An toan thong tin_ Nhom 11

Bắt đầu vào lúc	Sunday, 24 September 2023, 3:31 PM
Trạng thái	Đã xong
Kết thúc lúc	Sunday, 24 September 2023, 3:51 PM
Thời gian thực hiện	19 phút 53 giây
Điểm	8,00/20,00
Điểm	**4,00** trên 10,00 (**40**%)

Câu hỏi 1

Sai

Đạt điểm 0,00 trên 1,00

When seeking to hire new employees, what is the first step?

Select one:

- a. Request resumes
- b. Create a job description
- c. Screen candidates
- d. Set position classification

Your answer is incorrect.

The correct answer is: Create a job description

Câu hỏi 2

Đúng

Đạt điểm 1,00 trên 1,00

If an organization contracts with outside entities to provide key business functions or services, such as account or technical support, what is the process called that is used to ensure that these entities support sufficient security?

Select one:

- a. Qualitative analysis
- b. Third-party governance ✔
- c. Exit interview
- d. Asset identification

Your answer is correct.

The correct answer is: Third-party governance

Câu hỏi 3

Đúng

Đạt điểm 1,00 trên 1,00

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

Select one:

- a. CIA Triad
- b. Hash totals
- c. Nonrepudiation ✔ Nonrepudiation ensures that the subject of an activity or event cannot deny that the event occurred.
- d. Abstraction

Your answer is correct.

The correct answer is: Nonrepudiation

Câu hỏi 4

Sai

Đạt điểm 0,00 trên 1,00

What is encapsulation?

Select one:

- a. Verifying a person's identity
- b. Changing the source and destination addresses of a packet
- c. Adding a header and footer to data as it moves down the OSI stack
- d. Protecting evidence until it has been properly collected ✖

Your answer is incorrect.

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

Câu hỏi 5

Sai

Đạt điểm 0,00 trên 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. Layering
- b. Availability
- c. Encryption ✖
- d. Identification

Your answer is incorrect.

The correct answer is: Availability

Câu hỏi 6

Đúng

Đạt điểm 1,00 trên 1,00

Which one of the following would administrators use to connect to a remote server securely for administration?

Select one:

- a. Secure File Transfer Protocol (SFTP)
- b. Secure Shell (SSH) ✔ SSH is a secure alternative to Telnet because it encrypts data transmitted over a network. In contrast, Telnet transmits data in cleartext. SFTP and SCP are good methods for transmitting sensitive data over a network, but not for administration purposes.
- c. Telnet
- d. Secure Copy (SCP)

Your answer is correct.

The correct answer is: Secure Shell (SSH)

Câu hỏi 7

Đúng

Đạt điểm 1,00 trên 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

Câu hỏi 8

Sai

Đạt điểm 0,00 trên 1,00

Which one of the following data roles is most likely to assign permissions to grant users access to data?

Select one:

- a. Owner
- b. Administrator
- c. Custodian ✖
- d. User

Your answer is incorrect.

The correct answer is: Administrator

Câu hỏi 9

Đúng

Đạt điểm 1,00 trên 1,00

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

Select one:

- a. 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.
- b. Send out a broadcast email informing everyone that a specific employee is to be terminated.
- c. Inform the employee a few hours before they are officially terminated.
- d. Wait until you and the employee are the only people remaining in the building before announcing the termination

Your answer is correct.

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

Câu hỏi 10

Đúng

Đạt điểm 1,00 trên 1,00

Which networking technology is based on the IEEE 802.3 standard?

Select one:

- a. Ethernet ✔
- b. HDLC
- c. FDDI
- d. Token Ring

Your answer is correct.

The correct answer is: Ethernet

Câu hỏi 11

Sai

Đạt điểm 0,00 trên 1,00

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

Select one:

- a. Stealing passwords
- b. Eavesdropping
- c. Social engineering ✖
- d. Hardware destruction

Your answer is incorrect.

The correct answer is: Hardware destruction

Câu hỏi 12

Sai

Đạt điểm 0,00 trên 1,00

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

Select one:

- a. Due care ✖
- b. One or more of the CIA Triad principles
- c. Data usefulness
- d. Extent of liability

Your answer is incorrect.

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

Câu hỏi 13

Sai

Đạt điểm 0,00 trên 1,00

What type of plan outlines the procedures to follow when a disaster interrupts the normal operations of a business?

