


Question 1

Not yet answered

Marked out of 1.00

 Flag question

Shifali is concerned that some people in her company have more privileges than they should. This has occurred due to people moving from one position to another, and having cumulative rights that exceed the requirements of their current jobs. Which of the following would be most effective in mitigating this issue?

Select one:

- ☐ a. Separation of duties
- ☒ b. Permission auditing
- ☐ c. Job rotation
- ☐ d. Preventing job rotation

Question 2

Not yet answered

Marked out of 1.00

 Flag question

You are part of a team that has been hired to conduct penetration tests. Which term best describes your team?


Select one:

- ☐ a. Script kiddies
- ☒ b. Authorized hackers
- ☐ c. Semi-authorized hackers
- ☐ d. Unauthorized hackers

Question 3

Answer saved

Marked out of 1.00

 Remove flag

18) After a lengthy background check and interviewing process, your company hired a new payroll clerk named Tanvir. Tanvir will be using a web browser on a company computer at the office to access the payroll application on a public cloud provider web site over the Internet. Which type of document should Tanvir read and sign?

Select one:

- ☐ a. Password policy
- ☐ b. Remote access acceptable use policy
- ☒ c. Internet acceptable use policy
- ☐ d. Service level agreement

Question 4

Answer saved

Marked out of 1.00

 Flag question

Junaid is using the waterfall method for application development. At which phase should he implement security measures?

Select one:

- ☐ a. All of the phases mentioned
- ☒ b. Implementation
- ☐ c. Requirements
- ☐ d. Design

Question 5

Not yet answered

Marked out of 1.00

Flag question

Which of the following is not a government classification of data?

Select one:

- ☐ a. Top Secret
- ☒ b. Proprietary
- ☐ c. Secret
- ☐ d. Sensitive
- ☐ e. Confidential

Question 6

Not yet answered

Marked out of 1.00

Flag question

You just became the new security officer for a university. You are concerned that student workers who work late on campus could try and log in with faculty credentials. Which of the following would be most effective in preventing this?

Select one:

- ☒ a. Credential Management
- ☐ b. Usage auditing
- ☐ c. Password length
- ☐ d. Time of day restrictions

Question 7

Answer saved

Marked out of 1.00

Remove flag

Priyanka is concerned that some users on her network may be accessing files that they should not—specifically, files that are not required for their job tasks. Which of the following would be most effective in determining if this is happening?

Select one:

- ☐ a. Policy review
- ☒ b. Usage auditing and review
- ☐ c. Permissions auditing and review
- ☐ d. Account maintenance

Question 8

Not yet answered

Marked out of 1.00

Flag question

NIST's FIPS Publication 200 countermeasures in terms of minimum security requirements for Federal Information and Information Systems. One such requirement, "System and Communication Protection" is concerned with:

Select one:

- ☐ a. Protecting information systems media (both paper and digital)
- ☐ b. Tracking, documenting, and reporting incidents to appropriate organizational officials
- ☒ c. Employing architectural designs, software development techniques, and systems engineering principles
- ☐ d. Protecting information systems against environmental hazards

Question 9

Not yet answered

Marked out of 1.00

Flag question

Under which type of attack does an attacker's system appear to be the server to the real client and appear to be the client to the real server?


Select one:

- ☐ a. Replay
- ☒ b. Man-in-the-middle
- ☐ c. Eavesdropping
- ☐ d. Denial of Service

Question 10

Not yet answered

Marked out of 1.00

 Flag question

Which of the following techniques attempts to predict the likelihood a threat will occur and assigns monetary values should a loss occur?


Select one:

- ☐ a. Qualitative risk assessment
- ☐ b. Vulnerability assessment
- ☒ c. Quantitative risk assessment
- ☐ d. Change management

Question 11

Not yet answered

Marked out of 1.00

 Flag question

After your company implemented a clean desk policy, you have been asked to secure physical documents every night. Which of the following would be the best solution?

Select one:

- ☐ a. Onboarding
- ☒ b. Locking cabinets and drawers
- ☐ c. Department door lock
- ☐ d. Proximity card

Question 12

Not yet answered

Marked out of 1.00

 Flag question

Lohita is responsible for security on web applications for her company. She is checking to see that all applications have robust input validation. What is the best way to implement validation?


Select one:

- ☐ a. Client-side validation only
- ☐ b. Validate in transit
- ☐ c. Server-side validation only
- ☒ d. Client-side and server-side validation

Question 13

Not yet answered

Marked out of 1.00

 Flag question

You receive many calls from customers stating that your web site seems to be slow in responding. You analyze the traffic and notice that you are receiving a number of malformed requests on that web server at a high rate. What type of attack is occurring?

