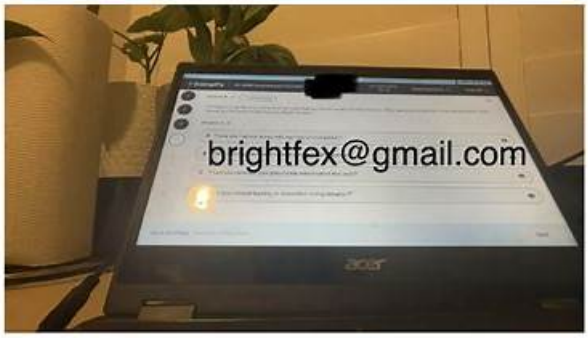
Pass4sure 212-82 Pass Guide | Practice 212-82 Exam



BONUS!!! Download part of Test4Sure 212-82 dumps for free: https://drive.google.com/open?id=1NBJkHkHRicT4SjYKpRWw889NfesO99d6

As the development of the science and technologies, there are a lot of changes coming up with the design of our 212-82 exam questions. We are applying new technology to perfect the 212-82 study materials. Through our test, the performance of our 212-82 learning quide becomes better than before. In a word, our 212-82 training braindumps will move with the times. Please pay great attention to our 212-82 actual exam.

To become a certified cybersecurity technician, a candidate must pass the 212-82 exam. Certified Cybersecurity Technician certification not only validates the individual's knowledge and skills but also demonstrates their commitment to cybersecurity best practices. 212-82 Exam is designed to test the candidate's ability to identify and mitigate security risks, manage vulnerabilities, and implement security controls.

>> Pass4sure 212-82 Pass Guide <<

Practice 212-82 Exam, Valid 212-82 Test Sims

We can't forget the advantages and the conveniences that reliable 212-82 study materials complied by our companies bring to us. First, by telling our customers what the key points of learning, and which learning 212-82 method is available, they may save our customers money and time. They guide our customers in finding suitable jobs and other information as well. Secondly, a wide range of practice types and different version of our 212-82 Study Materials receive technological support through our expert team.

ECCouncil Certified Cybersecurity Technician Sample Questions (Q122-

Q127):

NEW QUESTION # 122
Lorenzo, a security professional in an MNC, was instructed to establish centralized authentication, authorization, and accounting for remote-access servers. For this purpose, he implemented a protocol that is based on the client-server model and works at the transport layer of the OSI model. Identify the remote authentication protocol employed by Lorenzo in the above scenario.

- A. RADIUS
- B. POP3S
- C. IMAPS
- D. SNMPv3

Answer: A

Explanation:
It identifies the remote authentication protocol employed by Lorenzo in the above scenario.
RADIUS (Remote Authentication Dial-In User Service) is a protocol that provides centralized authentication, authorization, and accounting (AAA) for remote-access servers such as VPNs (Virtual Private Networks), wireless networks, or dial-up connections. RADIUS is based on the client-server model and works at the transport layer of the OSI model. RADIUS uses UDP (User Datagram Protocol) as its transport protocol and encrypts only user passwords in its messages.
In the above scenario, Lorenzo implemented RADIUS to provide centralized AAA for remote- access servers.

NEW QUESTION # 123
Wilson, a security specialist in an organization, was instructed to enhance its cloud network security. To achieve this, Wilson deployed a network routing solution that established and managed communication between the on-premises consumer network and VPCs via a centralized unit. Identity the method used by Wilson to achieve cloud network security in this scenario.

- A. VPC endpoint
- B. Public and private subnets
- C. Virtual private cloud (VPC)
- D. Transit gateways

Answer: D

Explanation:
Transit gateways are the method used by Wilson to achieve cloud network security in this scenario. Cloud network security is a branch of cybersecurity that focuses on protecting and securing the network infrastructure and traffic in a cloud environment. Cloud network security can involve various methods or techniques, such as encryption, firewall, VPN, IDS/IPS, etc. Transit gateways are a method of cloud network security that provide a network routing solution that establishes and manages communication between on-premises consumer networks and VPCs (Virtual Private Clouds) via a centralized unit . Transit gateways can be used to simplify and secure the connectivity between different networks or VPCs in a cloud environment . In the scenario, Wilson was instructed to enhance its cloud network security. To achieve this, Wilson deployed a network routing solution that established and managed communication between the on-premises consumer network and VPCs via a centralized unit. This means that he used transit gateways for this purpose. A virtual private cloud (VPC) is not a method of cloud network security, but a term that describes an isolated and private section of a public cloud that provides exclusive access to cloud resources to a single organization or entity . A VPC can be used to create and configure virtual networks in a cloud environment .
Public and private subnets are not methods of cloud network security, but terms that describe segments of a VPC that have different levels of accessibility orvisibility . A public subnet is a segment of a VPC that can be accessed from the internet or other networks . A private subnet is a segment of a VPC that cannot be accessed from the internet or other networks . A VPC endpoint is not a method of cloud network security, but a term that describes an interface that allows private connectivity between a VPC and other AWS (Amazon Web Services) services or resources .

