the results from Shields Up and Nessus and saved them in PDF format for analysis.

**What are the results?**

a) Shields Up:

The Shields Up scan revealed that my network had two closed ports. This means that the specified ports were detected but were closed to incoming connections. The closed ports indicate a reduced attack surface, which is a positive sign for network security.

b) Nessus:

The Nessus scan provided a detailed report of 48 vulnerabilities identified in my network. The report categorized the vulnerabilities based on their severity level: Critical, High, Medium, Low, and Informational. The critical and high-severity vulnerabilities require immediate attention and remediation to prevent potential cyber threats and security breaches. The medium and low-severity vulnerabilities should also be addressed to enhance overall network security.

**What did you learn?**

Through this assignment, I learned several important aspects of vulnerability scanning and network security: The significance of conducting regular vulnerability scans to identify potential weaknesses and security risks in a network. The importance of obtaining permission before performing any security-related scans on an organization's network to ensure compliance with policies and regulations. The role of web software tools like Shields Up and Nessus in providing comprehensive vulnerability assessments and identifying potential threats and vulnerabilities.

The criticality of addressing critical and high-severity vulnerabilities promptly to mitigate the risk of cyber attacks and data breaches. The value of reducing the attack surface by closing unnecessary or vulnerable ports, thereby minimizing the network's exposure to potential threats. The importance of continuous monitoring and remediation to maintain a robust and secure network infrastructure.

In the future, vulnerability scanning can be a valuable tool to ensure the ongoing security of the organization's network. It helps in proactively identifying vulnerabilities and taking corrective actions to strengthen the network's defenses against cyber threats. Additionally, regular vulnerability scanning can be integrated into the organization's cybersecurity strategy to enhance overall security posture and protect sensitive data and systems from potential attacks.