Free Questions for CISSP by certscare

Shared by Snow on 09-08-2024

For More Free Questions and Preparation Resources

Question 1

When configuring Extensible Authentication Protocol (EAP) in a Voice over Internet Protocol (VoIP) network, which of the following authentication types is the MOST secure?

Options:

A- EAP-Transport Layer Security (TLS)

B- EAP-Flexible Authentication via Secure Tunneling

C- EAP-Tunneled Transport Layer Security (TLS)

D- EAP-Protected Extensible Authentication Protocol (PEAP)

Answer:

C

Question 2

A financial organization that works according to agile principles has developed a new application for their external customer base to request a line of credit. A security analyst has been asked to assess the security risk of the minimum viable product (MVP). Which is the MOST important activity the analyst should assess?

Options:

A- The software has the correct functionality.

B- The software has been code reviewed.

C- The software had been branded according to corporate standards,

D- The software has been signed off for release by the product owner.

Answer:

A

Question 3

Question Type: **MultipleChoice**

Which of the following is the PRIMARY reason for selecting the appropriate level of detail for audit record generation?

Options:

A- Lower costs throughout the System Development Life Cycle (SDLC)

B- Facilitate a root cause analysis (RCA)

C- Enable generation of corrective action reports

D- Avoid lengthy audit reports

Answer:

B

Question 4

Question Type: **MultipleChoice**

Which of the following is the BEST option to reduce the network attack surface of a system?

Options:

A- Ensuring that there are no group accounts on the system

B- Removing unnecessary system user accounts

C- Disabling unnecessary ports and services

D- Uninstalling default software on the system

Answer:

C

Question 5

Question Type: **MultipleChoice**

Which of the following is a limitation of the Bell-LaPadula model?

Options:

A- Segregation of duties (SoD) is difficult to implement as the 'no read-up' rule limits the ability of an object to access information with a higher classification.

B- Mandatory access control (MAC) is enforced at all levels making discretionary access control (DAC) impossible to implement.

C- It contains no provision or policy for changing data access control and works well only with access systems that are static in nature.

D- It prioritizes integrity over confidentiality which can lead to inadvertent information disclosure.

Answer:

A

Question 6

Question Type: **MultipleChoice**

A web developer is completing a new web application security checklist before releasing the application to production. the task of disabling unecessary services is on the checklist. Which web application threat is being mitigated by this action?

Options:

A- Security misconfiguration

B- Sensitive data exposure

C- Broken access control

D- Session hijacking

Answer:

B

Question 7

Question Type: **MultipleChoice**

Which of the following goals represents a modern shift in risk management according to National Institute of Standards and Technology (NIST)?

Options:

A- Focus on operating environments that are changing, evolving, and full of emerging threats.

B- Secure information technology (IT) systems that store, process, or transmit organizational information.

C- Enable management to make well-informed risk-based decisions justifying security expenditure.

D- Provide an improved mission accomplishment approach.

Answer:

C

Question 8

Question Type: **MultipleChoice**

Which event magnitude is defined as deadly, destructive, and disruptive when a hazard interacts with human vulnerability?

Options:

A- Disaster

B- Catastrophe

C- Crisis

D- Accident

Answer:

B

Question 9

Question Type: **MultipleChoice**

A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes. What is the

BEST design approach to securing this environment?

Options:

A- Place firewalls around critical devices, isolating them from the rest of the environment.

B- Layer multiple detective and preventative technologies at the environment perimeter.

C- Use reverse proxies to create a secondary 'shadow' environment for critical systems.

D- Align risk across all interconnected elements to ensure critical threats are detected and handled.

Answer:

B

Question 10

Question Type: **MultipleChoice**

A company developed a web application which is sold as a Software as a Service (SaaS) solution to the customer. The application is hosted by a web server running on a 'specific operating system (OS) on a virtual machine (VM). During the transition phase of the service, it is determined that the support team will need access to the application logs. Which of the following privileges would be the MOST suitable?

Options:

A- Administrative privileges on the OS

B- Administrative privileges on the web server

C- Administrative privileges on the hypervisor

D- Administrative privileges on the application folders

Answer:

D