Free Questions for 212-82

Shared by Woodard on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Grace, an online shopping freak, has purchased a smart TV using her debit card. During online payment, Grace's browser redirected her from ecommerce website to a third-party payment gateway, where she provided her debit card details and OTP received on her registered mobile phone. After completing the transaction, Grace navigated to her online bank account and verified the current balance in her savings account.

Identify the state of data when it is being processed between the ecommerce website and the payment gateway in the above scenario.

Options:

A- Data at rest
B- Data in inactive
C- Data in transit
D- Data in use

Answer:

C

Explanation:

Data in transit is the state of data when it is being processed between the ecommerce website and the payment gateway in the above scenario. Data in transit is data that is moving from one location to another over a network, such as the internet, a LAN, or a WAN. Data in transit can be vulnerable to interception, modification, or theft by unauthorized parties, so it needs to be protected by encryption, authentication, and other security measures . Data at rest is data that is stored on a device or a media, such as a hard drive, a flash drive, or a cloud storage. Data in active is data that is currently being accessed or modified by an application or a user. Data in use is data that is loaded into the memory of a device or a system for processing or computation.

Question 2

Question Type: MultipleChoice

Elliott, a security professional, was appointed to test a newly developed application deployed over an organizational network using a Bastion host. Elliott initiated the process by configuring

the nonreusable bastion host. He then tested the newly developed application to identify the presence of security flaws that were not yet known; further, he executed services that were not secure. identify the type of bastion host configured by Elliott in the above scenario.

Options:

A- External services hosts
B- Victim machines
C- One-box firewalls
D- Non-routing dual-homed hosts

Answer:

D

Explanation:

Non-routing dual-homed hosts are the type of bastion hosts configured by Elliott in the above scenario. A bastion host is a system or device that is exposed to the public internet and acts as a gateway or a proxy for other systems or networks behind it. A bastion host can be used to provide an additional layer of security and protection for internal systems or networks from external threats and attacks . A bastion host can have different types based on its configuration or functionality. A non-routing dual-homed host is a type of bastion host that has two network interfaces: one connected to the public internet and one connected to the internal network. A non-routing dual-homed host does not allow any direct communication between the two networks and only allows specific services or applications to pass through it . A non-routing dual-homed host can be used to isolate and secure internal systems or networks from external access . In the scenario, Elliott was appointed to test a newly developed application deployed over an organizational network using a bastion host. Elliott initiated the process by configuring the non-reusable bastion host. He then tested the newly developed application to identify the presence of security flaws that were not yet known; further, he executed services that were not secure. This means that he configured a non-routing dual-homed host for this purpose. An external services host is a type of bastion host that provides external services, such as web, email, FTP, etc., to the public internet while protecting internal systems or networks from direct access . A victim machine is not a type of bastion host, but a term that describes a system or device that has been compromised or infected by an attacker or malware . A one-box firewall is not a type of bastion host, but a term that describes a firewall that performs both packet filtering and application proxy functions in one device .

Question 3

Question Type: MultipleChoice

Stella purchased a smartwatch online using her debit card. After making payment for the product through the

payment gateway, she received a transaction text message with a deducted and available balance from her

bank.

Identify the information security element that ensures that Stella's transaction status is immediately reflected in her bank account in this scenario.

Options:

A- Non-repudiation
B- Integrity
C- Availability
D- Confidentiality

Answer:

C

Explanation:

Availability is the information security element that ensures that Stella's transaction status is immediately reflected in her bank account in this scenario. Information security is the practice of protecting information and information systems from unauthorized access, use, disclosure, modification, or destruction. Information security can be based on three fundamental principles: confidentiality, integrity, and availability. Confidentiality is the principle that ensures that information is accessible only to authorized parties and not disclosed to unauthorized parties. Integrity is the principle that ensures that information is accurate, complete, and consistent and not altered or corrupted by unauthorized parties. Availability is the principle that ensures that information and information systems are accessible and usable by authorized parties when needed. In the scenario, Stella purchased a smartwatch online using her debit card. After making payment for the product through the payment gateway, she received a transaction text message with a deducted and available balance from her bank. This means that her transaction status was immediately reflected in her bank account, which indicates that availability was ensured by her bank's information system.

Question 4

Question Type: MultipleChoice

An organization's risk management team identified the risk of natural disasters in the organization's current location. Because natural disasters cannot be prevented using security controls, the team suggested to build a new office in another location to eliminate the identified risk. Identify the risk treatment option suggested by the risk management team in this scenario.

Options:

A- Risk modification
B- Risk avoidance
C- Risk sharing
D- Risk retention

Answer:

B

Explanation:

Risk avoidance is the risk treatment option suggested by the risk management team in this scenario. Risk avoidance is a risk treatment option that involves eliminating the identified risk by changing the scope, requirements, or objectives of the project or activity. Risk avoidance can be used when the risk cannot be prevented using security controls or when the risk outweighs the benefits2. Reference: Risk Avoidance

Question 5

Question Type: MultipleChoice

Miguel, a professional hacker, targeted an organization to gain illegitimate access to its critical information. He identified a flaw in the end-point communication that can disclose the target application's data.

