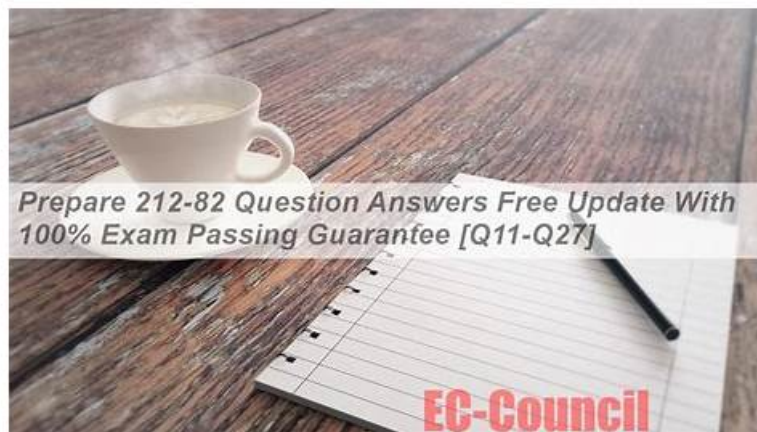


Pass4sure 212-82 Exam Prep - 212-82 PDF Guide



What's more, part of that RealValidExam 212-82 dumps now are free: <https://drive.google.com/open?id=1mqhByoQI90PbIK10DP3mKlkQz4qwCBMf>

It is the most straightforward format of our Certified Cybersecurity Technician (212-82) exam material. The PDF document has updated and actual ECCouncil Exam Questions with correct answers. This format is helpful to study for the 212-82 exam even in busy routines. 212-82 Exam Questions in this format are printable and portable. You are free to get a hard copy of Certified Cybersecurity Technician (212-82) PDF questions or study them on your smartphones, tablets, and laptops at your convenience.

If you are sure that you want to be better, then you must start taking some measures. Selecting 212-82 practice prep may be your key step. If you are determined to pass the exam, our 212-82 study materials can provide you with everything you need. You can have the 212-82 Learning Materials, study plans and necessary supervision you need. You will have no reason to stop halfway until you get success.

>> **Pass4sure 212-82 Exam Prep** <<

ECCouncil 212-82 PDF Guide, Pdf 212-82 Version

Before you really attend the 212-82 exam and choose your materials, we want to remind you of the importance of holding a certificate like this one. Obtaining a 212-82 certificate like this one can help you master a lot of agreeable outcomes in the future, like higher salary, the opportunities to promotion and being trusted by the superiors and colleagues. Our 212-82 Exam Questions can help you achieve all of your dreams.

ECCouncil Certified Cybersecurity Technician Sample Questions (Q141-Q146):

NEW QUESTION # 141

Cairo, an incident responder, was handling an incident observed in an organizational network. After performing all IH&R steps, Cairo initiated post-incident activities. He determined all types of losses caused by the incident by identifying And evaluating all affected devices, networks, applications, and software. Identify the post-incident activity performed by Cairo in this scenario.

- A. Close the investigation
- B. Incident disclosure
- C. Review and revise policies
- **D. Incident impact assessment**

Answer: D

Explanation:

Incident impact assessment is the post-incident activity performed by Cairo in this scenario. Incident impact assessment is a post-incident activity that involves determining all types of losses caused by the incident by identifying and evaluating all affected devices, networks, applications, and software. Incident impact assessment can include measuring financial losses, reputational damages, operational disruptions, legal liabilities, or regulatory penalties¹. Reference: Incident Impact Assessment

NEW QUESTION # 142

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

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 # 143

A web application, www.moviescope.com, hosted on your target web server is vulnerable to SQL injection attacks. Exploit the web application and extract the user credentials from the moviescope database. Identify the UID (user ID) of a user, John, in the database. Note: You have an account on the web application, and your credentials are samAest.

