An toan thong tin_ Nhom 03

Started on	Tuesday, 16 June 2020, 9:34 AM
State	Finished
Completed on	Tuesday, 16 June 2020, 9:56 AM
Time taken	22 mins 26 secs
Marks	37.00/39.00
Grade	**9.49** out of 10.00 (**95**%)

Question 1

Correct

Mark 1.00 out of 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. Escalation
- [x] b. Quarantine
- [ ] c. Identification
- [ ] d. Preparation
- [x] e. Notification

Your answer is correct.

The correct answers are: Notification, Quarantine

Question 2

Correct

Mark 1.00 out of 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. Access control list
- ( ) b. Load balancers
- ( ) c. Port security
- (•) d. 802.1X

Your answer is correct.

The correct answer is: 802.1X

Question 3

Correct

Mark 1.00 out of 1.00

What is the switch called in an 802.1x configuration?

Select one:

- a. AAA server
- b. Supplicant
- c. Authenticator The switch is responsible for communicating with the supplicant and sending information to the authenticating server. This device is called the authenticator
- d. RADIUS server

Your answer is correct.

The correct answer is: Authenticator

Question 4

Correct

Mark 1.00 out of 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. Remove Joe from the IT group and add him to the Sales group.
- b. 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.
- 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.

Question 5

Correct

Mark 1.00 out of 1.00

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

Select one or more:

- [x] a. PAP A password authentication protocol (PAP) is an authentication protocol that uses a password. PAP is used by Point to Point Protocol to validate users before allowing them access to server resources.
- [ ] b. RIPEMD
- [x] c. CHAP CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake.
- [ ] d. RC4
- [ ] e. Kerberos

Your answer is correct.

The correct answers are: PAP, CHAP

Question 6

Correct

Mark 1.00 out of 1.00

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

Select one:

- ( ) a. A password cannot be reused once changed for three years.
- ( ) b. The server stores passwords in the database for three days.
- ( ) c. After three hours a password must be re-entered to continue
- (•) d. Three different passwords are used before one can be reused. Password History defines the number of unique new passwords a user must use before an old password can be reused.

Your answer is correct.

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

Question 7

Correct

Mark 1.00 out of 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. Authorization
- b. Access control
- c. Identification
- d. Authentication

Your answer is correct.

The correct answer is: Identification

Question 8

Correct

Mark 1.00 out of 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. Increase the password expiration time frame
- b. Enforce a minimum password age policy.
  A minimum password age policy defines the period that a password must be used for before it can be changed.
- c. Assign users passwords based upon job role.
- d. Prevent users from choosing their own passwords.

Your answer is correct.

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

Question 9

Correct

Mark 1.00 out of 1.00

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

Select one:

- a. Disable unnecessary accounts
- b. Enable access lists
- c. Disable unused ports Disabling unused switch ports a simple method many network administrators use to help secure their network from unauthorized access.
- d. Print baseline configuration

Your answer is correct.

The correct answer is: Disable unused ports

Question 10

Correct

Mark 1.00 out of 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. Periodic access review
- c. Group based privileges
- d. Account lockout

Your answer is correct.

The correct answer is: Least privilege

Question 11

Correct

Mark 1.00 out of 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. Encryption
- b. Auditing
- c. Data ownership
- d. Access Control

Your answer is correct.

The correct answer is: Access Control

Question 12

Correct

Mark 1.00 out of 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. Password history
- c. Account expiration
- d. Password complexity

Your answer is correct.

The correct answer is: Account lockout

Question 13

Correct

Mark 1.00 out of 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:

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

Your answer is correct.

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

Question 14

Incorrect

Mark 0.00 out of 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

Question 15

Correct

Mark 1.00 out of 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. Discretionary access control
- c. Role based access control Role-based Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role.
- d. Common access card

Your answer is correct.

The correct answer is: Role based access control

Question 16

Correct

Mark 1.00 out of 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. Password history
- b. Discretionary access control
- c. Time of day restrictions
- d. Account expiration
- e. Least privilege
- f. Separation of duties

Your answer is correct.

The correct answers are: Least privilege, Account expiration

Question 17

Correct

Mark 1.00 out of 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. Single Sign-On Single sign-on means that once a user (or other subject) is authenticated into a realm, re-authentication is not required for access to resources on any realm entity. Single sign-on is able to internally translate and store credentials for the various mechanisms, from the credential used for original authentication.
- b. Same Sign-On
- c. Smart card access
- d. Multi-factor authentication

Your answer is correct.

The correct answer is: Single Sign-On

Question 18

Correct

Mark 1.00 out of 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 correct.

The correct answer is: 802.1x

Question 19

Correct

Mark 1.00 out of 1.00

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

Select one:

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

Your answer is correct.

The correct answer is: Authentication

Question 20

Correct

Mark 1.00 out of 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. Information security plan
- c. Succession planning
- d. 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.

