312-38 Test Question & New 312-38 Test Tips

BONUS!!! Download part of FreeCram 312-38 dumps for free: https://drive.google.com/open?id=1RAis3RVFrNaDLYpPC7leisVFd0gmeXVu

Our 312-38 guide torrent can help you to solve all these questions to pass the 312-38 exam. Our 312-38 study materials are simplified and compiled by many experts over many years according to the examination outline of the calendar year and industry trends. So our 312-38 learning materials are easy to be understood and grasped. There are also many people in life who want to change their industry. They often take the professional qualification exam as a stepping stone to enter an industry. If you are one of these people, our 312-38 Exam Engine will be your best choice.

Understanding functional and technical aspects of Certified Network Defender Business Principles and Practices

The following will be discussed in **ECCOUNCIL EC 312-38 Exam Dumps**:

- Discuss log monitoring and analysis on Firewall
- Understand incident response concept
- Discuss log monitoring and analysis on Routers
- Learn to leverage/consume threat intelligence for proactive defense
- Understand the attack surface analysis
- Understand the role of cyber threat intelligence in network defense
- Learn to conduct attack simulation
- Understand wireless network authentication methods
- Learn vulnerability assessment and scanning
- Understand and visualize your attack surface
- Discuss Security in Google Cloud Platform (GCP)
- Understand logging concepts
- Learn to reduce the attack surface
- Discuss security in Microsoft Azure Cloud
- Discuss log monitoring and analysis on Windows systems
- Introduction to Business Continuity (BC) and Disaster Recovery (DR)
- Learn to manage risk though risk management program
- Understand different types of threat Intelligence
- Discuss log monitoring and analysis on Mac
- Understand wireless network fundamentals
- Setting up the environment for network monitoring
- Describe incident handling and response process
- Discuss BC/DR Activities
- Learn to identify Indicators of Exposures (IoE)
- Perform network monitoring and analysis for suspicious traffic using Wireshark
- Discuss centralized log monitoring and analysis
- Learn to manage vulnerabilities through vulnerability management program
- Describe forensics investigation process
- Evaluate CSP for Security before Consuming Cloud Service
- Explain Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
- Understand the need and advantages of network traffic monitoring

>> 312-38 Test Question <<

New 312-38 Test Tips, Related 312-38 Exams

Everyone has their roles in society, and they are busy with their jobs and family. So the time and energy are very precious for the preparation of 312-38 actual test. While, now you are lucky. 312-38 cert guide will give you some instructions and help you do study plan for your coming test. If you are a fresh men in this industry, do not worry, EC-COUNCIL 312-38 PDF training will help you. The questions and knowledge points are very simple and easy to get. You can download the 312-38 test engine and install it on your phone. When you take the subway, you can open it and do test practice. To take full use of the spare time by 312-38 test engine, you will enjoy a high efficiency study experience.

EC-COUNCIL EC-Council Certified Network Defender CND Sample Questions (Q391-Q396):

NEW QUESTION # 391
Which of the following OSI layers establishes, manages, and terminates the connections between the local and remote applications?

- A. Application layer
- B. Data Link layer
- C. Network layer
- D. Session layer

Answer: D

Explanation:
The session layer of the OSI/RM controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls. Answer option C is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer. Answer option A is incorrect. The Data Link Layer is Layer 2 of the seven-layer OSI model of computer networking. It corresponds to or is part of the link layer of the TCP/IP reference model. The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The Data Link Layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC, and ADCCP for point-to-point (dual-node) connections. Answer option B is incorrect. The network layer controls the operation of subnet, deciding which physical path the data should take, based on network conditions, priority of service, and other factors. Routers work on the Network layer of the OSI stack.

NEW QUESTION # 392
Which of the following is a software tool used in passive attacks for capturing network traffic?

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

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 C 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 D 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 # 393
Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network vulnerability assessment plan?

- A. Their first step is the acquisition of required documents, reviewing of security policies and compliance.
- B. Their first step is to create an initial Executive report to show the management team.
- C. Their first step is to make a hypothesis of what their final findings will be.
- D. Their first step is to analyze the data they have currently gathered from the company or interviews.

Answer: A

Explanation:
The first step in creating a network vulnerability assessment plan is to acquire the necessary documents and review the organization's security policies and compliance requirements. This involves gathering all relevant information that will inform the scope and focus of the vulnerability assessment. It includes understanding the security policies in place, the regulatory compliance obligations the company must adhere to, and any existing security measures and controls. This foundational step ensures that the vulnerability assessment is aligned with the company's security posture and compliance mandates, providing a clear direction for the subsequent stages of the assessment process.

NEW QUESTION # 394
Which of the following attacks is a class of brute force attacks that depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations?

- A. Phishing attack
- B. Dictionary attack
- C. Replay attack
- D. Birthday attack

Answer: D

Explanation:
A birthday attack is a class of brute force attacks that exploits the mathematics behind the birthday problem in probability theory. It is a type of cryptography attack. The birthday attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations.
Answer option D is incorrect. A dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by searching likely possibilities. A dictionary attack uses a brute-force technique of successively trying all the words in an exhaustive list (from a pre- arranged list of values). In contrast with a normal brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words in a dictionary. Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), single words found in dictionaries, or simple, easily-predicted variations on words, such as appending a digit.
Answer option A is incorrect. Phishing is a type of internet fraud attempted by hackers. Hackers try to log into system by masquerading as a trustworthy entity and acquire sensitive information, such as, username, password, bank account details, credit

card details, etc. After collecting this information, hackers try to use this information for their gain.
Answer option B is incorrect. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution.

NEW QUESTION # 395
Fargo, head of network defense at Globadyne Tech, has discovered an undesirable process in several Linux systems, which causes machines to hang every 1 hour. Fargo would like to eliminate it; what command should he execute?

- A. # kill -9 [PID]
- B. # ps ax | grep [Target Process]
- C. # update-rc.d -f [service name] remove
- D. # service [service name] stop

Answer: A

Explanation:
To eliminate an undesirable process that is causing Linux systems to hang, Fargo should use the command # kill -9 [PID]. This command sends the SIGKILL signal to the process with the specified PID (Process ID), which forcefully stops the process immediately. The kill -9 command is used when a process cannot be terminated using normal shutdown commands. It is important to note that this command should be used with caution, as it does not allow the process to perform any cleanup operations before shutting down.
References:
* The use of the kill command is a common practice in Linux system administration for terminating unresponsive processes.
* The Certified Network Defender (CND) training includes understanding and managing Linux processes as part of network defense strategies.

NEW QUESTION # 396
.....

It is known to us that having a good job has been increasingly important for everyone in the rapidly developing world; it is known to us that getting a 312-38 certification is becoming more and more difficult for us. If you are tired of finding a high quality study material, we suggest that you should try our 312-38 Exam Prep. Because our materials not only has better quality than any other same learn products, but also can guarantee that you can pass the 312-38 exam with ease.

- myportal.utt.edu.tt, korodhsoaqoon.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.zazzle.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes

P.S. Free 2026 EC-COUNCIL 312-38 dumps are available on Google Drive shared by FreeCram: https://drive.google.com/open?id=1RAis3RVFrNaDLYpPC7leisVFd0gmeXVu