Select one:

- a. Vulnerability assessment
- b. Business continuity plan
- c. Disaster recovery plan
- d. Business impact assessment ✖

Your answer is incorrect.

The correct answer is: Disaster recovery plan

Câu hỏi 14

Sai

Đạt điểm 0,00 trên 1,00

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

Select one:

- a. The CIA Triad
- b. A stand-alone system
- c. A network's border perimeter ✖
- d. The Internet

Your answer is incorrect.

The correct answer is: The CIA Triad

Câu hỏi 15

Sai

Đạt điểm 0,00 trên 1,00

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

Select one:

- a. Endpoint security
- b. Network access control (NAC) ✖
- c. RADIUS
- d. VLAN

Your answer is incorrect.

The correct answer is: Endpoint security

Câu hỏi 16

Đúng

Đạt điểm 1,00 trên 1,00

Which one of the following identifies the primary a purpose of information classification processes?

Select one:

a. Define the requirements for transmitting data

b. Define the requirements for backing up data

c. Define the requirements for protecting sensitive data ✔ A primary purpose of information classification processes is to identify security classifications for sensitive data and define the requirements to protect sensitive data. Information classification processes will typically include requirements to protect sensitive data at rest (in backups and stored on media), but not requirements for backing up and storing any data. Similarly, information classification processes will typically include requirements to protect sensitive data in transit, but not any data

d. Define the requirements for storing data

Your answer is correct.

The correct answer is: Define the requirements for protecting sensitive data

Câu hỏi 17

Đúng

Đạt điểm 1,00 trên 1,00

What is the first step that individuals responsible for the development of a business continuity plan should perform?

Select one:

a. Legal and regulatory assessment

b. Business organization analysis ✔ The business organization analysis helps the initial planners select appropriate BCP team members and then guides the overall BCP process

c. BCP team selection

d. Resource requirements analysis

Your answer is correct.

The correct answer is: Business organization analysis

Câu hỏi 18

Sai

Đạt điểm 0,00 trên 1,00

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

Select one:

- a. Awareness training ✖
- b. Logical security
- c. Physical security
- d. Intrusion detection

Your answer is incorrect.

The correct answer is: Physical security

Câu hỏi 19

Sai

Đạt điểm 0,00 trên 1,00

What security control is directly focused on preventing collusion?

Select one:

- a. Qualitative risk analysis ✖
- b. Job descriptions
- c. Separation of duties
- d. Principle of least privilege

Your answer is incorrect.

The correct answer is: Separation of duties

Câu hỏi 20

Sai

Đạt điểm 0,00 trên 1,00

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

Select one:

- a. Internet connections ✖
- b. Software products
- c. Humans
- d. Security policies

Your answer is incorrect.

The correct answer is: Humans

◄ Chapter 1 - Computer Security Concepts

Chuyển tới...

Video: Review Chapter 1 and Excercise ►

An toan thong tin_ Nhom 11

Bắt đầu vào lúc	Monday, 25 September 2023, 9:20 AM
Trạng thái	Đã xong
Kết thúc lúc	Monday, 25 September 2023, 9:22 AM
Thời gian thực hiện	1 phút 56 giây
Điểm	7,00/30,00
Điểm	**2,33** trên 10,00 (**23**%)

Câu hỏi 1

Đúng một phần

Đạt điểm 0,50 trên 1,00

A recent audit had 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. Penetration testing ✖
- b. Implement an application firewall
- c. Change default password
- d. Deploy a honeypot
- e. Disable unnecessary services ✔

Your answer is partially correct.

Bạn đã chọn đúng 1.

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

Câu hỏi 2

Đúng

Đạt điểm 1,00 trên 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:

- [x] a. Change default passwords ✔
- [x] b. Disable unnecessary services ✔
- [ ] c. Penetration testing
- [ ] d. Deploy a honeypot
- [ ] e. Implement an application firewall

Your answer is correct.

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

Câu hỏi 3

Đúng

Đạt điểm 1,00 trên 1,00

Which of the following concepts allows an organization to group large numbers of servers together in order to deliver a common service?

Select one:

- a. Cold site
- b. RAID
- c. Clustering ✔ Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).
  Clustering is done whenever you connect multiple computers to work and act together as a single server. It is meant to utilize parallel processing and can also add to redundancy.
- d. Backup Redundancy

Your answer is correct.

