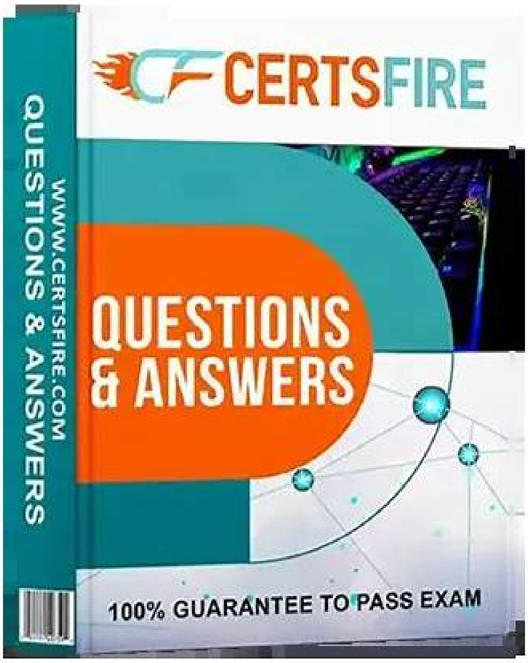
Updated CNSP CBT, Questions CNSP Exam



P.S. Free 2025 The SecOps Group CNSP dumps are available on Google Drive shared by Prep4sureExam: https://drive.google.com/open?id=12rFH7nCqPuuow7NdDkOPuk7rwudEpshr

If you are wandering for CNSP study material and the reliable platform that will lead you to success in exam, then stop considering this issue. Prep4sureExam is the solution to your problem. They offer you reliable and updated CNSP exam questions. The exam questions are duly designed by the team of subject matter experts; they are highly experienced and trained in developing exam material. Prep4sureExam offers a 100% money back guarantee, in case you fail in your CNSP. You claim revert, by showing your transcript and undergoing through the clearance process. Also, we provide 24/7 customer service to all our valued customers. Our dedicated team will answer all your all queries related to CNSP.

The SecOps Group CNSP Exam Syllabus Topics:

Topic	Details
Topic 1	• Common vulnerabilities affecting Windows Services: This section of the exam measures the skills of Network Engineers and focuses on frequently encountered weaknesses in core Windows components. It underscores the need to patch, configure, and monitor services to prevent privilege escalation and unauthorized use.
Topic 2	• Active Directory Security Basics: This section of the exam measures the skills of Network Engineers and introduces the fundamental concepts of directory services, highlighting potential security risks and the measures needed to protect identity and access management systems in a Windows environment.

Topic 3	- Cryptography: This section of the exam measures the skills of Security Analysts and focuses on basic encryption and decryption methods used to protect data in transit and at rest. It includes an overview of algorithms, key management, and the role of cryptography in maintaining data confidentiality.
Topic 4	- Linux and Windows Security Basics: This section of the exam measures skills of Security Analysts and compares foundational security practices across these two operating systems. It addresses file permissions, user account controls, and basic hardening techniques to reduce the attack surface.
Topic 5	- Database Security Basics: This section of the exam measures the skills of Network Engineers and covers how databases can be targeted for unauthorized access. It explains the importance of strong authentication, encryption, and regular auditing to ensure that sensitive data remains protected.
Topic 6	- Password Storage: This section of the exam measures the skills of Network Engineers and addresses safe handling of user credentials. It explains how hashing, salting, and secure storage methods can mitigate risks associated with password disclosure or theft.
Topic 7	- Network Architectures, Mapping, and Target Identification: This section of the exam measures the skills of Network Engineers and reviews different network designs, illustrating how to diagram and identify potential targets in a security context. It stresses the importance of accurate network mapping for efficient troubleshooting and defense.
Topic 8	- Testing Network Services
Topic 9	- Open-Source Intelligence Gathering (OSINT): This section of the exam measures the skills of Security Analysts and discusses methods for collecting publicly available information on targets. It stresses the legal and ethical aspects of OSINT and its role in developing a thorough understanding of potential threats.
Topic 10	- Network Security Tools and Frameworks (such as Nmap, Wireshark, etc)
Topic 11	- Network Discovery Protocols: This section of the exam measures the skills of Security Analysts and examines how protocols like ARP, ICMP, and SNMP enable the detection and mapping of network devices. It underlines their importance in security assessments and network monitoring.
Topic 12	- Testing Web Servers and Frameworks: This section of the exam measures skills of Security Analysts and examines how to assess the security of web technologies. It looks at configuration issues, known vulnerabilities, and the impact of unpatched frameworks on the overall security posture.

>> Updated CNSP CBT <<

Pass Guaranteed CNSP - The Best Updated Certified Network Security Practitioner CBT

Will you feel nervous when you are in the exam, and if you do, you can try our exam dumps.CNSP Soft test engine can stimulate the real environment, through this , you can know the procedure of the real exam, so that you can release your nervous . And you can build up your confidence when you face the real exam. Besides, CNSP Exam Dumps of us offer you free update for one year after purchasing, and our system will send the latest version to you automatically. We have online and offline chat service stuff, and if you have any questions, just have chat with them.

The SecOps Group Certified Network Security Practitioner Sample Questions (Q58-Q63):

NEW QUESTION # 58
Which one of the following is not an online attack?

- A. Password spraying attack
- B. Brute force attack

- C. Rainbow table attack
- D. Phishing attack

Answer: C

Explanation:
Online attacks require real-time interaction with a target system (e.g., a login interface), whereas offline attacks occur without direct system interaction, typically after obtaining data like password hashes. A rainbow table attack is an offline method that uses precomputed tables of hash values to reverse-engineer passwords from stolen hash databases, distinguishing it from the other options, which are online.
Why B is correct: Rainbow table attacks are performed offline after an attacker has already acquired a hash (e.g., from a compromised database). The attacker matches the hash against precomputed tables to find the plaintext password, requiring no interaction with the target system during the attack. CNSP classifies this as an offline password recovery technique.
Why other options are incorrect:
A: Brute force attacks involve repeatedly submitting password guesses to a live system (e.g., via SSH or a web login), making it an online attack.
C: Password spraying attacks test a few common passwords across many accounts on a live system, also an online attack aimed at avoiding lockouts.
D: Phishing attacks trick users into submitting credentials through fake interfaces (e.g., emails or websites), requiring real-time interaction and thus classified as online.

NEW QUESTION # 59
If a hash begins with $2a$, what hashing algorithm has been used?

- A. MD5
- B. SHA512
- C. Blowfish
- D. SHA256

Answer: C

Explanation:
The prefix $2a$ identifies the bcrypt hashing algorithm, which is based on the Blowfish symmetric encryption cipher (developed by Bruce Schneier). Bcrypt is purpose-built for password hashing, incorporating:
Salt: A random string (e.g., 22 Base64 characters) to thwart rainbow table attacks.
Work Factor: A cost parameter (e.g., $2a$10$ means 2