Vulnerability Response
Student Name: Tania Diaz
Date: 11/23/2025
Chapter: 13

1.- What would be your response to a known critical vulnerability in your network? Apply your current understanding of vulnerabilities and what it could do to your environment. Explain how you would handle this situation and what might happen if you did not get ahead of these vulnerabilities.

If a critical vulnerability is discovered in my network, my first step would be to identify and understand it. I would check vendor alerts, official CVE reports, and internal security scans to determine which systems are affected and how severe the impact could be.

Next, I would contain the vulnerability to prevent it from being exploited. This could involve isolating affected systems, disabling vulnerable services, or blocking specific network traffic temporarily.

The third step is remediation. I would apply vendor-released patches or updates immediately. If no patch is available, I would implement mitigation measures, such as adjusting system configurations, restricting network access, or segmenting vulnerable systems.

After remediation, I would verify and monitor the network to ensure the vulnerability has been resolved. Continuous monitoring would help detect any signs of attempted exploitation or unusual activity.

Finally, I would document the incident and communicate with stakeholders. Clear records of the vulnerability, actions taken, and lessons learned help improve future responses and maintain accountability.

Ignoring a critical vulnerability could lead to serious consequences, including unauthorized access, data breaches, ransomware attacks, or system downtime. Proactive and structured response ensures that risks are minimized and the network remains secure.