The correct answer is: Clustering

Câu hỏi 4

Sai

Đạt điểm 0,00 trên 1,00

Which of the following describes the process of removing unnecessary accounts and services from an application to reduce risk exposure?

Select one:

- a. Application patch management ✖
- b. Application hardening
- c. Cross-site script prevention
- d. Error and exception handling

Your answer is incorrect.

The correct answer is: Application hardening

Câu hỏi 5

Sai

Đạt điểm 0,00 trên 1,00

Failure to validate the size of a variable before writing it to memory could result in which of the following application attacks?

Select one:

- a. Cross-site scripting
- b. Malicious logic
- c. SQL injection ✖
- d. Buffer overflow

Your answer is incorrect.

The correct answer is: Buffer overflow

Câu hỏi 6

Sai

Đạt điểm 0,00 trên 1,00

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

Select one:

- a. 443
- b. 110 ✖
- c. 80
- d. 142

Your answer is incorrect.

The correct answer is: 443

Câu hỏi 7

Sai

Đạt điểm 0,00 trên 1,00

Ann, the software security engineer, works for a major software vendor. Which of the following practices should be implemented to help prevent race conditions, buffer overflows, and other similar vulnerabilities prior to each production release?

Select one:

- a. Product baseline report ✖
- b. Code review
- c. Input validation
- d. Patch regression testing

Your answer is incorrect.

The correct answer is: Code review

Câu hỏi 8

Sai

Đạt điểm 0,00 trên 1,00

Data execution prevention is a feature in most operating systems intended to protect against which type of attack?

Select one:

- a. Buffer overflow
- b. Header manipulation
- c. Cross-site scripting
- d. SQL injection ✖

Your answer is incorrect.

The correct answer is: Buffer overflow

Câu hỏi 9

Sai

Đạt điểm 0,00 trên 1,00

A Human Resources user is issued a virtual desktop typically assigned to Accounting employees. A system administrator wants to disable certain services and remove the local accounting groups installed by default on this virtual machine. The system administrator is adhering to which of the following security best practices?

Select one:

- a. Patch Management
- b. Black listing applications ✖
- c. Mandatory Access Control
- d. Operating System hardening

Your answer is incorrect.

The correct answer is: Operating System hardening

Câu hỏi 10

Đúng

Đạt điểm 1,00 trên 1,00

A server administrator notes that a legacy application often stops running due to a memory error. When reviewing the debugging logs, they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describe?

Select one:

- a. Malicious add-on
- b. Cross site scripting
- c. Zero-day
- d. Buffer overflow ✔

Your answer is correct.

The correct answer is: Buffer overflow

Câu hỏi 11

Đúng

Đạt điểm 1,00 trên 1,00

A malicious individual is attempting to write too much data to an application's memory. Which of the following describes this type of attack?

Select one:

- a. SQL injection
- b. Zero-day
- c. Buffer overflow ✔
- d. XSRF

Your answer is correct.

The correct answer is: Buffer overflow

Câu hỏi 12

Sai

Đạt điểm 0,00 trên 1,00

If you declare an array as A[100] in C and you try to write data to A[555], what will happen?

Select one:

- a. There will always be a runtime error
- b. Nothing ✖
- c. The C compiler will give you an error and won't compile
- d. Whatever is at A[555] will be overwritten

Your answer is incorrect.

The correct answer is: Whatever is at A[555] will be overwritten

Câu hỏi 13

Sai

Đạt điểm 0,00 trên 1,00

Which of the following is an example of a false positive?

Select one:

- a. A user account is locked out after the user mistypes the password too many times.
- b. Anti-virus identifies a benign application as malware.
- c. The IDS does not identify a buffer overflow
- d. A biometric iris scanner rejects an authorized user wearing a new contact lens. ✖

Your answer is incorrect.

The correct answer is: Anti-virus identifies a benign application as malware.

Câu hỏi 14

Sai

Đạt điểm 0,00 trên 1,00

Which of the following provides the BEST application availability and is easily expanded as demand grows?

Select one:

- a. Load balancing
- b. Server virtualization ✖
- c. Active-Passive Cluster
- d. RAID 6

Your answer is incorrect.

The correct answer is: Load balancing

Câu hỏi 15

Đúng

Đạt điểm 1,00 trên 1,00

Which of the following risk mitigation strategies will allow Ann, a security analyst, to enforce least privilege principles?

