Pass Guaranteed 2026 ECCouncil 212-82: Certified Cybersecurity Technician Marvelous Test Discount Voucher

P.S. Free & New 212-82 dumps are available on Google Drive shared by Pass4Test: https://drive.google.com/open?id=1FLxcuZzAF7B5T3pgv8sZje2gb-LgktcW

As a working person, the ECCouncil 212-82 practice exam will be a great help because you are left with little time to prepare for the ECCouncil 212-82 certification exam which you cannot waste to make time for the ECCouncil 212-82 Exam Questions. You can find yourself sitting in your dream office and enjoying the new opportunity.

If you want to make progress and mark your name in your circumstances, you should never boggle at difficulties. As far as we know, many customers are depressed by the exam ahead of them, afraid of they may fail it unexpectedly. Our 212-82 exam torrents can pacify your worries and even help you successfully pass it. The shortage of necessary knowledge of the exam may make you waver, while the abundance of our 212-82 Study Materials can boost your confidence increasingly.

>> 212-82 Test Discount Voucher <<

Pass 212-82 Exam with Realistic 212-82 Test Discount Voucher by Pass4Test

Pass4Test is an excellent platform where you get relevant, credible, and unique ECCouncil 212-82 exam dumps designed according to the specified pattern, material, and format as suggested by the ECCouncil 212-82 exam. To make the ECCouncil 212-82 Exam Questions content up-to-date for free of cost up to 365 days after buying them, our certified trainers work strenuously to formulate the exam questions in compliance with the ECCouncil 212-82 dumps.

ECCouncil 212-82 Certification is an excellent way for individuals to demonstrate their expertise in cybersecurity. It is a valuable credential for those seeking employment in the cybersecurity industry. Employers often look for candidates with this certification because it shows that the individual has a good understanding of the core concepts and practices of cybersecurity.

ECCouncil 212-82 Exam is an industry-recognized certification that is highly valued by employers in the cybersecurity industry. Certified Cybersecurity Technician certification is especially important for individuals who are just starting their careers in cybersecurity and are looking for ways to differentiate themselves from other job applicants. Certified Cybersecurity Technician certification can also help individuals who are looking to advance their careers and take on more senior roles within their organizations.

ECCouncil Certified Cybersecurity Technician Sample Questions (Q133-Q138):

NEW QUESTION # 133
An organization divided its IT infrastructure into multiple departments to ensure secure connections for data access. To provide high-

speed data access, the administrator implemented a PAID level that broke data into sections and stored them across multiple drives. The storage capacity of this RAID level was equal to the sum of disk capacities in the set. which of the following RAID levels was implemented by the administrator in the above scenario?

- A. RAID Level 5
- B. RAID Level 1
- C. RAID Level 3
- D. RAID Level 0

Answer: D

Explanation:
RAID Level 0 is the RAID level that was implemented by the administrator in the above scenario. RAID Level 0 is also known as striping, which breaks data into sections and stores them across multiple drives. RAID Level 0 provides high-speed data access and increases performance, but it does not provide any redundancy or fault tolerance. The storage capacity of RAID Level 0 is equal to the sum of disk capacities in the set3. Reference: RAID Level 0

NEW QUESTION # 134
In an organization, all the servers and database systems are guarded in a sealed room with a single-entry point. The entrance is protected with a physical lock system that requires typing a sequence of numbers and letters by using a rotating dial that intermingles with several other rotating discs. Which of the following types of physical locks is used by the organization in the above scenario?

- A. Mechanical locks
- B. Combination locks
- C. Digital locks
- D. Electromagnetic locks

Answer: B

Explanation:
It identifies the type of physical lock used by the organization in the above scenario. A physical lock is a device that prevents unauthorized access to a door, gate, cabinet, or other enclosure by using a mechanism that requires a key, code, or biometric factor to open or close it. There are different types of physical locks, such as:
Combination lock: This type of lock requires typing a sequence of numbers and letters by using a rotating dial that intermingles with several other rotating discs. This type of lock is suitable for securing safes, lockers, or cabinets that store valuable items or documents.
Digital lock: This type of lock requires entering a numeric or alphanumeric code by using a keypad or touchscreen. This type of lock is suitable for securing doors or gates that require frequent access or multiple users.
Mechanical lock: This type of lock requires inserting and turning a metal key that matches the shape and size of the lock. This type of lock is suitable for securing doors or gates that require simple and reliable access or single users.
Electromagnetic lock: This type of lock requires applying an electric current to a magnet that attracts a metal plate attached to the door or gate. This type of lock is suitable for securing doors or gates that require remote control or integration with other security systems.
In the above scenario, the organization used a combination lock that requires typing a sequence of numbers and letters by using a rotating dial that intermingles with several other rotating discs.

