**Week 2 Written Assignment**

Ayomide Stephen Oyedele

EC-Council University

**CIS 300: Fundamentals of Information Systems Security**

Dr. Franklin Orellana

January 16, 2024

The Window of Vulnerability (WoV) is the time span during which a system or network is exposed to potential security threats due to the existence of a known vulnerability before a patch or solution is implemented. The calculation involves considering the time from the identification of the vulnerability to the successful application of the patch.

In this scenario given in this Weeks Written Assignment, the steps to calculate the Window of Vulnerability for the SMB server are as follows:

1. **Identification of Vulnerability**: Vulnerability identified the previous day.

2. **Availability of Patch**: Patch available within three days.

3. **Time Required for Patch Installation**: LAN administrator needs at least one week.

Calculation of the Window of Vulnerability:

WoV = {(**Time to patch availability**)} + {(**Time for patch installation**)}

WoV = **3** {days} + **7** {days}

WoV = **10** {days}

Therefore, the **Window of Vulnerability for the SMB server is 10 days**. During this period, the server remains exposed to potential security threats until the patch is successfully installed.

Certainly, to enhance the robustness and professionalism of the scenario and calculation, we can consider incorporating the following aspects:

**1. Risk Assessment**: Conduct a brief risk assessment to evaluate the potential impact of the vulnerability. Assess the likelihood and severity of exploitation during the Window of Vulnerability.

**2. Communication Plan**: Include details about how the LAN administrator will communicate the situation to relevant stakeholders. This involves informing users about potential disruptions, setting expectations, and providing guidance on temporary measures.

**3. Mitigation Measures**: Discuss any interim measures or compensating controls that can be implemented to reduce the risk during the Window of Vulnerability. This might include firewall rules, network segmentation, or temporary access restrictions.

**4. Contingency Planning**: Describe contingency plans in case the patching process encounters unexpected issues or delays. Having a well-defined plan for contingencies adds a layer of preparedness.

**5. Coordination with Stakeholders**: Specify the coordination efforts with different groups affected by vulnerability. This could involve collaboration with IT teams, department heads, and end-users to ensure a smooth patch deployment process.

**6. Post-Patching Verification**: Include a step for post-patching verification to confirm the successful implementation of the patch and to ensure that the SMB server is secure. This verification process adds a layer of quality assurance.

**7. Documentation**: Emphasize the importance of documentation throughout the process. This includes documenting the vulnerability, the patching procedure, any issues encountered, and the verification steps taken. Well-documented processes contribute to a professional approach.

**8. Continuous Monitoring**: Highlight the need for continuous monitoring during the Window of Vulnerability to detect any signs of potential exploitation. This could involve enhanced log monitoring, intrusion detection systems, or other security measures.

By incorporating these aspects, the calculation not only becomes more robust but also reflects a comprehensive and **professional approach to handling security vulnerabilities within a network environment.**