An toan thong tin_ Nhom 03

Started on	Tuesday, 16 June 2020, 12:01 PM
State	Finished
Completed on	Tuesday, 16 June 2020, 12:23 PM
Time taken	21 mins 43 secs
Marks	28.00/28.00
Grade	**10.00** out of 10.00 (**100**%)

Question 1

Correct

Mark 1.00 out of 1.00

Which of the following attacks specifically impact data availability?

Select one:

○ a. MITM

● b. DDoS

○ c. Rootkit

○ d. Trojan

Your answer is correct.

The correct answer is: DDoS

Question 2

Correct

Mark 1.00 out of 1.00

Which of the following is not considered a violation of confidentiality?

Select one:

● a. Hardware destruction

○ b. Eavesdropping

○ c. Social engineering

○ d. Stealing passwords

Your answer is correct.

The correct answer is: Hardware destruction

Question 3

Correct

Mark 1.00 out of 1.00

A network administrator has purchased two devices that will act as failovers for each other. Which of the following concepts does this BEST illustrate?

Select one:

● a. Availability Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This strategy allows service to continue uninterrupted until the primary server can be restored. In the case of a network, this means processing switches to another network path in the event of a network failure in the primary path. This means availability

○ b. Integrity

○ c. Confidentiality

○ d. Authentication

Your answer is correct.

The correct answer is: Availability

Question 4

Correct

Mark 1.00 out of 1.00

Which of the following is the BEST reason to provide user awareness and training programs for organizational staff?

Select one:

○ a. To train staff on zero-days

○ b. To detail business impact analyses

● c. To reduce organizational IT risk Ideally, a security awareness training program for the entire organization should cover the following areas:
Importance of security
Responsibilities of people in the organization
Policies and procedures
Usage policies
Account and password-selection criteria
Social engineering prevention
You can accomplish this training either by using internal staff or by hiring outside trainers. This type of training will significantly reduce the organizational IT risk.

○ d. To ensure proper use of social media

Your answer is correct.

The correct answer is: To reduce organizational IT risk

Question 5

Correct

Mark 1.00 out of 1.00

The method to provide end users of IT systems and applications with requirements related to acceptable use, privacy, new threats and trends, and use of social networking is:

Select one:

○ a. Legal compliance training.

● b. Security awareness training. Security awareness and training are critical to the success of a security effort. They include explaining policies, procedures, and current threats to both users and management.

○ c. BYOD security training

○ d. Role-based security training.

Your answer is correct.

The correct answer is: Security awareness training.

Question 6

Correct

Mark 1.00 out of 1.00

Which of the following contains the primary goals and objectives of security?

Select one:

● a. The CIA Triad

○ b. A network’s border perimeter

○ c. A stand-alone system

○ d. The Internet

Your answer is correct.

The correct answer is: The CIA Triad

Question 7

Correct

Mark 1.00 out of 1.00

A web server hosted on the Internet was recently attacked, exploiting a vulnerability in the operating system. The operating system vendor assisted in the incident investigation and verified the vulnerability was not previously known. What type of attack was this?

Select one:

○ a. Denial-of-service

○ b. Botnet

● c. Zero-day exploit

○ d. Distributed denial-of-service

Your answer is correct.

The correct answer is: Zero-day exploit

Question 8

Correct

Mark 1.00 out of 1.00

If a security mechanism offers availability, then it offers a high level of assurance that authorized subjects can ______________________________ the data, objects, and resources.

Select one:

○ a. Control

● b. Access

○ c. Repudiate

○ d. Audit

Your answer is correct.

The correct answer is: Access

Question 9

Correct

Mark 1.00 out of 1.00

Joe has hired several new security administrators and have been explaining the design of the company’s network. He has described the position and descriptions of the company’s firewalls, IDS sensors, antivirus server, DMZs, and HIPS. Which of the following best describes the incorporation of these elements?

Select one:

○ a. Load balancers

○ b. UTM security appliance

○ c. Network segmentation

● d. Defense in depth

Your answer is correct.