Select one:

- a. Incident management
- b. Annual loss expectancy
- c. Risk based controls
- d. User rights reviews ✔

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

Your answer is correct.

The correct answer is: User rights reviews

Câu hỏi 16

Sai

Đạt điểm 0,00 trên 1,00

An analyst is reviewing a simple program for potential security vulnerabilities before being deployed to a Windows server. Given the following code:

```
void foo (char *bar)
{
  char random_user_input [12];
  strcpy (random_user_input, bar);
}
```

Which of the following vulnerabilities is present?

Select one:

- a. Integer overflow
- b. Backdoor
- c. Buffer overflow
- d. Bad memory pointer

Your answer is incorrect.

The correct answer is: Buffer overflow

Câu hỏi 17

Sai

Đạt điểm 0,00 trên 1,00

Which of the following protocols is the security administrator observing in this packet capture?
12:33:43, SRC 192.168.4.3:3389, DST 10.67.33.20:8080, SYN/ACK

Select one:

- a. SFTP
- b. RDP
- c. HTTPS
- d. HTTP

Your answer is incorrect.

The correct answer is: RDP

Câu hỏi 18

Sai

Đạt điểm 0,00 trên 1,00

A security administrator is investigating a recent server breach. The breach occurred as a result of a zero-day attack against a user program running on the server. Which of the following logs should the administrator search for information regarding the breach?

Select one:

- a. Application log
- b. Setup log ✖
- c. System log
- d. Authentication log

Your answer is incorrect.

The correct answer is: Application log

Câu hỏi 19

Sai

Đạt điểm 0,00 trên 1,00

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

Select one:

- a. 23
- b. 22
- c. 21
- d. 20 ✖

Your answer is incorrect.

The correct answer is: 23

Câu hỏi 20

Đúng

Đạt điểm 1,00 trên 1,00

Which of the following is a software vulnerability that can be avoided by using input validation?

Select one:

- a. Incorrect input ✔
- b. Error handling
- c. Buffer overflow
- d. Application fuzzing

Your answer is correct.

The correct answer is: Incorrect input

Câu hỏi 21

Sai

Đạt điểm 0,00 trên 1,00

What is likely to happen if you find a buffer overflow during testing by entering a random, long string for a C program?

Select one or more:

- a. The program crashes
- b. The program gives you a “Buffer overflow at line X” error ✖
- c. The C fairy sprinkles magic memory dust on the memory that was overwritten and makes everything okay again.
- d. Data is corrupted

Your answer is incorrect.

The correct answers are: Data is corrupted, The program crashes

Câu hỏi 22

Đúng một phần

Đạt điểm 0,50 trên 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 for business continuity if one provider goes out of business
- b. To allow load balancing for cloud support
- c. 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.
- d. To improve intranet communication speeds
- e. To allow for a hot site in case of disaster

Your answer is partially correct.

Bạn đã chọn đúng 1.

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

Câu hỏi 23

Sai

Đạt điểm 0,00 trên 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. Zero-day exploit
- b. Botnet
- c. Distributed denial-of-service
- d. Denial-of-service ✖

Your answer is incorrect.

The correct answer is: Zero-day exploit

Câu hỏi 24

Sai

Đạt điểm 0,00 trên 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
- b. Mandatory access
- c. Job rotation
- d. Rule-based access control ✖

Your answer is incorrect.

The correct answer is: Least privilege

Câu hỏi 25

Sai

Đạt điểm 0,00 trên 1,00

A network security engineer notices unusual traffic on the network from a single IP attempting to access systems on port 23. Port 23 is not used anywhere on the network. Which of the following should the engineer do to harden the network from this type of intrusion in the future?

Select one:

- a. Disable unnecessary services on servers
- b. Disable unused accounts on servers and network devices ✖
- c. Enable auditing on event logs
- d. Implement password requirements on servers and network devices

Your answer is incorrect.

The correct answer is: Disable unnecessary services on servers

Câu hỏi 26

Sai

Đạt điểm 0,00 trên 1,00

A vulnerability scan is reporting that patches are missing on a server. After a review, it is determined that the application requiring the patch does not exist on the operating system. Which of the following describes this cause?

Select one:

- a. Baseline code review
- b. Application hardening
- c. False negative ✖
- d. False positive

Your answer is incorrect.