NEW QUESTION # 135
Initiate an SSH Connection to a machine that has SSH enabled in the network. After connecting to the machine find the file flag.txt and choose the content hidden in the file. Credentials for SSH login are provided below:
Hint:
Username: sam
Password: admin@l23

- A. sam@bob
- B. sam2@bob
- C. bob@sam
- D. bob2@sam

Answer: C

Explanation:
Quid pro quo is the social engineering technique that Johnson employed in the above scenario. Social engineering is a technique that involves manipulating or deceiving people into performing actions or revealing information that can be used for malicious purposes. Social engineering can be performed through various methods, such as phone calls, emails, websites, etc. Quid pro quo is a social engineering method that involves offering a service or a benefit in exchange for information or access. Quid pro quo can be used to trick victims into believing that they are receiving help or assistance from a legitimate source, while in fact they are compromising their security or privacy . In the scenario, Johnson performed quid pro quo by claiming himself to represent a technical support team from a vendor and offering to help sibertech.org with a server issue, while in fact he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine. Diversion theft is a social engineering method that involves diverting the delivery or shipment of goods or assets to a different location or destination. Elicitation is a social engineering method that involves extracting information from a target by engaging them in a conversation or an interaction. Phishing is a social engineering method that involves sending fraudulent emails or messages that appear to come from a trusted source, such as a bank, a company, or a person, and asking the recipient to click on a link, open an attachment, or provide personal or financial information.

NEW QUESTION # 136
Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them. What is the technique used by Kevin to evade the IDS system?

- A. Urgency flag
- B. Obfuscating
- C. Session splicing
- D. Desynchronization

Answer: B

Explanation:
Obfuscating is the technique used by Kevin to evade the IDS system in the above scenario. Obfuscating is a technique that involves encoding or modifying packets or data with various methods or characters to make them unreadable or unrecognizable by an IDS (Intrusion Detection System). Obfuscating can be used to bypass or evade an IDS system that relies on signatures or patterns to detect malicious activities. Obfuscating can include encoding packets with Unicode characters, which are characters that can represent various languages and symbols. The IDS system cannot recognize the packet, but the target web server can decode them and execute them normally. Desynchronization is a technique that involves creating discrepancies or inconsistencies between the state of a connection as seen by an IDS system and the state of a connection as seen by the end hosts. Desynchronization can be used to bypass or evade an IDS system that relies on stateful inspection to track and analyze connections. Desynchronization can include sending packets with invalid sequence numbers, which are numbers that indicate the order of packets in a connection. Session splicing is a technique that involves splitting or dividing packets or data into smaller fragments or segments to make them harder to detect by an IDS system. Session splicing can be used to bypass or evade an IDS system that relies on packet size or content to detect malicious activities. Session splicing can include sending packets with small MTU (Maximum Transmission Unit) values, which are values that indicate the maximum size of packets that can be transmitted over a network. An urgency flag is a flag in the TCP (Transmission Control Protocol) header that indicates that the data in the packet is urgent and should be processed immediately by the receiver. An urgency flag is not a technique to evade an IDS system, but it can be used to trigger an IDS system to generate an alert or a response.

NEW QUESTION # 137
A company decided to implement the cloud infrastructure within its corporate firewall 10 secure sensitive data from external access. The company invested heavily in creating a cloud architecture within its premises to manage full control over its corporate data. Which of the following types of cloud deployment models did the company implement in this scenario?

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

Answer: C

Explanation:
Private cloud is the type of cloud deployment model that the company implemented in this scenario. Cloud computing is a model that

provides on-demand access to shared and scalable computing resources, such as servers, storage, networks, applications, etc., over the internet or a network. Cloud computing can have different types based on its service or deployment model. A cloud deployment model defines how and where the cloud infrastructure and services are hosted and accessed.A cloud deployment model can have different types, such as public cloud, private cloud, hybrid cloud, community cloud, etc. A private cloud is a type of cloud deployment model that provides exclusive access to cloud infrastructure and services to a single organization or entity.A private cloud can be hosted within or outside the organization's premises and managed by the organization or a third-party provider.A private cloud can be used to secure sensitive data from external access and maintain full control over the corporate data.In the scenario, the company decided to implement the cloud infrastructure within its corporate firewall to secure sensitive data from external access. The company invested heavily in creating a cloud architecture within its premises to manage full control over its corporate data. This means that the company implemented a private cloud for this purpose. A multi-cloud is not a type of cloud deployment model, but a term that describes a strategy that uses multiple public or private clouds from different providers for different purposes or functions.A public cloud is a type of cloud deployment model that provides open access to cloud infrastructure and services to multiple organizations or entities over the internet.A public cloud can be hosted and managed by a third- party provider that owns and operates the cloud infrastructure and services.A community cloud is a type of cloud deployment model that provides shared access to cloud infrastructure and services to multiple organizations or entities that have common interests or goals.

NEW QUESTION # 138

.....