Lab 1 (Task 2)

The following table contains vector string metric values for TLS Version 1.0 protocol detection and SSL version 2 and 3 protocol detection.

Table 1: Vector Metrics

Criteria:	**TLS Version 1.0 Protocol Detection**	**SSL Version 2 and 3 Protocol Detection**
Attack Vector	Network (0.85)	Network (0.85)
Attack Complexity	High (0.44)	Low (0.77)
Privileges Required	None (0.85)	None (0.85)
User Interaction	None (0.85)	None (0.85)
Confidentiality	High (0.56)	High (0.56)
Integrity	Low (0.22)	High (0.56)
Availability	None (0)	High (0.56)
Scope	Unchanged	Unchanged

Calculations

TLS Version 1.0 Protocol Detection:

Vector = CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N

ISS = 1 - [(1 - 0.56) * (1 - 0.22) * (1 - 0)] = 0.6568

Impact = 6.42 * 0.6568 = 4.216656

Exploitability = 8.22 * 0.85 * 0.44 * 0.85 * 0.85 = 2.2211673

BaseScore = Roundup (Minimum [(4.216656 + 2.2211673), 10] = **6.5**

SSL Version 2 and 3 Protocol Detection:

Vector = CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

ISS = 1 - [(1 - 0.56) * (1 - 0.56) * (1 - 0.56)] = 0.914816

Impact = 6.42 * 0.914816 = 5.87311872

Exploitability = 8.22 * 0.85 * 0.77 * 0.85 * 0.85 = 3.887042775

BaseScore = Roundup (Minimum [(5.87311872 + 3.887042775), 10] = **9.8**

Rational

The TLS Version 1.0 protocol detection and the SSL version 2 and 3 protocol detection CVSS v3.1 Base Scores were obtained from the metrics associated with each vulnerability's vector string in Table 1. Each Base Score was calculated by inputting the respective vector string numerical metrics into the Base Score Equation found in the CVSS Specification Document. The Base Scores consist of the Impact Sub-Score (ISS), Impact, Exploitability, and Scope. The ISS is calculated using each vulnerability's CIA; the Impact is determined by multiplying the constant value 6.42 by the ISS; and the Exploitability is found by multiplying the constant value 8.22 by Attack Vector, Attack Complexity, Privileges Required, and User Interaction.

Both vulnerabilities in Table 1 shared Base vector metrics under Attack Vector (Network), Privileges Required (None), User Interaction (None), Confidentiality (High), and Scope (Unchanged).

Attack Vector (Network) suggests that both vulnerabilities are susceptible to being exploited remotely by an attacker, raising the Base Scores. Privileges Required (None) suggests that an attacker does not need authorization to the system prior to causing damage, raising the Base Scores. User Interaction (None) suggests that a user does not need to perform an action on the system to initiate an attack, raising the Base Scores. Confidentiality (High) suggests that there is risk for widespread exposure of restricted information within the component during an attack, raising the Base Score. Since the Scope remains unchanged in both instances, only one security authority would be impacted by either of the vulnerabilities being exploited, lowering the Base Scores.

The vulnerabilities in Table 1 differ on Attack Complexity, Integrity, and Availability. TLS Version 1.0 protocol detection has Attack Complexity (High), Integrity (Low), and Availability (None). SSL Version 2 and 3 protocol detection has Attack Complexity (Low), Integrity (High), and Availability (High).

Attack Complexity (High) indicates that the attacker would have to stage the attack ahead of time and would be dependent on the right conditions. Attack Complexity (Low) indicates that the attacker would not require the right conditions and could conduct their attack at any time. Attack Complexity (High) lowers the Base Score while Attack Complexity (Low) raises the Base Score.

Integrity (Low) indicates that an attacker could make changes to component data, but there would not be serious consequences as a result. Integrity (High) indicates that an attacker would have the capability of making changes to all protected data on the component, resulting in major consequences. Integrity (Low) lowers the Base Score while Integrity (High) raises the Base Score.

Availability (None) signals that an attack would not impact the service availability or performance of this component. Availability (High) signals that an attacker could deny access to the service and cause major disruption. Availability (None) has no impact on the Base Score while Availability (High) raises the Base Score.