The correct answer is: False positive

Câu hỏi 27

Sai

Đạt điểm 0,00 trên 1,00

An IT security technician needs to establish host based security for company workstations. Which of the following will BEST meet this requirement?

Select one:

- a. Implement OS hardening by applying GPOs.
- b. Implement database hardening by applying vendor guidelines. ✖
- c. Implement perimeter firewall rules to restrict access.
- d. Implement IIS hardening by restricting service accounts.

Your answer is incorrect.

The correct answer is: Implement OS hardening by applying GPOs.

Câu hỏi 28

Sai

Đạt điểm 0,00 trên 1,00

Disabling unnecessary services, restricting administrative access, and enabling auditing controls on a server are forms of which of the following?

Select one:

- a. Application patch management
- b. Creating a security baseline ✖
- c. System hardening
- d. Cross-site scripting prevention

Your answer is incorrect.

The correct answer is: System hardening

Câu hỏi 29

Sai

Đạt điểm 0,00 trên 1,00

Which of the following preventative controls would be appropriate for responding to a directive to reduce the attack surface of a specific host?

Select one:

- a. Disabling unnecessary services
- b. Implementing an IDS
- c. Installing anti-malware ✖
- d. Taking a baseline configuration

Your answer is incorrect.

The correct answer is: Disabling unnecessary services

Câu hỏi 30

Sai

Đạt điểm 0,00 trên 1,00

Which of the following, if properly implemented, would prevent users from accessing files that are unrelated to their job duties? (Select TWO).

Select one or more:

- [x] a. Mandatory vacation ✖
- [ ] b. Time of day restrictions
- [ ] c. Least privilege
- [ ] d. Separation of duties
- [ ] e. Job rotation

Your answer is incorrect.

The correct answers are: Separation of duties, Least privilege

◄ Chapter 4 - LAB_Step-by-Step Exploit OS Vulnerabilities

Chuyển tới...

Video: OS Security ►

An toan thong tin_ Nhom 11

Bắt đầu vào lúc	Tuesday, 26 September 2023, 9:56 AM
Trạng thái	Đã xong
Kết thúc lúc	Tuesday, 26 September 2023, 10:06 AM
Thời gian thực hiện	9 phút 56 giây
Điểm	9,00/39,00
Điểm	**2,31** trên 10,00 (**23**%)

Câu hỏi 1

Đúng

Đạt điểm 1,00 trên 1,00

Which of the following types of access control uses fences, security policies, security awareness training, and antivirus software to stop an unwanted or unauthorized activity from occurring?

Select one:

a. Corrective

b. Detective

c. Authoritative

d. Preventive

A preventive access control helps stop an unwanted or unauthorized activity from occurring. Detective controls discover the activity after it has occurred, and corrective controls attempt to reverse any problems caused by the activity. Authoritative isn't a valid type of access control.

Your answer is correct.

The correct answer is: Preventive

Câu hỏi 2

Đúng

Đạt điểm 1,00 trên 1,00

Pete, a developer, writes an application. Jane, the security analyst, knows some things about the overall application but does not have all the details. Jane needs to review the software before it is released to production. Which of the following reviews should Jane conduct?

Select one:

- a. Business Impact Analysis
- b. Gray Box Testing ✔ Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program.
- c. Black Box Testing
- d. White Box Testing

Your answer is correct.

The correct answer is: Gray Box Testing

Câu hỏi 3

Đúng

Đạt điểm 1,00 trên 1,00

During the information gathering stage of a deploying role-based access control model, which of the following information is MOST likely required?

Select one:

- a. Normal hours of business operation
- b. Conditional rules under which certain systems may be accessed
- c. Clearance levels of all company personnel
- d. Matrix of job titles with required access privileges ✔

Your answer is correct.

The correct answer is: Matrix of job titles with required access privileges

Câu hỏi 4

Đúng

Đạt điểm 1,00 trên 1,00

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

Select one:

a. 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.

b. To ensure proper use of social media

c. To train staff on zero-days

d. To detail business impact analyses

Your answer is correct.

The correct answer is: To reduce organizational IT risk

Câu hỏi 5

Đúng

Đạt điểm 1,00 trên 1,00

Ann is a member of the Sales group. She needs to collaborate with Joe, a member of the IT group, to edit a file. Currently, the file has the following permissions:
Ann: read/write
Sales Group: read
IT Group: no access
If a discretionary access control list is in place for the files owned by Ann, which of the following would be the BEST way to share the file with Joe?