The correct answer is: Defense in depth

Question 10

Correct

Mark 1.00 out of 1.00

The internal audit group discovered that unauthorized users are making unapproved changes to various system configuration settings. This issue occurs when previously authorized users transfer from one department to another and maintain the same credentials. Which of the following controls can be implemented to prevent such unauthorized changes in the future?

Select one:

○ a. Group based privileges

○ b. Periodic access review

● c. Least privilege

○ d. Account lockout

Your answer is correct.

The correct answer is: Least privilege

Question 11

Correct

Mark 1.00 out of 1.00

What ensures that the subject of an activity or event cannot deny that the event occurred?

Select one:

● a. Nonrepudiation

○ b. CIA Triad

○ c. Abstraction

○ d. Hash totals

Your answer is correct.

The correct answer is: Nonrepudiation

Question 12

Correct

Mark 1.00 out of 1.00

Several employees clicked on a link in a malicious message that bypassed the spam filter and their PCs were infected with malware as a result. Which of the following BEST prevents this situation from occurring in the future?

Select one:

● a. Security awareness training Security awareness and training include explaining policies, procedures, and current threats to both users and management. A security awareness and training program can do much to assist in your efforts to improve and maintain security. Ideally, a security awareness training program for the entire organization should cover the following areas:
Importance of security
Responsibilities of people in the organization
Policies and procedures
Usage policies
Account and password-selection criteria
Social engineering prevention

○ b. Data loss prevention

○ c. Digital signatures

○ d. Enforcing complex passwords

Your answer is correct.

The correct answer is: Security awareness training

Question 13

Correct

Mark 1.00 out of 1.00

Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts?

Select one:

● a. Integrity Integrity means ensuring that data has not been altered. Hashing and message authentication codes are the most common methods to accomplish this. In addition, ensuring non repudiation via digital signatures supports integrity.

○ b. Confidentiality

○ c. Accounting

○ d. Availability

Your answer is correct.

The correct answer is: Integrity

Question 14

Correct

Mark 1.00 out of 1.00

After an assessment, auditors recommended that an application hosting company should contract with additional data providers for redundant high speed Internet connections. Which of the following is MOST likely the reason for this recommendation? (Select TWO).

Select one or more:

□ a. To allow load balancing for cloud support

☑ b. To allow for business continuity if one provider goes out of business

□ c. To improve intranet communication speeds

☑ d. To eliminate a single point of failure A high-speed internet connection to a second data provider could be used to keep an up-to-date replicate of the main site. In case of problem on the first site, operation can quickly switch to the second site. This eliminates the single point of failure and allows the business to continue uninterrupted on the second site.

□ e. To allow for a hot site in case of disaster

Your answer is correct.

The correct answers are: To allow for business continuity if one provider goes out of business, To eliminate a single point of failure

Question 15

Correct

Mark 1.00 out of 1.00

A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

Select one:

○ a. Integrity

○ b. Confidentiality

● c. Availability Simply making sure that the data and systems are available for authorized users is what availability is all about. Data backups, redundant systems, and disaster recovery plans all support availability. And creating a hot site is about providing availability.

○ d. Succession planning

Your answer is correct.

The correct answer is: Availability

Question 16

Correct

Mark 1.00 out of 1.00

When an employee is to be terminated, which of the following should be done?

Select one:

○ a. Send out a broadcast email informing everyone that a specific employee is to be terminated.

○ b. Wait until you and the employee are the only people remaining in the building before announcing the termination

● c. Disable the employee’s network access just as they are informed of the termination You should remove or disable the employee’s network user account immediately before or at the same time they are informed of their termination.

○ d. Inform the employee a few hours before they are officially terminated.

Your answer is correct.

The correct answer is: Disable the employee’s network access just as they are informed of the termination

Question 17

Correct

Mark 1.00 out of 1.00

Which of the following is a principle of the CIA Triad that means authorized subjects are granted timely and uninterrupted access to objects?