NEW QUESTION # 124
As the director of cybersecurity for a prominent financial Institution, you oversee the security protocols for a vast array of digital operations. The institution recently transitioned to a new core banking platform that integrates an artificial intelligence (Al)-based fraud detection system. This system monitors real-time transactions, leveraging pattern recognition and behavioral analytics.
A week post-transition, you are alerted to abnormal behavior patterns in the Al system. On closer examination, the system is mistakenly flagging genuine transactions as fraudulent, causing a surge in false positives. This not only disrupts the customers' banking

experience but also strains the manual review team. Preliminary investigations suggest subtle data poisoning attacks aiming to compromise the AI's training data, skewing its decision-making ability. To safeguard the AI-based fraud detection system and maintain the integrity of your financial data, which of the following steps should be your primary focus?

- A. Migrate back to the legacy banking platform until the new system is thoroughly vetted and all potential vulnerabilities are addressed.
- B. Engage in extensive customer outreach programs, urging them to report any discrepancies in their transaction records, and manually verifying flagged transactions.
- C. Liaise with third-party cybersecurity firms to conduct an exhaustive penetration test on the entire core banking platform, focusing on potential data breach points.
- D. Collaborate with the AI development team to retrain the model using only verified transaction data and implement real time monitoring to detect data poisoning attempts.

Answer: D

Explanation:
To address the issue of the AI-based fraud detection system flagging genuine transactions as fraudulent due to data poisoning, the primary focus should be on:
* Retraining the AI Model:
* Verified Data: Use only verified, clean transaction data to retrain the model. This helps to eliminate any compromised data that might be skewing the AI's decision-making process.
* Model Integrity: Ensure the integrity of the training data to prevent future data poisoning attempts.
* Real-Time Monitoring:
* Detection Systems: Implement real-time monitoring to detect any attempts at data poisoning as they happen. This involves setting up alerts for abnormal patterns that could indicate malicious
* activity.
* Continuous Learning: Integrate continuous learning systems that can adapt and respond to new threats in real-time, ensuring the AI system remains robust against evolving attack vectors.
References:
* NIST guidelines on AI and data integrity:NIST AI
* Research on data poisoning and mitigation techniques:IEEE Xplore

NEW QUESTION # 125
Myles, a security professional at an organization, provided laptops for all the employees to carry out the business processes from remote locations. While installing necessary applications required for the business, Myles has also installed antivirus software on each laptop following the company's policy to detect and protect the machines from external malicious events over the Internet.
Identify the PCI-DSS requirement followed by Myles in the above scenario.

- A. PCI-DSS requirement no 1.3.1
- B. PCI-DSS requirement no 5.1
- C. PCI-DSS requirement no 1.3.5
- D. PCI-DSS requirement no 1.3.2

Answer: B

NEW QUESTION # 126
Charlie, a security professional in an organization, noticed unauthorized access and eavesdropping on the WLAN. To thwart such attempts, Charlie employed an encryption mechanism that used the RC4 algorithm to encrypt information in the data link layer.
Identify the type of wireless encryption employed by Charlie in the above scenario.

- A. CCMP
- B. AES
- C. WEP
- D. TKIP

Answer: C

Explanation:
WEP is the type of wireless encryption employed by Charlie in the above scenario. Wireless encryption is a technique that involves

encoding or scrambling the data transmitted over a wireless network to prevent unauthorized access or interception. Wireless encryption can use various algorithms or protocols to encrypt and decrypt the data, such as WEP, WPA, WPA2, etc.
WEP (Wired Equivalent Privacy) is a type of wireless encryption that uses the RC4 algorithm to encrypt information in the data link layer.WEP can be used to provide basic security and privacy for wireless networks, but it can also be easily cracked or compromised by various attacks.In the scenario, Charlie, a security professional in an organization, noticed unauthorized access and eavesdropping on the WLAN (Wireless Local Area Network). To thwart such attempts, Charlie employed an encryption mechanism that used the RC4 algorithm to encrypt information in the data link layer. This means that he employed WEP for this purpose. TKIP (Temporal Key Integrity Protocol) is a type of wireless encryption that uses the RC4 algorithm to encrypt information in the data link layer with dynamic keys.TKIP can be used to provide enhanced security and compatibility for wireless networks, but it can also be vulnerable to certain attacks.AES (Advanced Encryption Standard) is a type of wireless encryption that uses the Rijndael algorithm to encrypt information in the data link layer with fixed keys.AES can be used to provide strong security and performance for wireless networks, but it can also require more processing power and resources.CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is a type of wireless encryption that uses the AES algorithm to encrypt information in the data link layer with dynamic keys.CCMP can be used to provide robust security and reliability for wireless networks, but it can also require more processing power and resources.

NEW QUESTION # 127
.....

ECCouncil 212-82 reliable brain dumps are promised to help you clear your 212-82 test certification with high scores. 212-82 questions & answers will contain comprehensive knowledge, which will ensure high hit rate and best pass rate. When you choose 212-82 Pdf Torrent, you will get your 212-82 certification with ease, which will be the best choice to accelerate your career as a professional in the Information Technology industry.