Select one:

- a. Give Joe the appropriate access to the file directly. ✔ Joe needs access to only one file. He also needs to 'edit' that file. Editing a file requires Read and Write access to the file. The best way to provide Joe with the minimum required permissions to edit the file would be to give Joe the appropriate access to the file directly.
- b. Remove Joe from the IT group and add him to the Sales group.
- c. Add Joe to the Sales group.
- d. Have the system administrator give Joe full access to the file.

Your answer is correct.

The correct answer is: Give Joe the appropriate access to the file directly.

Câu hỏi 6

Đúng

Đạt điểm 1,00 trên 1,00

A process in which the functionality of an application is tested without any knowledge of the internal mechanisms of the application is known as:

Select one:

- a. Black hat testing
- b. White box testing
- c. Gray box testing
- d. Black box testing ✔

Your answer is correct.

The correct answer is: Black box testing

Câu hỏi 7

Đúng

Đạt điểm 1,00 trên 1,00

A recent online password audit has identified that stale accounts are at risk to brute force attacks. Which the following controls would best mitigate this risk?

Select one:

- a. Password length
- b. Account lockouts ✔
- c. Account disablement
- d. Password complexity

Your answer is correct.

The correct answer is: Account lockouts

Câu hỏi 8

Đúng

Đạt điểm 1,00 trên 1,00

After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service?

Select one:

- a. Business impact analysis
- b. Disaster recovery plan ✔ A disaster-recovery plan, or scheme, helps an organization respond effectively when a disaster occurs. Disasters may include system failure, network failure, infrastructure failure, and natural disaster. The primary emphasis of such a plan is reestablishing services and minimizing losses.
- c. Succession planning
- d. Information security plan

Your answer is correct.

The correct answer is: Disaster recovery plan

Câu hỏi 9

Sai

Đạt điểm 0,00 trên 1,00

Internet banking customers currently use an account number and password to access their online accounts. The bank wants to improve security on high value transfers by implementing a system which call users back on a mobile phone to authenticate the transaction with voice verification. Which of the following authentication factors are being used by the bank?

Select one:

- a. Something you know, something you do, and something you have ✖
- b. Something you have, something you are, and something you know
- c. Something you are, something you do and something you know
- d. Something you do, somewhere you are, and something you have

Your answer is incorrect.

The correct answer is: Something you are, something you do and something you know

Câu hỏi 10

Đúng

Đạt điểm 1,00 trên 1,00

RADIUS provides which of the following?

Select one:

- a. Authentication, Authorization, Auditing
- b. Authentication, Authorization, Accounting ✔
- c. Authentication, Accounting, Auditing
- d. Authentication, Authorization, Availability

Your answer is correct.

The correct answer is: Authentication, Authorization, Accounting

Câu hỏi 11

Không trả lời

Đạt điểm 1,00

A company determines a need for additional protection from rogue devices plugging into physical ports around the building. Which of the following provides the highest degree of protection from unauthorized wired network access?

Select one:

- a. Intrusion Prevention Systems
- b. 802.1x
- c. MAC filtering
- d. Flood guards

Your answer is incorrect.

The correct answer is: 802.1x

Câu hỏi 12

Không trả lời

Đạt điểm 1,00

An auditing team has found that passwords do not meet best business practices. Which of the following will MOST increase the security of the passwords? (Select TWO).

Select one or more:

- a. Password Length
- b. Password Expiration
- c. Password Age
- d. Password History
- e. Password Complexity

Your answer is incorrect.

The correct answers are: Password Complexity, Password Length

Câu hỏi 13

Không trả lời

Đạt điểm 1,00

A user ID and password together provide which of the following?

Select one:

- a. Auditing
- b. Authentication
- c. Identification
- d. Authorization

Your answer is incorrect.

The correct answer is: Authentication

Câu hỏi 14

Không trả lời

Đạt điểm 1,00

What is the end device that sends credentials for 802.1x called?

Select one:

- a. Authenticator
- b. AAA server
- c. RADIUS server
- d. Supplicant

Your answer is incorrect.

The correct answer is: Supplicant

Câu hỏi 15

Không trả lời

Đạt điểm 1,00

Which of the following is a management control?

Select one:

- a. SYN attack prevention
- b. Logon banners
- c. Written security policy
- d. Access Control List (ACL)

Your answer is incorrect.