Select one:

○ a. Identification

● b. Availability

○ c. Encryption

○ d. Layering

Your answer is correct.

The correct answer is: Availability

Question 18

Correct

Mark 1.00 out of 1.00

Which of the following is a principle of the CIA Triad that means authorized subjects are granted timely and uninterrupted access to objects?

Select one:

○ a. Encryption

○ b. Layering

● c. Availability

○ d. Identification

Your answer is correct.

The correct answer is: Availability

Question 19

Correct

Mark 1.00 out of 1.00

One of the system administrators at a company is assigned to maintain a secure computer lab. The administrator has rights to configure machines, install software, and perform user account maintenance. However, the administrator cannot add new computers to the domain, because that requires authorization from the Information Assurance Officer. This is an example of which of the following?

Select one:

● a. Least privilege A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more.

○ b. Rule-based access control

○ c. Job rotation

○ d. Mandatory access

Your answer is correct.

The correct answer is: Least privilege

Question 20

Correct

Mark 1.00 out of 1.00

Which of the following is the most important aspect of security?

Select one:

● a. Physical security Physical security is the most important aspect of overall security. Without physical security, none of the other aspects of security are sufficient

○ b. Awareness training

○ c. Intrusion detection

○ d. Logical security

Your answer is correct.

The correct answer is: Physical security

Question 21

Correct

Mark 1.00 out of 1.00

Vulnerabilities and risks are evaluated based on their threats against which of the following?

Select one:

○ a. Data usefulness

○ b. Extent of liability

● c. One or more of the CIA Triad principles

○ d. Due care

Your answer is correct.

The correct answer is: One or more of the CIA Triad principles

Question 22

Correct

Mark 1.00 out of 1.00

Which of the following is the weakest element in any security solution?

Select one:

● a. Humans

○ b. Internet connections

○ c. Software products

○ d. Security policies

Your answer is correct.

The correct answer is: Humans

Question 23

Correct

Mark 1.00 out of 1.00

Which of the following is a management control?

Select one:

○ a. Access Control List (ACL)

● b. Written security policy Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment; and written security policy falls in this category

○ c. SYN attack prevention

○ d. Logon banners

Your answer is correct.

The correct answer is: Written security policy

Question 24

Correct

Mark 1.00 out of 1.00

What security concept encourages administrators to install firewalls, malware scanners, and an IDS on every host?

Select one:

○ a. Network access control (NAC)

○ b. VLAN

● c. Endpoint security

○ d. RADIUS

Your answer is correct.

The correct answer is: Endpoint security

Question 25

Correct

Mark 1.00 out of 1.00

A recent audit has revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the security posture during deployment? (Select TWO).

Select one or more:

□ a. Deploy a honeypot

☑ b. Disable unnecessary services

□ c. Penetration testing

☑ d. Change default passwords

□ e. Implement an application firewall

Your answer is correct.

The correct answers are: Disable unnecessary services, Change default passwords

Question 26

Correct

Mark 1.00 out of 1.00

Which of the following ports will be used for logging into secure websites?

Select one:

○ a. 142

○ b. 110

● c. 443

○ d. 80

Your answer is correct.

The correct answer is: 443

Question 27

Correct

Mark 1.00 out of 1.00

Which of the following ports is used for TELNET by default?

Select one:

○ a. 21

○ b. 22

○ c. 20

● d. 23

Your answer is correct.

The correct answer is: 23

Question 28

Correct

Mark 1.00 out of 1.00

What is encapsulation?

Select one:

○ a. Changing the source and destination addresses of a packet

○ b. Protecting evidence until it has been properly collected

● c. Adding a header and footer to data as it moves down the OSI stack

○ d. Verifying a person’s identity

Your answer is correct.

The correct answer is: Adding a header and footer to data as it moves down the OSI stack

◄ Video - computer security concepts (reference)

Q&A - C1 ►

Return to: Chapter 1. Comp...