Select one:

- ☒ a. Denial of service
- ☐ b. Social engineer
- ☐ c. Man-in-the-middle
- ☐ d. Eavesdrop

Question 14

Not yet answered

Marked out of 1.00

 Flag question

You are working for a large company. You are trying to find a solution that will provide controlled physical access to the building and record every employee who enters the building. Which of the following would be the best for you to implement?

Select one:

- ☐ a. A security guard with a sign-in sheet
- ☒ b. Smart card access
- ☐ c. A camera by the entrance
- ☐ d. A sign-in sheet by the front door

Question 15

Not yet answered

Marked out of 1.00

 Flag question

Which of the following processes transpires when a user provides a correct username and password?


Select one:

- ☐ a. Identification
- ☐ b. Accounting
- ☐ c. Authorization
- ☒ d. Authentication

Question 16

Not yet answered

Marked out of 1.00

 Flag question

You are a security administrator for an insurance company. You have discovered that there are a few active accounts for employees who left the company over a year ago. Which of the following would best address this issue?

Select one:

- ☐ a. Password complexity
- ☐ b. Password expiration
- ☐ c. Onboarding procedures
- ☒ d. Offboarding procedures

Question 17

Answer saved

Marked out of 1.00

 Flag question

Your company restricts firewall administrators from modifying firewall rules unless they make the modifications with a member of the IT security team. What is this an example of?


Select one:

- ☒ a. Principle of least privilege
- ☐ b. Acceptable use
- ☐ c. Separation of duties
- ☐ d. Due care

Question 18

Not yet answered

Marked out of 1.00

 Flag question

Ganesh is concerned about unauthorized people entering the company's building. Which of the following would be most effective in preventing this?


Select one:

- ☐ a. Alarm systems
- ☐ b. Cameras
- ☐ c. Fencing
- ☒ d. Security guards

Question 19

Not yet answered

Marked out of 1.00

 Flag question

Which type of threat action involves acquiring sensitive data by disassembling and analyzing the design of a system component?


Select one:

- ☐ a. Exposure
- ☐ b. Incapacitation
- ☐ c. Tampering
- ☐ d. Scavenging
- ☒ e. Reverse Engineering

Question 20

Not yet answered

Marked out of 1.00

 Flag question

Despite years of research and development, it has not been possible to develop security design and implementation techniques that eliminates security flaws and prevent all unauthorized actions. Which of the following design principles is concerned with permissions rather than exclusion?


Select one:

- ☐ a. Separation of privileges
- ☐ b. Fail-safe default
- ☒ c. Least privilege
- ☐ d. Economy of mechanism

Question 21

Answer saved

Marked out of 1.00

 Remove flag

In which of the following scenarios would using a shared account pose the least security risk?

Select one:

- ☒ a. For accounts with few privileges
- ☐ b. For a group of tech support personnel
- ☐ c. For students logging in at a university
- ☐ d. For guest Wi-Fi access

Question 22

Not yet answered

Marked out of 1.00

Flag question

The assets of a computer system can be categorized as hardware, software, data, and communication lines and networks. Protecting these assets against threats is very important. In relating these four categories to the concepts of Integrity, Confidentiality, and Availability, under what category does a stolen unencrypted USB drive falls?

Select one:

- ☐ a. Hardware-Availability
- ☐ b. Data-Integrity
- ☐ c. Software-Confidentiality
- ☒ d. Hardware-Confidentiality
- ☐ e. Data-Confidentiality
- ☐ f. Data-Availability

Question 23

Not yet answered

Marked out of 1.00

Flag question

Ramesh is responsible for setting up new accounts for your company network. What is the most important thing to keep in mind when setting up new accounts?

Select one:

- ☐ a. Password length
- ☐ b. Account age
- ☒ c. Least privileges
- ☐ d. Password complexity

Question 24

Not yet answered

Marked out of 1.00

Flag question

Sameer is responsible for password management at a large company. Sometimes users cannot recall their passwords. What would be the best solution for him to address this?

Select one:

- ☐ a. Eliminating password complexity
- ☐ b. Changing password history length
- ☐ c. Lengthening password age
- ☒ d. Implementing password recovery

Question 25

Not yet answered

Marked out of 1.00

Flag question

Your organization has begun quarterly lunch-and-learn sessions to educate employees about current scams and computer security threats to increase their awareness and help prevent security issues such as data leaks. To which of the following items does this initiative best apply?

Select one:

- ☐ a. State actor
- ☐ b. Advanced persistent threat
- ☒ c. Insider threat
- ☐ d. Hacktivist