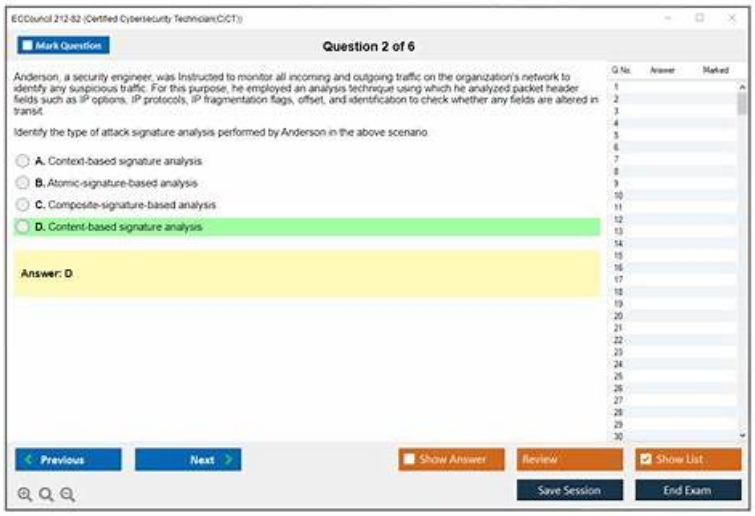
ECCouncil 212-82 Dump Check - 212-82 Reliable Braindumps



DOWNLOAD the newest TestValid 212-82 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1vEcT3MkdCkkg_egi0CR4GB0dhed6cD78

The competition in the ECCouncil field is rising day by day and candidates around the globe are striving to validate their capabilities. Because of the rising competition, candidates lack opportunities to pursue their goals. That is why has launched the ECCouncil 212-82 Exam to assess your capabilities and give you golden career opportunities. Getting a Certified Cybersecurity Technician (212-82) certification after passing the ECCouncil 212-82 exam is proof of the capabilities of a candidate.

ECCouncil 212-82 exam is a challenging and comprehensive exam that requires candidates to have a deep understanding of cybersecurity concepts and technologies. 212-82 exam is designed to test both the theoretical knowledge and practical skills of candidates, ensuring that they are well-equipped to handle real-world cybersecurity challenges. 212-82 exam is also updated regularly to reflect the latest developments in the field, ensuring that certified professionals are up-to-date with the latest cybersecurity trends and technologies.

ECCouncil 212-82 Exam is a valuable certification for individuals who want to pursue a career in cybersecurity. It covers a wide range of topics related to cybersecurity, and it is designed to validate practical knowledge and hands-on experience. Certified Cybersecurity Technician certification is vendor-neutral and widely recognized in the industry, making it an excellent choice for IT professionals who want to enhance their skills in this field.

>> ECCouncil 212-82 Dump Check <<

212-82 Reliable Braindumps, 212-82 Training Pdf

The team appointed by the TestValid is dedicated and hardworking and strives hard to refine the ECCouncil 212-82 dumps and make them meet the standards set by the ECCouncil. It does so by taking the valuable suggestions of more than 90,000 professionals in this field. The unique, trustworthy, and error-free material will turn your preparation for the ECCouncil 212-82 certification exam productive, organized, and helpful.

ECCouncil 212-82 (Certified Cybersecurity Technician) Exam is a certification designed for individuals who are interested in pursuing a career in cybersecurity. Certified Cybersecurity Technician certification is widely recognized in the industry and is a testament to an individual's knowledge and skills in the field of cybersecurity. 212-82 Exam covers a range of topics, including network security, cryptography, ethical hacking, and incident response.

ECCouncil Certified Cybersecurity Technician Sample Questions (Q26-Q31):

NEW QUESTION # 26
An IoT device placed in a hospital for safety measures has sent an alert to the server. The network traffic has been captured and

stored in the Documents folder of the "Attacker Machine-1". Analyze the loTdeviceTraffic.pcapng file and identify the command the loT device sent over the network. (Practical Question)

- A. High_Tcmpe
- B. Low_Tem p e
- C. Temp_High
- D. Tempe_Low

Answer: C

Explanation:
The loT device sent the command Temp_High over the network, which indicates that the temperature in the hospital was above the threshold level. This can be verified by analyzing the loTdeviceTraffic.pcapng file using a network protocol analyzer tool such as Wireshark4. The command Temp_High can be seen in the data field of the UDP packet sent from the loT device (192.168.0.10) to the server (192.168.0.1) at 12:00:03. The screenshot below shows the packet details5: References: Wireshark User's Guide, [loTdeviceTraffic.pcapng]

NEW QUESTION # 27
During which phase of the incident response process are containment and eradication activities performed?

- A. Detection and analysis
- B. Preparation
- C. Recovery
- D. Containment

Answer: D

NEW QUESTION # 28
Riley sent a secret message to Louis. Before sending the message, Riley digitally signed the message using his private key. Louis received the message, verified the digital signature using the corresponding key to ensure that the message was not tampered during transit. Which of the following keys did Louis use to verify the digital signature in the above scenario?

- A. Riley's private key
- B. Louis's private key
- C. Louis's public key
- D. Riley's public key

Answer: D

Explanation:
Riley's public key is the key that Louis used to verify the digital signature in the above scenario. A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document. A digital signature is created by applying a hash function to the message or document and then encrypting the hash value with the sender's private key. A digital signature can be verified by decrypting the hash value with the sender's public key and comparing it with the hash value of the original message or document.Riley's public key is the key that corresponds to Riley's private key, which he used to sign the message. Louis's public key is the key that corresponds to Louis's private key, which he may use to encrypt or decrypt messages with Riley.
Louis's private key is the key that only Louis knows and can use to sign or decrypt messages.
Riley's private key is the key that only Riley knows and can use to sign or encrypt messages.

NEW QUESTION # 29
A threat intelligence feed data file has been acquired and stored in the Documents folder of Attacker Machine-1 (File Name: Threatfeed.txt). You are a cybersecurity technician working for an ABC organization. Your organization has assigned you a task to analyze the data and submit a report on the threat landscape. Select the IP address linked with http://securityabc.s21sec.com.

- A. 5.9.200.150
- B. 5.9.110.120
- C. 5.9.200.200
- D. 5.9.188.148

Answer: D

NEW QUESTION # 30
Malachi, a security professional, implemented a firewall in his organization to trace incoming and outgoing traffic. He deployed a firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate.
Identify the firewall technology implemented by Malachi in the above scenario.

- A. Circuit-level gateways
- B. Next generation firewall (NGFW)
- C. Network address translation (NAT)
- D. Packet filtering

Answer: A

Explanation:
A circuit-level gateway is a type of firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate. It does not inspect the contents of each packet, but rather relies on the session information to filter traffic

NEW QUESTION # 31
.....