Exercise: Evaluating threats

Introduction

By now, you know that it's critical for businesses to protect the data they produce and collect from potential threats. In this exercise, you will assess and rate a security vulnerability using the Common Vulnerability Scoring System (CVSS).

Case study

Sam's Scoops' unusual ice cream recipes are a big part of their appeal to customers. These formulations are safeguarded within a Microsoft SQL Database and further protected with their custom-built firewall. However, their formulations are at risk because of a critical vulnerability in the firewall that several cybersecurity team members have confirmed exists. This vulnerability offers potential remote entry without requiring physical access or pre-established authentication. To make matters worse, it also doesn't require user interaction, such as clicking on malicious links or files, so it's quite simple to exploit. And, unfortunately, easy-to-use code can be used to exploit the firewall vulnerability. Furthermore, there are no known patches or workarounds at this point.
Essentially, this vulnerability could permit unauthorized access to breach the firewall, compromising Sam's Scoops ice cream recipes. Also, gaining access via the firewall poses a further chain reaction risk to interconnected systems and sensitive data. The unauthorized access the firewall vulnerability offers to a potential attacker exposes sensitive information. It also allows data tampering or even disrupting services that rely on the system.

Instructions

Your task is to assess and rate the severity of this firewall vulnerability using the CVSS via the NIST-provided CVSS Calculator.

Step 1: Access the CVSS Calculator

Visit the NIST National Vulnerability Database (NVD) website to access the CVSS Calculator. Before proceeding, it's recommended that you review the *CVSS Calculator cheat sheet*, which provides comprehensive details on how to utilize this calculator effectively. For additional guidance on how to use the CVSS calculator consult the CVSS user guide.
Note: The tool will display a " NA" (not applicable) notification while the metrics are still blank. It only responds with a value once you filled in the metrics.

Step 2: Calculate the CVSS score

To calculate the CVSS score, consider the specific metrics related to the vulnerability. The Base Score Metrics are required for the calculator to determine a CVSS score, so you must complete these. Optionally, you can customize the Base Score with the Temporal and Environmental Metrics if you feel up to the challenge.

To calculate the score, select the desired option for each metric in the CVSS Calculator. The tool will automatically calculate the score. Ensure you input the required information to derive an accurate CVSS score.

Base Score Metrics

- Attack Vector (AV)
- Attack Complexity (AC)
- Privileges Required (PR)
- User Interaction (UI)
- Scope (S)
- Confidentiality Impact (C)
- Integrity Impact (I)
- Availability Impact (A)

Temporal Score Metrics

- Exploit Code Maturity (E)
- Remediation Level (RL)
- Report Confidence (RC)

Environmental Score Metrics

- Modified Attack Vector (MAV)
- Modified Attack Complexity (MAC)
- Modified Privileges Required (MPR)
- Modified User Interaction (MUI)
- Modified Scope (MS)
- Modified Confidentiality Impact (MC)
- Modified Integrity Impact (MI)
- Modified Availability Impact (MA)
- Confidentiality Requirement (CR)
- Integrity Requirement (IR)
- Availability Requirement (AR)

Step 3: Interpret the score

The CVSS Calculator will generate a numerical score between 0 and 10, representing the overall severity of the vulnerability. Interpret the CVSS score according to the provided severity levels:

Severity level	**Score**
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-8.9

Critical	9.0-10.0

Step 4: Mitigation and remediation

List potential mitigation and remediation measures to address the vulnerability.

Conclusion

Remember, assessing and rating potential threats is a vital practice in cybersecurity. This exercise helped you to assess and rate a firewall vulnerability using the Common Vulnerability Scoring