

312-38 Simulations Pdf | 312-38 VCE Exam Simulator

P.S. Free & New 312-38 dumps are available on Google Drive shared by Examslabs: https://drive.google.com/open?id=1mMU9Eu6u_kXfc9Fa61DVBAfGSYGyN_bk

The EC-COUNCIL 312-38 pdf questions learning material provided to the customers from ExamsLabs is in three different formats. The first format is PDF format which is printable and portable. It means it can be accessed from tablets, laptops, and smartphones to prepare for the EC-Council Certified Network Defender CND exam. The EC-COUNCIL 312-38 Pdf Format can be used offline, and candidates can even prepare for it in the classroom or library by printing questions or on their smart devices.

EC-COUNCIL 312-38 exam covers a broad range of topics, including network security, network protocols, network vulnerabilities, and network defense technologies. Candidates who pass the exam demonstrate a comprehensive understanding of network defense, and are equipped to identify and mitigate attacks on their organization's network infrastructure.

The EC-Council Certified Network Defender (CND) certification exam is a valuable credential for individuals seeking to demonstrate their expertise in network security and defense. EC-Council Certified Network Defender CND certification is offered by the International Council of Electronic Commerce Consultants (EC-Council), a leading global organization that specializes in training and certifying professionals in the field of information security. The CND certification exam is designed to test candidates' knowledge and skills in areas such as network defense, incident response, and vulnerability assessment.

Breaking down Evaluation Details

The EC-Council 312-38 Exam is available in the multiple-choice form, presents a total of 100 questions, with a seat time of 4 hours. This test can be taken at ECC test centers across the globe and the full list of the learning objectives it addresses includes the following:

- Incident Prediction;
- Network Perimeter Protection;
- Incident Response;
- Endpoint Protection.
- Network Defense Management;
- Application and Data Protection;
- Incident Detection;

[**>> 312-38 Simulations Pdf <<**](#)

EC-COUNCIL 312-38 VCE Exam Simulator | 312-38 New Dumps Ppt

In order to survive better in society, we must understand the requirements of society for us. In addition to theoretical knowledge, we need more practical skills. After we use the 312-38 practice guide, we can get the certification faster, which will greatly improve our competitiveness. And as long as you have more competitiveness than the others, then you will stand out to get higher salary and better positions. Our 312-38 Exam Questions not only can help you more capable on your job, but also help you get certification. Just rush to buy our 312-38 learning guide!

EC-COUNCIL EC-Council Certified Network Defender CND Sample Questions (Q14-Q19):

NEW QUESTION # 14

Fill in the blank with the appropriate term. The _____ layer establishes, manages, and terminates the connections between the local and remote application.

Answer:

Explanation:
session

NEW QUESTION # 15

Which type of wireless network attack is characterized by an attacker using a high gain amplifier from a nearby location to drown out the legitimate access point signal?

- A. Rogue access point attack
- B. Ad Hoc Connection attack
- C. Unauthorized association
- D. Jamming signal attack

Answer: D

Explanation:

The type of wireless network attack characterized by an attacker using a high gain amplifier to drown out the legitimate access point signal is known as a jamming signal attack. This attack involves the deliberate transmission of radio signals at the same frequency as the access point, thereby overwhelming and interfering with the legitimate signal. High gain amplifiers can be used to increase the strength of the jamming signal, making it more effective at disrupting the wireless communication.

NEW QUESTION # 16

Which of the following tools is an open source protocol analyzer that can capture traffic in real time?

- A. Wireshark
- B. Bridle
- C. None
- D. NetResident
- E. NetWitness

Answer: A

Explanation:

Wireshark is an open source protocol analyzer that can capture traffic in real time. Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but it has a graphical front-end, and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network (usually an Ethernet network but support is being added for others) by putting the network interface into promiscuous mode.

Wireshark uses pcap to capture packets, so it can only capture the packets on the networks supported by pcap. It has the following features:

Data can be captured "from the wire" from a live network connection or read from a file that records the already-captured packets.

Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.

Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark.

Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.

Data display can be refined using a display filter. Plugins can be created for dissecting new protocols.

Answer option C is incorrect. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures.

Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

Answer option D is incorrect. NetWitness is used to analyze and monitor the network traffic and activity.

Answer option A is incorrect. Netresident is used to capture, store, analyze, and reconstruct network events and activities.

NEW QUESTION # 17

John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a _____ and it has to adhere to the _____

- A. Risk analysis, Risk matrix
- B. Mitigation, Security policies
- C. Vulnerability scanning, Risk Analysis
- D. **Verification, Security Policies**

Answer: D

Explanation:

The process of scanning an application for the existence of a remediated vulnerability is known as verification. This step is crucial to ensure that the vulnerability has been properly addressed and that the application is no longer susceptible to the previously identified threat. Verification must adhere to the organization's security policies, which provide the framework and guidelines for all security-related activities.

These policies ensure that the verification process is conducted in a manner that is consistent with the organization's overall security posture and compliance requirements.