Which of the following secure application design principles was not met by the application in the above scenario?

Options:

A- Secure the weakest link
B- Do not trust user input
C- Exception handling
D- Fault tolerance

Answer:

C

Explanation:

Exception handling is a secure application design principle that states that the application should handle errors and exceptions gracefully and securely, without exposing sensitive information or compromising the system's functionality. Exception handling can help prevent attackers from exploiting errors or exceptions to gain access to data or resources or cause denial-of-service attacks. In the scenario, Miguel identified a flaw in the end-point communication that can disclose the target application's data, which means that the application did not meet the exception handling principle.

Question 6

Question Type: MultipleChoice

A web application www.movieabc.com was found to be prone to SQL injection attack. You are given a task to exploit the web application and fetch the user credentials. Select the UID which is mapped to user john in the database table.

Note:

Username: sam

Pass: test

Options:

A- 5
B- 3
C- 2
D- 4

Answer:

D

Explanation:

4 is the UID that is mapped to user john in the database table in the above scenario. SQL injection is a type of web application attack that exploits a vulnerability in a web application that allows an attacker to inject malicious SQL statements into an input field, such as a username or password field, and execute them on the database server. SQL injection can be used to bypass authentication, access or modify sensitive data, execute commands, etc. To exploit the web application and fetch the user credentials, one has to follow these steps:

Open a web browser and type www.movieabc.com

Press Enter key to access the web application.

Enter sam as username and test as password.

Click on Login button.

Observe that a welcome message with username sam is displayed.

Click on Logout button.

Enter sam' or '1'='1 as username and test as password.

Click on Login button.

Observe that a welcome message with username admin is displayed, indicating that SQL injection was successful.

Click on Logout button.

Enter sam'; SELECT * FROM users; -- as username and test as password.

Click on Login button.

Observe that an error message with user credentials from users table is displayed.

The user credentials from users table are:

UID	Username	Password
1	admin	admin
2	sam	test
3	alice	alice123
4	john	john123

The UID that is mapped to user john is 4.

Question 7

Question Type: MultipleChoice

Stephen, a security professional at an organization, was instructed to implement security measures that prevent corporate data leakage on employees' mobile devices. For this purpose, he employed a technique using which all personal and corporate data are isolated on an employee's mobile device. Using this technique, corporate applications do not have any control of or communication with the private applications or data of the employees.

Which of the following techniques has Stephen implemented in the above scenario?

Options:

A- Full device encryption
B- Geofencing
C- Containerization
D- OTA updates

Answer:

C

Explanation:

Containerization is the technique that Stephen has implemented in the above scenario. Containerization is a technique that isolates personal and corporate data on an employee's mobile device. Containerization creates separate encrypted containers or partitions on the device, where corporate applications and data are stored and managed. Containerization prevents corporate data leakage on employees' mobile devices by restricting access, sharing, copying, or transferring of data between containers. Containerization also allows remote wiping of corporate data in case of device loss or theft . Full device encryption is a technique that encrypts all the data on a mobile device using a password or a key. Geofencing is a technique that uses GPS or RFID to define geographical boundaries and trigger actions based on the location of a mobile device. OTA (Over-the-Air) updates are updates that are delivered wirelessly to mobile devices without requiring physical connection to a computer.

Question 8

Question Type: MultipleChoice

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical Information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

Options:

A- Quid pro quo
B- Diversion theft
C- Elicitation
D- Phishing

Answer:

A

Explanation:

Quid pro quo is the social engineering technique that Johnson employed in the above scenario. Quid pro quo is a social engineering method that involves offering a service or a benefit in exchange for information or access. Quid pro quo can be used to trick victims into believing that they are receiving help or assistance from a legitimate source, while in fact they are compromising their security or privacy. In the scenario, Johnson performed quid pro quo by claiming himself to represent a technical support team from a vendor and offering to help sibertech.org with a server issue, while in fact he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine. If you want to learn more about social engineering techniques, you can check out these resources:

[1] A guide to different types of social engineering attacks and how to prevent them: [https://www.csoonline.com/article/2124681/what-is-social-engineering.html]

[2] A video that explains how quid pro quo works and how to avoid falling for it: [https://www.youtube.com/watch?v=3Yy0gZ9xw8g]

[3] A quiz that tests your knowledge of social engineering techniques and scenarios: [https://www.proprofs.com/quiz-school/story.php?title=social-engineering-quiz]

To Get Premium Files for 212-82 Visit
https://www.p2pexams.com/products/212-82

For More Free Questions Visit
https://www.p2pexams.com/eccouncil/pdf/212-82

