Eccouncil 112-51 NDE Practice Questions

Shared by Burch on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following access control models refers to assigning permissions to a user role based on the rules defined for each user role by the administrator?

Options:

A- Discretionary rule access control
B- Mandatory rule access control
C- Rule-based access control
D- Role-based access control

Answer:

D

Explanation:

Role-based access control (RBAC) is a type of access control model that refers to assigning permissions to a user role based on the rules defined for each user role by the administrator. In RBAC, the administrator creates different roles and assigns them the appropriate access rights to the resources. The administrator then assigns users to those roles based on their job functions. This way, the administrator can manage the access of users to the resources without having to deal with each user individually. RBAC can simplify the administration, enhance the security, and improve the scalability of the access control system12. Reference: Network Defense Essentials - EC-Council Learning, Role-Based Access Control (RBAC) and Role-Based Security

Question 2

Question Type: MultipleChoice

George, a professional hacker, targeted a bank employee and tried to crack his password while he was attempting to log on to the remote server to perform his regular banking operations. In this process, George used sniffing tools to capture the password pairwise master key (PMK) associated with the handshake authentication process. Then, using the PMK, he gained unauthorized access to the server to perform malicious activities.

Identify the encryption technology on which George performed password cracking.

Options:

A- WPA3
B- WPA
C- WPA2
D- WEP

Answer:

C

Explanation:

WPA2 (Wi-Fi Protected Access 2) is an encryption technology that secures wireless networks using the IEEE 802.11i standard. WPA2 uses a four-way handshake to authenticate the client and the access point, and to generate a pairwise transient key (PTK) for encrypting the data. The PTK is derived from the password pairwise master key (PMK), which is a shared secret between the client and the access point. The PMK can be obtained either by using a pre-shared key (PSK) or by using an 802.1X authentication server. In the above scenario, George performed password cracking on WPA2, as he used sniffing tools to capture the PMK associated with the handshake authentication process. Then, using the PMK, he was able to derive the PTK and decrypt the data exchanged between the client and the access point. Reference:

WPA2 - Wikipedia

How WPA2-PSK encryption works? - Cryptography Stack Exchange

WPA2 Encryption and Configuration Guide - Cisco Meraki Documentation

Question 3

Question Type: MultipleChoice

An loT sensor in an organization generated an emergency alarm indicating a security breach. The servers hosted in an loT layer accepted, stored, and processed the sensor data received from loT gateways and created dashboards for monitoring, analyzing, and implementing proactive decisions to tackle the issue.

Which of the following layers in the loT architecture performed the above activities after receiving an alert from the loT sensor?

Options:

A- Device layer
B- Cloud layer
C- Process layer
D- Communication Layer

Answer:

B

Explanation:

The cloud layer of IoT architecture is the layer that hosts the servers that accept, store, and process the sensor data received from IoT gateways. The cloud layer also creates dashboards for monitoring, analyzing, and implementing proactive decisions to tackle the issue. The cloud layer provides scalability, reliability, and security for the IoT system. The cloud layer can use various cloud computing models, such as public, private, hybrid, or community clouds12. Reference: Network Defense Essentials - EC-Council Learning, IoT Architecture: The 4 Layers of an IoT System

Question 4

Question Type: MultipleChoice

Kelly, a cloud administrator at TechSol Inc., was instructed to select a cloud deployment model to secure the corporate data and retain full control over the data.

Which of the following cloud deployment models helps Kelly in the above scenario?

Options:

A- Public cloud
B- Multi cloud
C- Community cloud
D- Private cloud

Answer:

D

Explanation:

A private cloud is a cloud deployment model that is exclusively used by a single organization and is hosted either on-premises or off-premises by a third-party provider. A private cloud offers the highest level of security and control over the data and resources, as the organization can customize the cloud infrastructure and services according to its needs and policies. A private cloud also ensures better performance and availability, as the organization does not share the cloud resources with other users. A private cloud is suitable for organizations that have sensitive or confidential data, strict compliance requirements, or high demand for scalability and flexibility. A private cloud can help Kelly secure the corporate data and retain full control over the data in the above scenario. Reference:

Private Cloud - Week 6: Virtualization and Cloud Computing

Private Cloud vs Public Cloud vs Hybrid Cloud

Private Cloud Security: Challenges and Best Practices

Question 5

Question Type: MultipleChoice

John, from a remote location, was monitoring his bedridden grandfather's health condition at his home. John has placed a smart wearable ECG on his grandfather's wrist so that he can receive alerts to his mobile phone and can keep a track over his grandfather's health condition periodically.

Which of the following types of loT communication model was demonstrated in the above scenario?