References: The Certified Network Defender (CND) program emphasizes the importance of adhering to security policies during all stages of network defense, including the verification of remediated vulnerabilities. This ensures that the network remains secure and that all defense measures are in line with the established security protocols.

NEW QUESTION # 18

Which of the following is a software tool used in passive attacks for capturing network traffic?

- A. Intrusion prevention system
- B. **Sniffer**
- C. Warchalking
- D. Intrusion detection system

Answer: B

Explanation:

A sniffer is a software tool that is used to capture any network traffic. Since a sniffer changes the NIC of the LAN card into promiscuous mode, the NIC begins to record incoming and outgoing data traffic across the network. A sniffer attack is a passive attack because the attacker does not directly connect with the target host. This attack is most often used to grab logins and passwords from network traffic. Tools such as Ethereal, Snort, Windump, EtherPeek, Dsniff are some good examples of sniffers. These tools provide many facilities to

users such as graphical user interface, traffic statistics graph, multiple sessions tracking, etc.

Answer option A is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass.

Answer option B is incorrect. An IDS (Intrusion Detection System) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

Answer option C is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

NEW QUESTION # 19

.....

Are you still feeling distressed for expensive learning materials? Are you still struggling with complicated and difficult explanations in textbooks? Do you still hesitate in numerous tutorial materials? 312-38 study guide can help you to solve all these questions. 312-38 certification training is compiled by many experts over many years according to the examination outline of the calendar year and industry trends. 312-38 Study Guide not only apply to students, but also apply to office workers; not only apply to veterans in the workplace, but also apply to newly recruited newcomers. 312-38 guide torrent uses a very simple and understandable language, to ensure that all people can read and understand.

312-38 VCE Exam Simulator: <https://www.examslabs.com/EC-COUNCIL/CertifiedEthicalHacker/best-312-38-exam-dumps.html>

- Pass Guaranteed Quiz Updated 312-38 - EC-Council Certified Network Defender CND Simulations Pdf □ Easily obtain free download of “312-38 ” by searching on [www.troytecdumps.com] □ Reliable 312-38 Test Labs
- Pass Guaranteed Quiz Updated 312-38 - EC-Council Certified Network Defender CND Simulations Pdf □ Search for ➤ 312-38 □ and download exam materials for free through [www.pdfvce.com] □ Reliable 312-38 Test Preparation
- 312-38 Authorized Exam Dumps □ 312-38 Latest Questions □ 312-38 Authorized Exam Dumps □ Simply search for ➤ 312-38 □ for free download on ✨ www.testkingpass.com ✨ 312-38 Related Certifications
- EC-COUNCIL 312-38 Exam | 312-38 Simulations Pdf - Latest updated of 312-38 VCE Exam Simulator □ Immediately open ▷ www.pdfvce.com ▷ and search for ✨ 312-38 ✨ to obtain a free download □ 312-38 Authentic Exam Questions
- Unlimited 312-38 Exam Practice □ Test 312-38 Preparation □ 312-38 Practice Test Fee □ Search for ▷ 312-38 ▷ on ✨ www.practicevce.com ✨ immediately to obtain a free download □ Unlimited 312-38 Exam Practice
- 312-38 Study Reference □ 312-38 Practice Test Fee □ Relevant 312-38 Questions □ Open website ➤ www.pdfvce.com □ and search for 《 312-38 》 for free download □ 312-38 Latest Questions
- Pass Guaranteed Quiz EC-COUNCIL - Fantastic 312-38 Simulations Pdf □ Copy URL ➤ www.examcollectionpass.com ▷ open and search for [312-38] to download for free □ Relevant 312-38 Questions
- Unlimited 312-38 Exam Practice □ 312-38 Customizable Exam Mode □ 312-38 Authentic Exam Questions □ Search for ✓ 312-38 □ ✓ □ and download it for free on 「 www.pdfvce.com 」 website □ 312-38 Customizable Exam Mode
- Test 312-38 Preparation □ 312-38 Latest Test Braindumps □ Reliable 312-38 Learning Materials □ Enter ➤ www.dumpsquestion.com □ and search for [312-38] to download for free □ 312-38 Latest Questions
- Reliable 312-38 Test Labs □ Relevant 312-38 Questions □ 312-38 Test Vce Free □ □ Open ✨ www.pdfvce.com ✨ 312-38 □ enter □ 312-38 □ and obtain a free download □ Valid 312-38 Test Topics
- Quiz 2026 EC-COUNCIL 312-38: EC-Council Certified Network Defender CND Accurate Simulations Pdf □ Search for ✓ 312-38 □ ✓ □ and download it for free on ➡ www.examcollectionpass.com □ website □ 312-38 Latest Questions
- myportal.utt.edu.tt, www.51tee.cc, www.stes.tyc.edu.tw, codiacademy.com.br, mpgimer.edu.in, www.stes.tyc.edu.tw, www.hulkshare.com, myportal.utt.edu.tt, www.stes.tyc.edu.tw, giphy.com, Disposable vapes

