

IT 113-Information Assurance and Security 2

Quiz

Name: Heart M. Cabillo

Section: *QQR1*

Program: BSIT

Essay: Answer the following based on the video provided. (50 points)

1. What is the importance of Vulnerability Assessment in a computing infrastructure?

Answer: Conducting a vulnerability assessment is extremely important in computing infrastructure as it helps to identify any potential weaknesses or vulnerabilities in the system. Addressing these vulnerabilities before they can be exploited by attackers helps to keep the system secure. Regular vulnerability assessments are essential in ensuring that the system remains protected from cyber threats. Moreover, protecting against cyber attacks and vulnerability assessment plays a critical role in maintaining the cybersecurity of any organization's computing infrastructure. By regularly conducting vulnerability assessments and taking necessary measures to address any identified vulnerabilities, organizations can ensure that their system remains secure and compliant with relevant regulations.

2. What are the drawbacks of Manual vulnerability assessment?

Answer: The drawbacks of manual vulnerability assessment is that it consumes a lot of time, not consistent, limited scope and it is costly. It is costly because it requires trained personnel to accomplish the assesment.

3. What are the advantages of fully automated vulnerability assessment?

Answer: The advantages of fully automated vulnerability assessment includes speed, efficiency, accuracy, consistency, and it is cost-effective than manual, as automated requires fewer resources. And it helps to improve the security posture of an organization.

4. How machine learning techniques can help in vulnerabilities classification?

Answer: Machine learning can aid in the categorization of vulnerabilities by educating models on vast datasets of identified vulnerabilities and their associated classifications. These models can recognize similarities and differences between various types of vulnerabilities by analyzing features and patterns of known vulnerabilities. Specific machine learning techniques that can be used for this purpose include supervised learning, unsupervised learning, and deep learning. Supervised learning involves training a model on labeled data, while unsupervised learning entails discovering patterns and groupings in unlabeled datasets of vulnerabilities.

5. What is the significance of vulnerability assessment in the following:

1. Confidentiality

- Vulnerability assessment assists in identifying weaknesses in the system that can be exploited by attackers to gain access to confidential information without authorization. The absence of vulnerability assessment puts confidential information at risk of unauthorized disclosure, resulting in potential financial losses and reputational damage for the organization.

2. Availability

- The process of vulnerability assessment aids in the detection of possible system weaknesses and vulnerabilities that could result in service disruptions or unavailability. Regularly conducting these assessments allows organizations to take preventive measures to address such vulnerabilities before cyber attackers exploit them. This ensures that critical systems and services remain available to authorized users, reducing the impact of potential attacks and sustaining the organization's business operations without interruptions.

3. Integrity of organization's and user's private data

- Conducting regular vulnerability assessments can help organizations identify possible security weaknesses that may result in unauthorized access, modification, or destruction of sensitive information. Addressing these vulnerabilities in a timely manner can ensure that the organization's data remains protected against cyber threats, thus minimizing the risk of data breaches, identity theft, and other types of cyber attacks that could severely compromise the integrity and security of private data belonging to both the organization and its users.