212-82 Q&As

Certified Cybersecurity Technician(C|CT)

Pass EC-COUNCIL 212-82 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/212-82.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

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?

A. Full device encryption

B. Geofencing

C. Containerization

D. OTA updates

Correct 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 2

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.

A. Data at rest

B. Data in inactive

C. Data in transit

D. Data in use

Correct 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 3

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?

A. Secure the weakest link

B. Do not trust user input

C. Exception handling

D. Fault tolerance

Correct 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 4

A software company develops new software products by following the best practices for secure application development. Dawson, a software analyst, is responsible for checking the performance of applications in the client\\'s network to determine any issue faced by end users while accessing the application.

Which of the following tiers of the secure application development lifecycle involves checking the application performance?

A. Development

B. Staging

C. Testing

D. Quality assurance (QA)

Correct Answer: C

Explanation: Testing is the tier of the secure application development lifecycle that involves checking the application performance in the above scenario. Secure application development is a process that involves designing, developing, deploying, and maintaining software applications that are secure and resilient to threats and attacks. Secure application development can be based on various models or frameworks, such as SDLC (Software Development Life Cycle), OWASP (Open Web Application Security Project), etc. Secure application development consists of various tiers or stages that perform different tasks or roles. Testing is a tier of the secure application development lifecycle that involves

verifying and validating the functionality and security of software applications before releasing them to end users. Testing can include various types of tests, such as unit testing, integration testing, system testing, performance testing, security testing, etc. Testing can be used to check the application performance and identify any errors, bugs, or vulnerabilities in the software applications. In the scenario, a software company develops new software products by following the best practices for secure application development. Dawson, a software analyst, is responsible for checking the performance of applications in the client\\'s network to determine any issue faced by end users while accessing the application. This means that he performs testing for this purpose. Development is a tier of the secure application development lifecycle that involves creating and coding software applications according to the design and specifications. Staging is a tier of the secure application development lifecycle that involves deploying software applications to a simulated or pre-production environment for testing or evaluation purposes. Quality assurance (QA) is a tier of the secure application development lifecycle that involves ensuring that software applications meet the quality standards and expectations of end users and stakeholders

QUESTION 5

George, a security professional at an MNC, implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. Identify the type of Internet access policy implemented by George in this scenario.

A. Permissive policy

B. Paranoid policy

C. Prudent policy

D. Promiscuous policy

Correct Answer: A

Explanation: Permissive policy is the type of Internet access policy implemented by George in this scenario. An Internet access policy is a policy that defines the rules and guidelines for accessing the Internet from a system or network. An Internet access policy can be based on various factors, such as security, productivity, bandwidth, etc. An Internet access policy can have different types based on its level of restriction or control. A permissive policy is a type of Internet access policy that allows users to access any site, download any application, and access any computer or network without any restrictions. A permissive policy can be used to provide maximum flexibility and freedom to users, but it can also pose significant security risks and challenges. In the scenario, George implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. This means that he implemented a permissive policy for those employees. A paranoid policy is a type of Internet access policy that blocks or denies all Internet access by default and only allows specific sites, applications, or computers that are explicitly authorized. A prudent policy is a type of Internet access policy that allows most Internet access but blocks or restricts some sites, applications, or computers that are deemed inappropriate, malicious, or unnecessary. A promiscuous policy is not a type of Internet access policy, but a term that describes a network mode that allows a network interface card (NIC) to capture all packets on a network segment, regardless of their destination address.