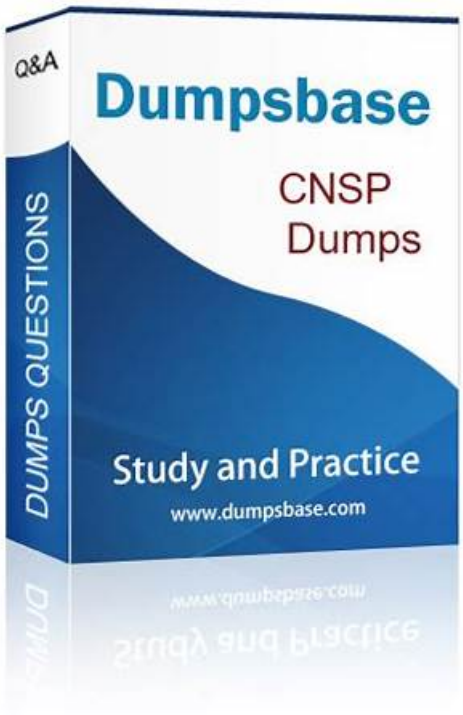
CNSP test questions, CNSP dumps torrent, CNSP pdf



P.S. Free 2025 The SecOps Group CNSP dumps are available on Google Drive shared by GetValidTest: https://drive.google.com/open?id=1p-KHjBDrfXSD7Yi1q8D_sOvKNwyRZoHX

The CNSP training pdf provided by GetValidTest is really the best reference material you can get from anywhere. The experts of GetValidTest are trying their best to develop and research the high quality and CNSP exam preparation material to help you strengthen technical job skills. When you complete your payment, you will receive an email attached with CNSP practice pdf, then you can instantly download it and install on your phone or computer for study. The high efficiency preparation by CNSP exam dumps can ensure you 100% pass with ease.

The SecOps Group CNSP Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• Social Engineering attacks: This section of the exam measures the skills of Security Analysts and addresses the human element of security breaches. It describes common tactics used to manipulate users, emphasizes awareness training, and highlights how social engineering can bypass technical safeguards.
Topic 3	• 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 4	• Testing Network Services

Topic 5	• This section of the exam measures the skills of Network Engineers and explains how to verify the security and performance of various services running on a network. It focuses on identifying weaknesses in configurations and protocols that could lead to unauthorized access or data leaks.
Topic 6	• Network Scanning & Fingerprinting: This section of the exam measures the skills of Security Analysts and covers techniques for probing and analyzing network hosts to gather details about open ports, operating systems, and potential vulnerabilities. It emphasizes ethical and legal considerations when performing scans.
Topic 7	• 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 8	• 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 9	• 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 10	• Basic Malware Analysis: This section of the exam measures the skills of Network Engineers and offers an introduction to identifying malicious software. It covers simple analysis methods for recognizing malware behavior and the importance of containment strategies in preventing widespread infection.
Topic 11	• Network Security Tools and Frameworks (such as Nmap, Wireshark, etc)
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.
Topic 13	• TCP • IP (Protocols and Networking Basics): This section of the exam measures the skills of Security Analysts and covers the fundamental principles of TCP • IP, explaining how data moves through different layers of the network. It emphasizes the roles of protocols in enabling communication between devices and sets the foundation for understanding more advanced topics.

2025 Professional The SecOps Group Reliable CNSP Test Testking

As long as you study with our CNSP training braindumps, you will find that our CNSP learning quiz is not famous for nothing but for its unique advantages. The CNSP exam questions and answers are rich with information and are easy to remember due to their simple English and real exam simulations and graphs. So many customers praised that our CNSP praparation guide is well-written. With our CNSP learning engine, you are success guaranteed!

The SecOps Group Certified Network Security Practitioner Sample Questions (Q40-Q45):

NEW QUESTION # 40
An 'EICAR' file can be used to?

- A. Test the response of an antivirus program
- B. Test the encryption algorithms

Answer: A

Explanation:
The EICAR test file is a standardized tool in security testing, designed for a specific purpose.
Why A is correct: The EICAR file (a 68-byte string) triggers antivirus detection without harm, testing response capabilities. CNSP recommends it for AV validation.
Why B is incorrect: It has no role in testing encryption; it's solely for AV functionality.

NEW QUESTION # 41
What types of attacks are phishing, spear phishing, vishing, scareware, and watering hole?

- A. Probes
- B. Social engineering
- C. Ransomware
- D. Insider threats

Answer: B

Explanation:
Social engineering exploits human psychology to manipulate individuals into divulging sensitive information, granting access, or performing actions that compromise security. Unlike technical exploits, it targets the "human factor," often bypassing technical defenses. The listed attacks fit this category:
Phishing: Mass, untargeted emails (e.g., fake bank alerts) trick users into entering credentials on spoofed sites. Uses tactics like urgency or trust (e.g., typosquatting domains).
Spear Phishing: Targeted phishing against specific individuals/organizations (e.g., CEO fraud), leveraging reconnaissance (e.g., LinkedIn data) for credibility.
Vishing (Voice Phishing): Phone-based attacks (e.g., fake tech support calls) extract info via verbal manipulation. Often spoofs caller ID.
Scareware: Fake alerts (e.g., "Your PC is infected!" pop-ups) scare users into installing malware or paying for bogus fixes. Exploits fear and urgency.
Watering Hole: Compromises trusted websites frequented by a target group (e.g., industry forums), infecting visitors via drive-by downloads. Relies on habitual trust.
Technical Details:
Delivery: Email (phishing), VoIP (vishing), web (watering hole/scareware).
Payloads: Credential theft, malware (e.g., trojans), or financial fraud.
Mitigation: User training, email filters (e.g., DMARC), endpoint protection.
Security Implications: Social engineering accounts for ~90% of breaches (e.g., Verizon DBIR 2023), as it exploits unpatchable human error. CNSP likely emphasizes awareness (e.g., phishing simulations) and layered defenses (e.g., MFA).
Why other options are incorrect:
A . Probes: Reconnaissance techniques (e.g., port scanning) to identify vulnerabilities, not manipulation-based like these attacks.
B . Insider threats: Malicious actions by authorized users (e.g., data theft by employees), not external human-targeting tactics.
D . Ransomware: A malware type (e.g., WannaCry) that encrypts data for ransom, not a manipulation method-though phishing often delivers it.
Real-World Context: The 2016 DNC hack used spear phishing to steal credentials, showing social engineering's potency.