The correct answer is: Written security policy

Câu hỏi 16

Không trả lời

Đạt điểm 1,00

A customer has provided an email address and password to a website as part of the login process. Which of the following BEST describes the email address?

Select one:

- a. Identification
- b. Authentication
- c. Access control
- d. Authorization

Your answer is incorrect.

The correct answer is: Identification

Câu hỏi 17

Không trả lời

Đạt điểm 1,00

Which of the following best practices makes a wireless network more difficult to find?

Select one:

- a. Power down unused WAPs
- b. Implement MAC filtering
- c. UseWPA2-PSK
- d. Disable SSID broadcast

Your answer is incorrect.

The correct answer is: Disable SSID broadcast

Câu hỏi 18

Không trả lời

Đạt điểm 1,00

A company wants to ensure that all credentials for various systems are saved within a central database so that users only have to login once for access to all systems. Which of the following would accomplish this?

Select one:

- a. Smart card access
- b. Same Sign-On
- c. Multi-factor authentication
- d. Single Sign-On

Your answer is incorrect.

The correct answer is: Single Sign-On

Câu hỏi 19

Không trả lời

Đạt điểm 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. Role-based security training.
- b. Legal compliance training.
- c. BYOD security training.
- d. Security awareness training.

Your answer is incorrect.

The correct answer is: Security awareness training.

Câu hỏi 20

Không trả lời

Đạt điểm 1,00

Connections using point-to-point protocol authenticate using which of the following? (Select TWO).

Select one or more:

- a. PAP
- b. RIPEMD
- c. RC4
- d. CHAP
- e. Kerberos

Your answer is incorrect.

The correct answers are: PAP, CHAP

Câu hỏi 21

Không trả lời

Đạt điểm 1,00

A password history value of three means which of the following?

Select one:

- a. The server stores passwords in the database for three days.
- b. After three hours a password must be re-entered to continue
- c. Three different passwords are used before one can be reused.
- d. A password cannot be reused once changed for three years.

Your answer is incorrect.

The correct answer is: Three different passwords are used before one can be reused.

Câu hỏi 22

Không trả lời

Đạt điểm 1,00

Which of the following would be used to allow a subset of traffic from a wireless network to an internal network?

Select one:

- a. 802.1X
- b. Port security
- c. Load balancers
- d. Access control list

Your answer is incorrect.

The correct answer is: 802.1X

Câu hỏi 23

Không trả lời

Đạt điểm 1,00

What is the switch called in an 802.1x configuration?

Select one:

- a. Supplicant
- b. RADIUS server
- c. Authenticator
- d. AAA server

Your answer is incorrect.

The correct answer is: Authenticator

Câu hỏi 24

Không trả lời

Đạt điểm 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. Least privilege
- b. Group based privileges
- c. Account lockout
- d. Periodic access review

Your answer is incorrect.

The correct answer is: Least privilege

Câu hỏi 25

Không trả lời

Đạt điểm 1,00

A system administrator has noticed that users change their password many times to cycle back to the original password when their passwords expire. Which of the following would BEST prevent this behavior?

Select one:

a. Prevent users from choosing their own passwords.

b. Enforce a minimum password age policy.

c. Increase the password expiration time frame

d. Assign users passwords based upon job role.

Your answer is incorrect.

The correct answer is: Enforce a minimum password age policy.

Câu hỏi 26

Không trả lời

Đạt điểm 1,00

A penetration tester was able to obtain elevated privileges on a client workstation and multiple servers using the credentials of an employee. Which of the following controls would mitigate these issues? (Select TWO)

Select one or more:

a. Account expiration

b. Discretionary access control

c. Least privilege

d. Time of day restrictions

e. Separation of duties

f. Password history

Your answer is incorrect.

The correct answers are: Least privilege, Account expiration

Câu hỏi 27

Không trả lời

Đạt điểm 1,00

A quality assurance analyst is reviewing a new software product for security, and has complete access to the code and data structures used by the developers. This is an example of which of the following types of testing?

Select one:

- a. White box
- b. Black box
- c. Penetration
- d. Gray box

Your answer is incorrect.

The correct answer is: White box

Câu hỏi 28

Không trả lời

Đạt điểm 1,00

Which of the following controls would allow a company to reduce the exposure of sensitive systems from unmanaged devices on internal networks?