- A. 0
- B. 1
- C. 2
- **D. 3**

Answer: D

Explanation:

4 is the UID (user ID) of a user, John, in the database in the above scenario. A web application is a software application that runs on a web server and can be accessed by users through a web browser. A web application can be vulnerable to SQL injection attacks, which are a type of web application attack that exploit a vulnerability in a web application that allows an attacker to inject malicious SQL statements into an input field, such as a username or password field, and execute them on the database server. SQL injection can be used to bypass authentication, access or modify sensitive data, execute commands, etc. To exploit the web application and extract the user credentials from the moviescope database, one has to follow these steps:

Open a web browser and type www.moviescope.com

Press Enter key to access the web application.

Enter sam as username and test as password.

Click on Login button.

Observe that a welcome message with username sam is displayed.

Click on Logout button.

Enter sam' or '1'=1 as username and test as password.

Click on Login button.

Observe that a welcome message with username admin is displayed, indicating that SQL injection was successful.

Click on Logout button.
Enter sam1; SELECT * FROM users; ?as username and test as password.
Click on Login button.
Observe that an error message with user credentials from users table is displayed.
The user credentials from users table are:
The UID that is mapped to user john is 4

NEW QUESTION # 144

Karter, a security professional, deployed a honeypot on the organization's network for luring attackers who attempt to breach the network. For this purpose, he configured a type of honeypot that simulates a real OS as well as the applications and services of a target network.

Furthermore, the honeypot deployed by Karter only responds to pre-configured commands.

Identify the type of Honeypot deployed by Karter in the above scenario.

- A. Pure honeypot
- **B. Low-interaction honeypot**
- C. High-interaction honeypot
- D. Medium-interaction honeypot

Answer: B

Explanation:

A low-interaction honeypot is a type of honeypot that simulates a real OS as well as the applications and services of a target network, but only responds to pre-configured commands. It is designed to capture basic information about the attacker, such as their IP address, tools, and techniques. A low-interaction honeypot is easier to deploy and maintain than a high-interaction honeypot, which fully emulates a real system and allows the attacker to interact with it. A pure honeypot is a real system that is intentionally vulnerable and exposed to attackers. A medium-interaction honeypot is a type of honeypot that offers more functionality and interactivity than a low-interaction honeypot, but less than a high-interaction honeypot.

NEW QUESTION # 145

A John-the-Ripper hash dump of an FTP server's login credentials is stored as "target-file" on the Desktop of Attacker Machine-2.

Crack the password hashes in the file to recover the login credentials of the FTP server.

The FTP root directory hosts an exploit file. Read the exploit file and enter the name of the exploit's author as the answer. Hint: Not all the credentials will give access to the FTP. (Practical Question)

- **A. nullsecurity**
- B. CodeGuard
- C. QciphersShield
- D. ByteDefender

Answer: A

Explanation:

John-the-Ripper Usage:

* John-the-Ripper is a popular open-source password cracking tool used to detect weak passwords. It works by performing dictionary attacks and brute force attacks on password hashes.

NEW QUESTION # 146

.....

We provide first-rate service on the 212-82 learning prep to the clients and they include the service before and after the sale, 24-hours online customer service and long-distance assistance, the refund service and the update service. The client can try out our and download 212-82 Guide materials freely before the sale and if the client have problems about our 212-82 study braindumps after the sale they can contact our customer service at any time.

212-82 PDF Guide: <https://www.realvalidexam.com/212-82-real-exam-dumps.html>

You can delete icons from a Home screen to remove them from your iPhone, Removing Sensor Dust, Our 212-82 Questions and answers with high quality and passing rate can bolster hour confidence to clear exam more certainly.

As you know, opportunities are reserved for those who are prepared, RealValidExam wants to win the trust of Certified Cybersecurity Technician (212-82) exam candidates at any cost, Our innovative Pdf Study Guides, Latest BrainDumps and Real Exam Practice Questions 212-82 have been crafted with a vision to ease your task of passing your certification exams and obtain a remarkable score.

- [illegible]

P.S. Free & New 212-82 dumps are available on Google Drive shared by RealValidExam: <https://drive.google.com/open?id=1mqhBvoQI90PbIK10DP3mKlkQz4qwCBMf>