Options:

A- Device-to-gateway model
B- Device-to-cloud model
C- Cloud-to-cloud communication model
D- Device-to-device model

Answer:

B

Explanation:

A device-to-cloud model is a type of IoT communication model that connects the IoT devices directly to the cloud platform, where the data is stored, processed, and analyzed. The device-to-cloud model enables remote access, real-time monitoring, and scalability of IoT applications. The device-to-cloud model requires the IoT devices to have internet connectivity and cloud compatibility. In the above scenario, John used a device-to-cloud model to monitor his grandfather's health condition, as he placed a smart wearable ECG on his grandfather's wrist that sent the data to the cloud platform, where John could access it from his mobile phone and receive alerts periodically. Reference:

Communication Models in IoT (Internet of Things) - Section: Device-to-Cloud Model

IoT Communication Models - IoTbyHVM - Section: Device to Cloud Communication Model

Logical Design of IoT | Communication Models | APIs | Functional Blocks - Section: Device-to-Cloud Communication Model

Question 6

Question Type: MultipleChoice

George, a certified security professional, was hired by an organization to ensure that the server accurately responds to customer requests. In this process, George employed a security solution to monitor the network traffic toward the server. While monitoring the traffic, he identified attack signatures such as SYN flood and ping of death attempts on the server.

Which option best categories of suspicious traffic signature has George identified in the above scenario?

Options:

A- Informational
B- Reconnaissance
C- Unauthorized access
D- Denial-of-service (DoS)

Answer:

D

Explanation:

Denial-of-service (DoS) is the category of suspicious traffic signature that George identified in the above scenario. DoS signatures are designed to detect attempts to disrupt or degrade the

availability or performance of a system or network by overwhelming it with excessive or malformed traffic. SYN flood and ping of death are examples of DoS attacks that exploit the TCP/IP protocol to consume the resources or crash the target server. A SYN flood attack sends a large number of TCP SYN packets to the target server, without completing the three-way handshake, thus creating a backlog of half-open connections that exhaust the server's memory or bandwidth. A ping of death attack sends a malformed ICMP echo request packet that exceeds the maximum size allowed by the IP protocol, thus causing the target server to crash or reboot. DoS attacks can cause serious damage to the organization's reputation, productivity, and revenue, and should be detected and mitigated as soon as possible123. Reference:

Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-33 to 3-34

What is a denial-of-service attack?, Cloudflare, 2020

Denial-of-service attack - Wikipedia, Wikipedia, March 16, 2021

Question 7

Question Type: MultipleChoice

Which of the following practices helps security professionals protect mobile applications from various attacks?

Options:

A- Always cache app data
B- Use containerization for critical corporate data
C- Use query string while handling sensitive data
D- Allow apps to save passwords to avoid multiple logins

Answer:

B

Explanation:

Containerization is a practice that helps security professionals protect mobile applications from various attacks. Containerization is a technique that isolates critical corporate data from the rest of the device data and applications. Containerization creates a secure and encrypted environment on the device where the corporate data and applications can be accessed and managed. This way, containerization prevents unauthorized access, data leakage, malware infection, or device theft from compromising the corporate data and applications12. Reference: Network Defense Essentials - EC-Council Learning, Mobile Application Security:

Containerization vs. App Wrapping vs. SDK

Question 8

Question Type: MultipleChoice

Which of the following acts was enacted in 2002 and aims to protect the public and investors by increasing the accuracy and reliability of corporate disclosures?

Options:

A- Sarbanes-Oxley Act (SOX)
B- Digital Millennium Copyright Act (DMCA)
C- Gramm-Leach-Bliley Act
D- Payment Card Industry-Data Security Standard (PCI-DSS)

Answer:

A

Explanation:

The Sarbanes-Oxley Act (SOX) is a US law that was enacted in 2002 in response to the corporate scandals involving Enron, WorldCom, and others. The SOX aims to protect the public and investors by increasing the accuracy and reliability of corporate disclosures, such as financial statements, audit reports, and internal controls. The SOX also establishes the Public Company Accounting Oversight Board (PCAOB) to oversee the auditing of public companies and imposes criminal penalties for fraud and non-compliance12. Reference: Network Defense Essentials - EC-Council Learning, Sarbanes-Oxley Act of 2002 (SOX) | U.S. Department of Labor

Question 9

Question Type: MultipleChoice

Alice was working on her major project; she saved all her confidential files and locked her laptop. Bob wanted to access Alice's laptop for his personal use but was unable to access the laptop due to biometric authentication.

Which of the following network defense approaches was employed by Alice on her laptop?

