How to Prepare For 212-82 Exam?

2025 Latest VCEDumps 212-82 PDF Dumps and 212-82 Exam Engine Free Share: https://drive.google.com/open?id=1_2k3hwiTAPmUftHjJxm-N3zf3AW0DPDI

Our 212-82 study materials can provide you with multiple modes of experience, there are three main modes to choose from: PDF, Software and Online. Firstly, the PDF version is printable. Secondly, the Software version of 212-82 exam questions can simulate the real exam environment to give you exam experience more vividly. Thirdly, the online version supports all web browsers so that it can be worked on all the operating systems. And our 212-82 Study Materials will help you in a more relaxed learning atmosphere to pass the 212-82 exam.

ECCouncil 212-82 (Certified Cybersecurity Technician) certification exam is designed for individuals who want to demonstrate their knowledge and skills in the field of cybersecurity. Certified Cybersecurity Technician certification is ideal for technicians, network administrators, and other IT professionals who want to advance their careers and prove their expertise in cybersecurity. 212-82 exam covers a wide range of topics including network security, incident response, malware analysis, and vulnerability assessment.

The EC-Council 212-82 (Certified Cybersecurity Technician) exam is an entry-level certification that is ideal for individuals who are looking to start their career in cybersecurity or switch their career path to cybersecurity. 212-82 Exam covers a wide range of topics and is vendor-neutral, which means that it is not affiliated with any particular technology or solution. 212-82 exam is computer-based and can be taken at any Pearson VUE testing center worldwide. Certified Cybersecurity Technician certification is valid for three years and can be renewed by taking a recertification exam or earning continuing education credits.

>> 212-82 Exam Certification <<

Advantages Of ECCouncil 212-82 PDF Dumps Format

Our 212-82 test questions can help you have a good preparation for exam effectively. Also you don't need to worry about if our 212-82 study materials are out of validity. We provide one year free updates for every buyer, after purchasing you can download our latest version of 212-82 Training Questions always within one year. And if you have any question on our 212-82 learning guide, you can contact with our service at any time, we will help you pass the 212-82 exam with our high quality of 212-82 exam questions and good service.

ECCouncil Certified Cybersecurity Technician Sample Questions (Q74-Q79):

NEW QUESTION # 74
A startup firm contains various devices connected to a wireless network across the floor. An AP with Internet connectivity is placed in a corner to allow wireless communication between devices.
To support new devices connected to the network beyond the APS range, an administrator used a network device that extended the signals of the wireless AP and transmitted it to uncovered area, identify the network component employed by the administrator to extend signals in this scenario.

- A. Wireless repeater
- B. Wireless router
- C. wireless modem

- D. Wireless bridge

Answer: A

Explanation:
Wireless repeater is the network component employed by the administrator to extend signals in this scenario. A wireless network is a type of network that uses radio waves or infrared signals to transmit data between devices without using cables or wires. A wireless network can consist of various components, such as wireless access points (APs), wireless routers, wireless adapters, wireless bridges, wireless repeaters, etc. A wireless repeater is a network component that extends the range or coverage of a wireless signal by receiving it from an AP or another repeater and retransmitting it to another area.A wireless repeater can be used to support new devices connected to the network beyond the AP's range.In the scenario, a startup firm contains various devices connected to a wireless network across the floor. An AP with internet connectivity is placed in a corner to allow wireless communication between devices. To support new devices connected to the network beyond the AP's range, an administrator used a network component that extended the signals of the wireless AP and transmitted it to the uncovered area. This means that he used a wireless repeater for this purpose. A wireless bridge is a network component that connects two or more wired or wireless networks or segments together.A wireless bridge can be used to expand the network or share resources between networks.A wireless modem is a network component that modulates and demodulates wireless signals to enable data transmission over a network.A wireless modem can be used to provide internet access to devices via a cellular network or a satellite network.A wireless router is a network component that performs the functions of both a wireless AP and a router.A wireless router can be used to create a wireless network and connect it to another network, such as the internet.

NEW QUESTION # 75
Andre, a security professional, was tasked with segregating the employees' names, phone numbers, and credit card numbers before sharing the database with clients. For this purpose, he implemented a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#).
Which of the following techniques was employed by Andre in the above scenario?