Select one:

- a. Password strength
- b. BGP
- c. 802.1x
- d. Data encryption

Your answer is incorrect.

The correct answer is: 802.1x

Câu hỏi 29

Không trả lời

Đạt điểm 1,00

A security administrator must implement all requirements in the following corporate policy: Passwords shall be protected against offline password brute force attacks. Passwords shall be protected against online password brute force attacks. Which of the following technical controls must be implemented to enforce the corporate policy? (Select THREE).

Select one or more:

- a. Screen locks
- b. Password complexity
- c. Minimum password length
- d. Account lockout
- e. Account expiration
- f. Minimum password lifetime

Your answer is incorrect.

The correct answers are: Account lockout, Password complexity, Minimum password length

Câu hỏi 30

Không trả lời

Đạt điểm 1,00

Which technology will give selective access to the network based upon authentication?

Select one:

- a. 802.1x
- b. ACLs
- c. Firewall
- d. 802.1Q

Your answer is incorrect.

The correct answer is: 802.1x

Câu hỏi 31

Không trả lời

Đạt điểm 1,00

Which of the following is a best practice when securing a switch from physical access?

Select one:

- a. Disable unnecessary accounts
- b. Print baseline configuration
- c. Disable unused ports
- d. Enable access lists

Your answer is incorrect.

The correct answer is: Disable unused ports

Câu hỏi 32

Không trả lời

Đạt điểm 1,00

An incident occurred when an outside attacker was able to gain access to network resources. During the incident response, investigation security logs indicated multiple failed login attempts for a network administrator. Which of the following controls, if in place could have BEST prevented this successful attack?

Select one:

- a. Account lockout
- b. Account expiration
- c. Password history
- d. Password complexity

Your answer is incorrect.

The correct answer is: Account lockout

Câu hỏi 33

Không trả lời

Đạt điểm 1,00

Which of the following would allow users from outside of an organization to have access to internal resources?

Select one:

- a. VLANS
- b. NAT
- c. NAC
- d. VPN

Your answer is incorrect.

The correct answer is: VPN

Câu hỏi 34

Không trả lời

Đạt điểm 1,00

Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

Select one:

- a. Mandatory access control
- b. Common access card
- c. Discretionary access control
- d. Role based access control

Your answer is incorrect.

The correct answer is: Role based access control

Câu hỏi 35

Không trả lời

Đạt điểm 1,00

Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access. Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO).

Select one or more:

- a. Disable SSID broadcast
- b. Use channels 1, 4 and 7 only
- c. Enable MAC filtering
- d. Switch from 802.11a to 802.11b
- e. Disable the wired ports

Your answer is incorrect.

The correct answers are: Enable MAC filtering, Disable SSID broadcast

Câu hỏi 36

Không trả lời

Đạt điểm 1,00

XYZ Company has a database containing personally identifiable information for all its customers. Which of the following options would BEST ensure employees are only viewing information associated to the customers they support?

Select one:

- a. Data ownership
- b. Auditing
- c. Access Control
- d. Encryption

Your answer is incorrect.

The correct answer is: Access Control

Câu hỏi 37

Không trả lời

Đạt điểm 1,00

At an organization, unauthorized users have been accessing network resources via unused network wall jacks. Which of the following would be used to stop unauthorized access?

Select one:

- a. Configure an access list.
- b. Configure port security.
- c. Configure loop protection.
- d. Configure spanning tree protocol.

Your answer is incorrect.

The correct answer is: Configure port security.

Câu hỏi 38

Không trả lời

Đạt điểm 1,00

A security Operations Center was scanning a subnet for infections and found a contaminated machine. One of the administrators disabled the switch port that the machine was connected to, and informed a local technician of the infection. Which of the following steps did the administrator perform?

Select one or more:

- a. Quarantine
- b. Notification
- c. Identification
- d. Escalation
- e. Preparation

Your answer is incorrect.

The correct answers are: Notification, Quarantine

Câu hỏi 39

Không trả lời

Đạt điểm 1,00

A company requires that a user's credentials include providing something they know and something they are in order to gain access to the network. Which of the following types of authentication is being described?

Select one:

- a. Token
- b. Biometrics
- c. Kerberos
- d. Two-factor

Your answer is incorrect.

The correct answer is: Two-factor

◄ Video: Access control - RBAC&ABAC

Chuyển tới...

Access Control - Reference ►