Options:

A- Retrospective approach
B- Preventive approach
C- Reactive approach
D- Proactive approach

Answer:

B

Explanation:

The network defense approach that was employed by Alice on her laptop was the preventive approach. The preventive approach aims to stop or deter potential attacks before they happen by implementing security measures that reduce the attack surface and increase the difficulty of exploitation. Biometric authentication is an example of a preventive measure that uses a physical characteristic, such as a fingerprint, iris, or face, to verify the identity of the user and grant access to the device or system. Biometric authentication is more secure than traditional methods, such as passwords or PINs, because it is harder to forge, guess, or steal. By locking her laptop and using biometric authentication, Alice prevented Bob from accessing her laptop and her confidential files without her permission. Reference:

Network Defense Essentials Courseware, EC-Council, 2020, pp. 1-7 to 1-8

What is Biometric Authentication?, Norton, July 29, 2020

An introduction to network defense basics, Enable Sysadmin, November 26, 2019

Question 10

Question Type: MultipleChoice

In an organization, employees are restricted from using their own storage devices, and only the company's portable storage devices are allowed. As employees are carrying the company's portable device outside their premises, the data should be protected from unauthorized access.

Which of the following techniques can be used to protect the data in a portable storage device?

Options:

A- Data retention
B- Data encryption
C- Data resilience
D- Disk mirroring

Answer:

B

Explanation:

Data encryption is the technique that can be used to protect the data in a portable storage device. Data encryption is the process of transforming data into an unreadable format using a secret key or algorithm. Only authorized parties who have the correct key or algorithm can decrypt and access the data. Data encryption provides security and privacy for the data stored on a portable storage device, such as a USB flash drive or an external hard drive, by preventing unauthorized access, modification, or disclosure. If the device is lost or stolen, the data will remain protected and inaccessible to the unauthorized user. Data encryption can be implemented using software or hardware solutions, such as BitLocker, VeraCrypt, or encrypted USB drives. Data encryption is one of the best practices for securely storing data on portable devices123. Reference:

7 Ways to Secure Sensitive Data on a USB Flash Drive, UpGuard, August 17, 2022

How to Protect Data on Portable Drives, PCWorld, January 10, 2011

Securely Storing Data, Security.org, December 20, 2022

Question 11

Question Type: MultipleChoice

Which of the following types of network segmentation is an easy approach to divide a network but can be expensive as it occupies more space?

Options:

A- VLAN segmentation
B- Logical segmentation
C- Network virtualization
D- Physical segmentation

Answer:

D

Question 12

Question Type: MultipleChoice

Which of the following ISO standards provides guidance to ensure that cloud service providers offer appropriate information security controls to protect the privacy of their customer's clients by securing personally identifiable information entrusted to them?

Options:

A- ISO/IEC 27001
B- ISO/IEC 27018
C- ISO/IEC 27011
D- ISO/IEC 27007

Answer:

B

Explanation:

ISO/IEC 27018 is the ISO standard that provides guidance to ensure that cloud service providers offer appropriate information security controls to protect the privacy of their customer's clients by securing personally identifiable information entrusted to them. ISO/IEC 27018 is a code of practice for protecting personal information in cloud storage. The term for the personal data it covers is Personally Identifiable Information or PII. ISO/IEC 27018 is an addendum to ISO/IEC 27001, the first international code of practice for cloud privacy. It helps cloud service providers who process PII to assess risk and implement controls for protecting PII. ISO/IEC 27018 was created in 2014 and updated in 2019. It has the following objectives:

Help the public cloud service provider to comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through contract.

Enable the public cloud PII processor to be transparent in relevant matters so that cloud service customers can select well-governed cloud-based PII processing services.

Assist the cloud service customer and the public cloud PII processor in entering into a contractual agreement.

Provide cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where individual cloud service customer audits of data hosted in a

multiparty, virtualized server (cloud) environment can be impractical technically and can increase risks to those physical and logical network security controls in place123.

ISO/IEC 27018: Protecting PII in Public Clouds - ISMS.online, ISMS.online, 2019

ISO/IEC 27018 - Wikipedia, Wikipedia, 2021

ISO/IEC 27018:2019 - Information technology --- Security techniques --- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, ISO, 2019

Question 13

Question Type: MultipleChoice

Stephen, a security specialist, was instructed to identify emerging threats on the organization's network. In

this process, he employed a computer system on the Internet intended to attract and trap those who

attempt unauthorized host system utilization to penetrate the organization's network.

Identify the type of security solution employed by Stephen in the above scenario.

Options:

A- Firewall
B- Honeypot
C- IDS
D- Proxy server

Answer:

B

To Get Premium Files for 112-51 Visit

https://www.p2pexams.com/products/112-51

For More Free Questions Visit

https://www.p2pexams.com/eccouncil/pdf/112-51