NEW QUESTION # 42
A system encrypts data prior to transmitting it over a network, and the system on the other end of the transmission media decrypts it. If the systems are using a symmetric encryption algorithm for encryption and decryption, which of the following statements is true?

- A. A symmetric encryption algorithm does not use keys to encrypt and decrypt data at both ends of the transmission media.
- B. A symmetric encryption algorithm uses the same key to encrypt and decrypt data at both ends of the transmission media.
- C. A symmetric encryption algorithm is an insecure method used to encrypt data transmitted over transmission media.
- D. A symmetric encryption algorithm uses different keys to encrypt and decrypt data at both ends of the transmission media.

Answer: B

Explanation:
Symmetric encryption is a cryptographic technique where the same key is used for both encryption and decryption processes. In the context of network security, when data is encrypted prior to transmission and decrypted at the receiving end using a symmetric encryption algorithm (e.g., AES or Triple-DES), both the sender and receiver must share and utilize an identical secret key. This key is applied by the sender to transform plaintext into ciphertext and by the receiver to reverse the process, recovering the original

plaintext. The efficiency of symmetric encryption makes it ideal for securing large volumes of data transmitted over networks, provided the key is securely distributed and managed.
Why A is correct: Option A accurately describes the fundamental property of symmetric encryption-using a single shared key for both encryption and decryption. This aligns with CNSP documentation, which emphasizes symmetric encryption's role in securing data in transit (e.g., via VPNs or secure file transfers).
Why other options are incorrect:
B: This describes asymmetric encryption (e.g., RSA), where different keys (public and private) are used for encryption and decryption, not symmetric encryption.
C: Symmetric encryption inherently relies on keys; the absence of keys contradicts its definition and operational mechanism.
D: Symmetric encryption is not inherently insecure; its security depends on key strength and management practices, not the algorithm itself. CNSP highlights that algorithms like AES are widely regarded as secure when implemented correctly.

NEW QUESTION # 43
What ports can be queried to perform a DNS zone transfer?

- A. None of the above
- B. 53/UDP
- C. Both 1 and 2
- D. 53/TCP

Answer: D

Explanation:
A DNS zone transfer involves replicating the DNS zone data (e.g., all records for a domain) from a primary to a secondary DNS server, requiring a reliable transport mechanism.
Why A is correct: DNS zone transfers use TCP port 53 because TCP ensures reliable, ordered delivery of data, which is critical for transferring large zone files. CNSP notes that TCP is the standard protocol for zone transfers (e.g., AXFR requests), as specified in RFC 5936.
Why other options are incorrect:
B . 53/UDP: UDP port 53 is used for standard DNS queries and responses due to its speed and lower overhead, but it is not suitable for zone transfers, which require reliability over speed.
C . Both 1 and 2: This is incorrect because zone transfers are exclusively TCP-based, not UDP-based.
D . None of the above: Incorrect, as 53/TCP is the correct port for DNS zone transfers.

NEW QUESTION # 44
Which of the following attacks are associated with an ICMP protocol?

- A. Ping of death
- B. ICMP flooding
- C. Smurf attack
- D. All of the following

Answer: D

Explanation:
ICMP (Internet Control Message Protocol), per RFC 792, handles diagnostics (e.g., ping) and errors in IP networks. It's exploitable in:
A . Ping of Death:
Method: Sends oversized ICMP Echo Request packets (>65,535 bytes) via fragmentation. Reassembly overflows buffers, crashing older systems (e.g., Windows 95).
Fix: Modern OSes cap packet size (e.g., ping -s 65500).
B . Smurf Attack:
Method: Spoofs ICMP Echo Requests to a network's broadcast address (e.g., 192.168.255.255). All hosts reply, flooding the victim.
Amplification: 100 hosts = 100x traffic.
C . ICMP Flooding:
Method: Overwhelms a target with ICMP Echo Requests (e.g., ping -f), consuming bandwidth/CPU.
Variant: BlackNurse attack targets firewalls.
Technical Details:

ICMP Type 8 (Echo Request), Type 0 (Echo Reply) are key.
Mitigation: Rate-limit ICMP, disable broadcasts (e.g., no ip directed-broadcast).
Security Implications: ICMP attacks are DoS vectors. CNSP likely teaches filtering (e.g., iptables -p icmp -j DROP) balanced with diagnostics need.
Why other options are incorrect:
A, B, C individually: All are ICMP-based; D is comprehensive.
Real-World Context: Smurf attacks peaked in the 1990s; modern routers block them by default.

NEW QUESTION # 45
.....

CNSP exam questions are being offered in three easy-to-use and compatible formats. The The SecOps Group CNSP PDF dumps file, desktop practice test software, and web-based practice test software. All three CNSP Exam Questions format contain the The SecOps Group CNSP actual questions and help you in CNSP exam preparation entirely.