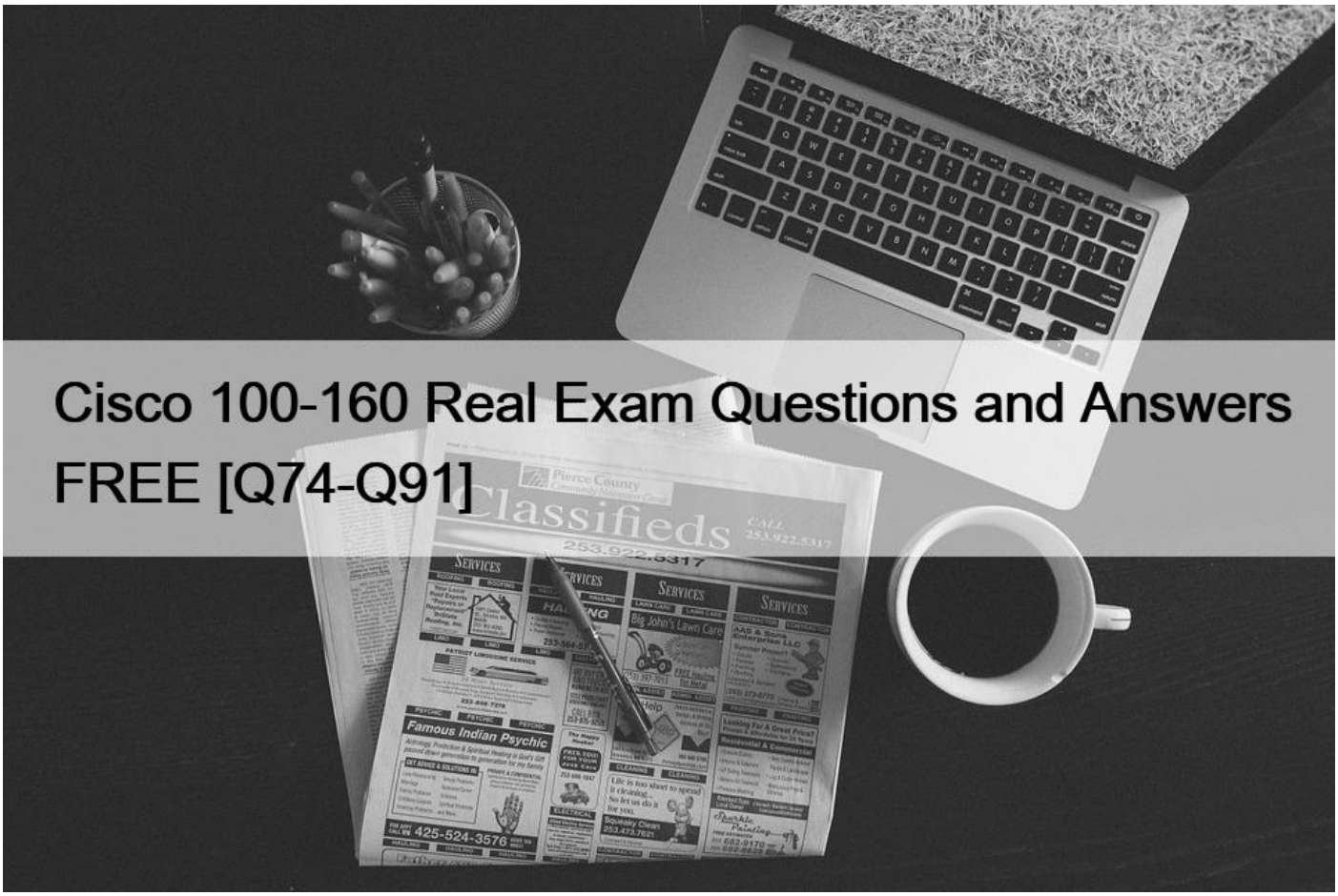
Cisco 100-160 Real Exam Questions and Answers FREE [Q74-Q91



Cisco 100-160 Real Exam Questions and Answers FREE
Exam Dumps 100-160 Practice Free Latest Cisco Practice Tests

QUESTION 74

Why is it important to stay current with automated threat intelligence technologies?
* All of the above
* To leverage the latest advancements in machine learning and AI
* To enhance the effectiveness of security measures
* To adapt to evolving cybersecurity threats

Staying current with automated threat intelligence technologies is vital in the field of cybersecurity. Firstly, as cyber threats continuously evolve, staying up to date allows organizations to adapt their defenses and countermeasures accordingly. Secondly, leveraging the latest advancements in machine learning and artificial intelligence helps improve the accuracy and efficiency of threat detection and response. Lastly, by staying current, organizations can enhance the overall effectiveness of their security measures and stay ahead of potential threats.