- A. Hashing
- B. Masking
- C. Bucketing
- D. Tokenization

Answer: B

Explanation:
Masking is the technique that Andre employed in the above scenario. Masking is a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#). Masking can help protect sensitive data from unauthorized access or disclosure, while preserving the format and structure of the original data . Tokenization is a deidentification technique that can replace the critical information in database fields with random tokens that have no meaning or relation to the original data. Hashing is a deidentification technique that can transform the critical information in database fields into fixed-length strings using a mathematical function. Bucketing is a deidentification technique that can group the critical information in database fields into ranges or categories based on certain criteria.

NEW QUESTION # 76
Omar, an encryption specialist in an organization, was tasked with protecting low-complexity applications such as RFID tags, sensor-based applications, and other IbT-based applications. For this purpose, he employed an algorithm for all lower-powered devices that used less power and resources without compromising device security.
identify the algorithm employed by Omar in this scenario.

- A. Lightweight cryptography
- B. Quantum cryptography
- C. Homomorphic encryption
- D. Elliptic curve cryptography

Answer: A

Explanation:
Lightweight cryptography is an algorithm that is designed for low-complexity applications such as RFID tags, sensor-based applications, and other IoT-based applications. Lightweight cryptography uses less power and resources without compromising

device security. Lightweight cryptography can be implemented using symmetric-key algorithms, asymmetric-key algorithms, or hash functions1.
References: Lightweight Cryptography

NEW QUESTION # 77
An employee was fired from his security analyst job due to misconduct. While leaving, he installed a Trojan server on his workstation at 172.30.20.75. As an ethical hacker, you are asked to identify and connect to the Trojan server and explore available files. Enter the name of the VBScript file located in the Pictures folder of the workstation. Hint: You can use one of the Ttojan client applications available at "Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Ttojans (RAT)" of Attacker Machine-1. (Practical Question)

- A. ReboundBlitz
- B. EchoStrike
- C. B00m3rang
- D. Recoil Wave

Answer: B

NEW QUESTION # 78
A pfSense firewall has been configured to block a web application www.abchacker.com. Perform an analysis on the rules set by the admin and select the protocol which has been used to apply the rule.
Hint: Firewall login credentials are given below:
Username: admin
Password: admin@l23

- A. POP3
- B. FTP
- C. ARP
- D. TCP/UDP

Answer: D

Explanation:
TCP/UDP is the protocol that has been used to apply the rule to block the web application www.abchacker.com in the above scenario. pfSense is a firewall and router software that can be installed on a computer or a device to protect a network from various threats and attacks. pfSense can be configured to block or allow traffic based on various criteria, such as source, destination, port, protocol, etc. pfSense rules are applied to traffic in the order they appear in the firewall configuration . To perform an analysis on the rules set by the admin, one has to follow these steps:
Open a web browser and type 20.20.10.26
Press Enter key to access the pfSense web interface.
Enter admin as username and admin@l23 as password.
Click on Login button.
Click on Firewall menu and select Rules option.
Click on LAN tab and observe the rules applied to LAN interface.
The rules applied to LAN interface are:

Action	Interface	Protocol	Source	Port	Destination	Port	Description
Block	LAN	TCP/UDP	any	any	www.abchacker.com	any	Block abchacker website
Pass	LAN	any	any	any	any	any	Default allow LAN to any rule

The first rule blocks any traffic from LAN interface to www.abchacker.com website using TCP/UDP protocol. The second rule allows any traffic from LAN interface to any destination using any protocol. Since the first rule appears before the second rule, it has higher priority and will be applied first. Therefore, TCP/UDP is the protocol that has been used to apply the rule to block the web

application www.abchacker.com. POP3 (Post Office Protocol 3) is a protocol that allows downloading emails from a mail server to a client device. FTP (File Transfer Protocol) is a protocol that allows transferring files between a client and a server over a network. ARP (Address Resolution Protocol) is a protocol that resolves IP addresses to MAC (Media Access Control) addresses on a network.

NEW QUESTION # 79

.....