Your answer is correct.

The correct answer is: Disaster recovery plan

Question 21

Correct

Mark 1.00 out of 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. Black box
- b. Penetration
- c. White box White box testing is the process of testing an application when you have detailed knowledge of the inner workings of the application.
- d. Gray box

Your answer is correct.

The correct answer is: White box

Question 22

Correct

Mark 1.00 out of 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. 802.1x
- b. Data encryption
- c. Password strength
- d. BGP

Your answer is correct.

The correct answer is: 802.1x

Question 23

Incorrect

Mark 0.00 out of 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 are, something you do and something you know
- b. Something you have, something you are, and something you know
- c. Something you do, somewhere you are, and something you have
- d. Something you know, something you do, and something you have

Your answer is incorrect.

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

Question 24

Correct

Mark 1.00 out of 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. Biometrics
- b. Two-factor Two-factor authentication is when two different authentication factors are provided for authentication purposes. In this case, "something they know and something they are".
- c. Token
- d. Kerberos

Your answer is correct.

The correct answer is: Two-factor

Question 25

Correct

Mark 1.00 out of 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. Gray box testing
- c. White box testing
- d. Black box testing

Your answer is correct.

The correct answer is: Black box testing

Question 26

Correct

Mark 1.00 out of 1.00

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

Select one:

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

Your answer is correct.

The correct answer is: Disable SSID broadcast

Question 27

Correct

Mark 1.00 out of 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:

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

Your answer is correct.

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

Question 28

Correct

Mark 1.00 out of 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. BYOD security training.
- b. Role-based security training.
- c. Legal compliance training.
- d. Security awareness training. Security awareness and training are critical to the success of a security effort. They include explaining policies, procedures, and current threats to both users and management.

Your answer is correct.

The correct answer is: Security awareness training.

Question 29

Correct

Mark 1.00 out of 1.00

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

Select one:

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

Your answer is correct.

The correct answer is: VPN

Question 30

Correct

Mark 1.00 out of 1.00

Which of the following is a management control?

Select one:

- a. Logon banners
- b. SYN attack prevention
- c. Written security policy Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment; and written security policy falls in this category
- d. Access Control List (ACL)

Your answer is correct.

The correct answer is: Written security policy

Question 31

Correct

Mark 1.00 out of 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. Black Box Testing
- b. White Box Testing
- c. 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.
- d. Business Impact Analysis

Your answer is correct.

The correct answer is: Gray Box Testing

Question 32

Correct

Mark 1.00 out of 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. Detective
- b. Corrective
- 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

Question 33

Correct

Mark 1.00 out of 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. Clearance levels of all company personnel
- b. Normal hours of business operation
- c. Conditional rules under which certain systems may be accessed
- 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

Question 34

Correct

Mark 1.00 out of 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 spanning tree protocol.
- c. Configure port security. Port security in IT can mean several things. It can mean the physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port. This can be accomplished by locking down the wiring closet and server vaults and then disconnecting the workstation run from the patch panel (or punch-down block) that leads to a room's wall jack. Any unneeded or unused wall jacks can (and should) be physically disabled in this manner. Another option is to use a smart patch panel that can monitor the MAC address of any device connected to each and every wall port across a building and detect not just when a new device is connected to an empty port, but also when a valid device is disconnected or replaced by an invalid device.
- d. Configure loop protection.

Your answer is correct.

The correct answer is: Configure port security.

Question 35

Correct

Mark 1.00 out of 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. Password complexity
- c. Account disablement
- d. Account lockouts

Your answer is correct.

The correct answer is: Account lockouts

Question 36

Correct

Mark 1.00 out of 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 History
- [x] b. Password Complexity
- [x] c. Password Length
- [ ] d. Password Age
- [ ] e. Password Expiration

Your answer is correct.

The correct answers are: Password Complexity, Password Length

Question 37

Correct

Mark 1.00 out of 1.00

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

Select one:

- (•) a. Supplicant The end device that sends credentials is called the supplicant. The supplicant is a piece of software in the operating system that supplies the credentials for AAA authentication.
- ( ) b. Authenticator
- ( ) c. AAA server
- ( ) d. RADIUS server

Your answer is correct.

The correct answer is: Supplicant

Question 38

Correct

Mark 1.00 out of 1.00

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

Select one:

- a. To detail business impact analyses
- b. To ensure proper use of social media
- c. 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.
- d. To train staff on zero-days

Your answer is correct.

The correct answer is: To reduce organizational IT risk

Question 39

Correct

Mark 1.00 out of 1.00

RADIUS provides which of the following?

Select one:

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

Your answer is correct.

The correct answer is: Authentication, Authorization, Accounting

◄ Video - Access control models (ref)

Q&A - C3 ►

Return to: Chapter 3. Auth...