QUESTION 75

What is the purpose of a firewall in a network security system?
* To prevent unauthorized access to or from private networks
* To scan and filter network traffic for potential threats
* To encrypt data transmitted over the network
* To provide secure remote access to the network

Option 1: Correct. A firewall is designed to prevent unauthorized access to or from private networks by monitoring and controlling network traffic based on predetermined security rules.

Option 2: Incorrect. While a firewall can scan and filter network traffic for potential threats, this is not its primary purpose.

Option 3: Incorrect. While encryption may be a feature of some firewalls, it is not the primary purpose of a firewall in a network security system.

Option 4: Incorrect. While a secure remote access solution may include a firewall, this is not the primary purpose of a firewall in a network security system.

QUESTION 76

What is the purpose of app distribution in cybersecurity?
* Deploying network firewalls
* Testing the security of applications
* Configuring access control policies
* Distributing security patches and updates

App distribution in cybersecurity refers to the process of distributing security patches and updates for applications. This is vital in maintaining the security of software and preventing vulnerabilities from being exploited. By regularly distributing and installing updates, organizations can address known security flaws, improve application performance, and ensure that their systems remain protected against emerging threats.

QUESTION 77

What is a common security threat in which an attacker attempts to overwhelm a targeted system by flooding it with Internet traffic?
* Ransomware
* Distributed Denial of Service (DDoS) attack
* Phishing
* SQL injection

Option 1: Ransomware is a type of malicious software that encrypts a victim’s files and demands a ransom in exchange for the decryption key. While it can cause damage to systems, it is not specifically designed to overwhelm a system with Internet traffic.

Option 2: Correct. A Distributed Denial of Service (DDoS) attack is a common security threat in which an attacker attempts to overwhelm a targeted system by flooding it with Internet traffic. This can result in a loss of service availability for legitimate users.

Option 3: Phishing is a type of social engineering attack in which an attacker masquerades as a trustworthy entity to trick individuals into providing sensitive information. It does not involve overwhelming a system with Internet traffic.

Option 4: SQL injection is a type of web application attack in which an attacker manipulates a SQL query to gain unauthorized access to a database. It does not involve overwhelming a system with Internet traffic.

QUESTION 78

Which of the following is a security best practice for securing data in the cloud?

* Storing sensitive data in clear text
* Implementing multi-factor authentication
* Allowing unrestricted access to data
* Using weak passwords

Option 1: Incorrect. Storing sensitive data in clear text is not a security best practice. It leaves the data vulnerable to unauthorized access and breaches.

Option 2: Correct. Implementing multi-factor authentication is a security best practice for securing data in the cloud. This adds an extra layer of protection by requiring users to provide additional verification beyond just a password.

Option 3: Incorrect. Allowing unrestricted access to data is not a security best practice. Access to data should be properly controlled and limited to authorized individuals or groups.

Option 4: Incorrect. Using weak passwords is not a security best practice. Strong and complex passwords should be used to prevent unauthorized access to data.

QUESTION 79

What is the purpose of an Access Control List (ACL) in cybersecurity?

* To encrypt traffic between two networks
* To filter network traffic based on predefined rules
* To monitor network traffic for potential security threats
* To authenticate users before granting them access

An Access Control List (ACL) is a list of rules that determines which network traffic is allowed and which is denied. It is used to filter network traffic based on criteria such as source/destination IP address, port numbers, and protocols. By implementing an ACL, organizations can control access to their networks, prevent unauthorized access, and enforce security policies.

QUESTION 80

Which technology is responsible for monitoring network traffic and identifying potential threats?

* IDS
* Firewall
* Server
* IPS

An Intrusion Detection System (IDS) is a technology that monitors network traffic and analyzes it for potential security breaches or vulnerabilities. It detects and alerts administrators to any suspicious activity, allowing them to take appropriate actions to mitigate potential threats.

QUESTION 81

Which of the following is an element of an incident response plan?

* Installing antivirus software
* Conducting regular backups
* Developing security policies
* Identifying vulnerabilities

An incident response plan outlines the steps and procedures to be followed when a cybersecurity incident occurs. One of the elements of an incident response plan is developing security policies. These policies serve as a framework for managing and responding to security incidents.

QUESTION 82

Which of the following helps to ensure the confidentiality of data in computer operations?
* Data integrity controls
* Access control lists (ACLs)
* Intrusion Detection System (IDS)
* Antivirus software

Access control lists (ACLs) are a security mechanism used in computer operations to enforce and manage access permissions for users and resources. ACLs enable organizations to control who can access specific data or resources, helping to ensure the confidentiality of sensitive information.

QUESTION 83

Which of the following is a common authentication protocol used in wireless networks?
* FTP
* WPA
* SSH
* SMTP

WPA (Wi-Fi Protected Access) is a widely used authentication protocol for securing wireless networks. It provides stronger security than the older WEP (Wired Equivalent Privacy) protocol by utilizing encryption algorithms and dynamic key generation. WPA offers better protection against unauthorized access and helps ensure the confidentiality and integrity of wireless communications.

