COMP3052 Computer Security

Session 03: Foundations of Security

Videoclip: DDoS Attack Explained

https://www.youtube.com/watch?v=ilhGh9CEIwM

Videoclip: Smurf Attack Explained

https://www.youtube.com/watch?v=u_75dJCQFGg&t=57s

1. What is the CIA triad?

(A) Ongoing validation processes involving all employees in an organization

(B) A mandatory security framework involving the selection of appropriate controls

(C) A foundational security model used to set up security policies and systems

(D) A set of security controls used to update systems and networks

2. Which element of the CIA triad specifies that only authorized users can access specific information?

(A) Confirmation

(B) Confidentiality

(C) Integrity

(D) Access

Reference: Test your knowledge: The CIA triad Quiz Answers

https://niyander.com/test-your-knowledge-the-cia-triad-quiz-answers/

Reference: What is the CIA Triad?

https://www.youtube.com/watch?v=kPPFNrlN3zo

1. What is the CIA triad?

(A) Ongoing validation processes involving all employees in an organization

(B) A mandatory security framework involving the selection of appropriate controls

(C) A foundational security model used to set up security policies and systems

(D) A set of security controls used to update systems and networks

Answer: The CIA triad is a foundational security model used to set up security policies and systems. The core principles of the model are confidentiality, integrity, and availability.

2. Which element of the CIA triad specifies that only authorized users can access specific information?

(A) Confirmation

(B) Confidentiality

(C) Integrity

(D) Access

Answer: Confidentiality specifies that only authorized users can access specific information.

Reference: Test your knowledge: The CIA triad Quiz Answers

https://niyander.com/test-your-knowledge-the-cia-triad-quiz-answers/

Reference: What is the CIA Triad?

https://www.youtube.com/watch?v=kPPFNrlN3zo

3. A security analyst discovers that certain data is inaccessible to authorized users, which is preventing these employees from doing their jobs efficiently. The analyst works to fix the application involved in order to allow for timely and reliable access. Which element of the CIA triad does this scenario describe?

(A) Availability

(B) Capacity

(C) Applicability

(D) Integrity

4. According to the CIA triad, _____ refers to ensuring that an organization's data is verifiably correct, authentic, and reliable.

(A) Availability

(B) Accuracy

(C) Integrity

(D) Credibility

Reference: Test your knowledge: The CIA triad Quiz Answers

https://niyander.com/test-your-knowledge-the-cia-triad-quiz-answers/

3. A security analyst discovers that certain data is inaccessible to authorized users, which is preventing these employees from doing their jobs efficiently. The analyst works to fix the application involved in order to allow for timely and reliable access. Which element of the CIA triad does this scenario describe?

(A) Availability

(B) Capacity

(C) Applicability

(D) Integrity

Answer: This scenario describes availability. Availability specifies that data is accessible to authorized users.

4. According to the CIA triad, _____ refers to ensuring that an organization's data is verifiably correct, authentic, and reliable.

(A) Availability

(B) Accuracy

(C) Integrity

(D) Credibility

Answer: According to the CIA triad, integrity refers to ensuring that an organization's data is verifiably correct, authentic, and reliable.

Reference: Test your knowledge: The CIA triad Quiz Answers

https://niyander.com/test-your-knowledge-the-cia-triad-quiz-answers/

5. Which of the following statements accurately describes a Smurf attack?
   (A) A DoS attack that is caused when an attacker pings a system by sending it oversized ICMP packet that is bigger than the maximum size
   (B) A network attack performed when an attacker sniffs an authorized user's IP address and floods it with packets
   (C) A DoS attack performed by an attacker repeatedly sending ICMP packets to a network server
   (D) A network attack performed when an attacker intercepts a data packet in transit and delays it or repeats it at another time

Reference: Course 3 – Connect and protect: networks and network security

https://quiztudy.com/coursera-google-courses/google-cybersecurity/secure-against-network-intrusions-course-3-module-3/

Reference: Smurf attack: What it is and how it works

https://nordvpn.com/blog/what-is-smurf-attack/

5. Which of the following statements accurately describes a Smurf attack?

   (A) A DoS attack that is caused when an attacker pings a system by sending it oversized ICMP packet that is bigger than the maximum size

   (B) A network attack performed when an attacker sniffs an authorized user's IP address and floods it with packets

   (C) A DoS attack performed by an attacker repeatedly sending ICMP packets to a network server

   (D) A network attack performed when an attacker intercepts a data packet in transit and delays it or repeats it at another time

Explanation: A Smurf attack is a network attack performed when an attacker sniffs an unauthorized user's IP address and floods it with packets. It is a combination of a DDoS attack and an IP Spoofing attack.

Reference: Course 3 – Connect and protect: networks and network security

https://quiztudy.com/coursera-google-courses/google-cybersecurity/secure-against-network-intrusions-course-3-module-3/

Reference: Smurf attack: What it is and how it works

https://nordvpn.com/blog/what-is-smurf-attack/

6. What term means that a user cannot deny a specific action because there is positive proof that he or she performed it?

   (A) Accountability

   (B) Auditing

   (C) Nonrepudiation

   (D) Validation

Reference: Identity and Access Management

https://www.pearsonitcertification.com/articles/article.aspx?p=2738310

6. What term means that a user cannot deny a specific action because there is positive proof that he or she performed it?

   (A) Accountability

   (B) Auditing

   (C) Nonrepudiation

   (D) Validation

Reference: Identity and Access Management

https://www.pearsonitcertification.com/articles/article.aspx?p=2738310

7. What is the difference between the security and safety aspects of a system? Explain with an example.

Answer: Safety in the context of a nuclear power plant disaster refers to the impact of the event on the environment and human health. The explosion and subsequent release of radioactive material from the nuclear power plant has devastating consequences for the surrounding area. The safety concerns revolve around the radiation exposure to the population, the contamination of soil and water, and the long-term health effects on individuals.

Security, on the other hand, refers to the system's failures or vulnerabilities that may lead to a disaster. There may be several security failures that may contribute to the accident. These include design flaws in the reactor, inadequate operating protocols, human errors, and a lack of proper training for the operators. The security failures in this case may be the underlying causes that may allow the disaster to occur.

So, in summary, safety concerns the impact on the environment and human health following a disaster, while security focuses on the failures within the system that may lead to a disaster.