QUESTION 84

Which of the following best describes the main purpose of malware removal?
* To disinfect network devices from malware infections
* To secure a system against potential malware attacks
* To detect and remove malware that is already present on a system
* To prevent malware from being installed on a system

Malware removal refers to the process of identifying and eliminating malicious software that has already infected a system. This is essential to prevent further harm and restore the system’s security.

QUESTION 85

Which of the following best defines risk management in the context of cybersecurity?
* The process of analyzing potential threats and determining the likelihood and impact of those threats on an organization.
* The process of ensuring the confidentiality, integrity, and availability of an organization’s information assets.
* The process of mitigating threats to an organization’s information assets by implementing appropriate security controls.
* The process of identifying, assessing, and prioritizing vulnerabilities in an organization’s networks and systems.

Risk management is the process of identifying, assessing, and prioritizing potential threats to an organization’s information assets. By analyzing the likelihood and impact of these threats, organizations can make informed decisions on how to mitigate risks effectively. This process involves activities such as risk assessment, risk analysis, risk mitigation, and risk monitoring. The focus is on evaluating the probability and impact of potential cybersecurity incidents and implementing appropriate measures to reduce or eliminate these risks.

QUESTION 86

Which of the following is a common security threat that targets web applications?
* SQL injection
* DNS poisoning
* Man-in-the-middle attack

* Distributed Denial of Service (DDoS)

Option 1: Correct: SQL injection is a common security threat that targets web applications. It involves inserting malicious SQL code into input fields to manipulate the application’s database and gain unauthorized access or retrieve sensitive information.

Option 2: Incorrect: DNS poisoning is not a common security threat that targets web applications. It involves corrupting the DNS cache and redirecting users to malicious websites.

Option 3: Incorrect: Man-in-the-middle attack is not a common security threat that specifically targets web applications. It involves intercepting communication between two parties and can affect various types of network communication.

Option 4: Incorrect: Distributed Denial of Service (DDoS) is not a common security threat that targets web applications specifically. It involves overwhelming a target system with a flood of traffic from multiple sources, rendering it inaccessible.

QUESTION 87

What is meant by the term “collective intelligence” in the context of cybersecurity?

* Intelligence gathered by individuals or organizations without sharing it with others.
* Intelligence gathered from publicly available sources.
* Intelligence collected through collaboration and information sharing among individuals or organizations.
* Intelligence collected through automated threat intelligence platforms.

Collective intelligence refers to the practice of pooling knowledge, insights, and resources from multiple individuals or organizations to enhance cybersecurity. It involves collaboration, information sharing, and coordinated efforts to identify and mitigate threats collectively. By leveraging the collective intelligence, cybersecurity practitioners can gain a broader view of the threat landscape, share threat intelligence, and develop effective strategies to combat cyber threats.

QUESTION 88

Which of the following is a primary goal of monitoring security events “as they occur”?

* To detect and respond to security incidents in a timely manner
* To enforce security policies and access controls
* To ensure zero incidents and vulnerabilities in the network
* To meet regulatory compliance requirements

Monitoring security events “as they occur” is primarily aimed at quickly identifying and responding to security incidents. By continuously monitoring for potential threats and vulnerabilities, organizations can detect and mitigate security incidents in a timely manner, minimizing damage and reducing downtime.

QUESTION 89

Which type of encryption protects data while it is being transmitted over a network?

* Transport Layer Security (TLS)
* Asymmetric encryption
* Symmetric encryption
* Hash encryption

Transport Layer Security (TLS) is a cryptographic protocol that provides secure communication over a network. It ensures the confidentiality and integrity of data while in transit by encrypting it. TLS is commonly used to protect sensitive information during online transactions, such as credit card numbers or login credentials.

QUESTION 90

Which network infrastructure component allows for the translation of domain names to IP addresses?

* Firewall
* Router
* DNS server
* DHCP server

DNS (Domain Name System) is a network infrastructure component that translates domain names (e.g., www.example.com) into their corresponding IP addresses (e.g., 192.168.1.1). DNS servers maintain a distributed database that maps domain names to IP addresses, allowing users to access websites and other resources using easy-to-remember names instead of complex IP addresses.

QUESTION 91

Which of the following best describes the concept of automation in cybersecurity testing?

* Implementing security controls to prevent attacks
* Using software and tools to automatically conduct security tests
* Performing physical tests on network infrastructure
* Conducting manual security tests

Automation in cybersecurity testing involves using software and tools to automatically conduct security tests. This approach helps to increase efficiency and accuracy by automating repetitive tasks, such as vulnerability scanning, penetration testing, and log analysis. It allows for the identification of security issues and vulnerabilities in a timely manner.