Free PDF Quiz 2026 The SecOps Group CNSP: High-quality Certified Network Security Practitioner Free Exam

BONUS!!! Download part of Pass4sures CNSP dumps for free: https://drive.google.com/open?id=1v_oBgkQ6klQV57jwAkZsiWvGD1aUBpG8

The latest CNSP exam torrent covers all the qualification exam simulation questions in recent years, including the corresponding matching materials at the same time. Do not have enough valid CNSP practice materials, can bring inconvenience to the user, such as the delay progress, learning efficiency and to reduce the learning outcome was not significant, these are not conducive to the user persistent finish learning goals. Therefore, to solve these problems, the CNSP test material is all kinds of qualification examination, the content of the difficult point analysis, let users in the vast amounts of find the information you need in the study materials, the CNSP practice materials improve the user experience, to lay the foundation for good grades through qualification exam.

Begin Your Preparation with The SecOps Group CNSP Real Questions. The Pass4sures is a reliable platform that is committed to making your preparation for the The SecOps Group CNSP examination easier and more effective. To meet this objective, the Pass4sures is offering updated and real Understanding Certified Network Security Practitioner exam dumps. These The SecOps Group CNSP Exam Questions are approved by experts.

>> CNSP Free Exam <<

Study Materials CNSP Review - CNSP Reliable Test Syllabus

If you are not certain whether the CNSP prep guide from our company is suitable for you or not, so you are hesitate to buy and use our study materials. Do not worry, in order to help you solve your problem and let you have a good understanding of our CNSP study practice dump, the experts and professors from our company have designed the trial version for all people. You can have a try of using the CNSP Prep Guide from our company before you purchase it. We believe that the trial version provided by our company will help you know about our study materials well and make the good choice for yourself. More importantly, the trial version of the CNSP exam questions from our company is free for all people. We believe that the trial version will help you a lot.

The SecOps Group CNSP Exam Syllabus Topics:

Topic	Details
Topic 1	- 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.
Topic 2	- 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 3	- 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 4	- 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 5	- 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 6	- 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 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	- 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 9	- Testing Network Services
Topic 10	- 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 11	- This section of the exam measures skills of Network Engineers and explores the utility of widely used software for scanning, monitoring, and troubleshooting networks. It clarifies how these tools help in detecting intrusions and verifying security configurations.
Topic 12	- Network Security Tools and Frameworks (such as Nmap, Wireshark, etc)
Topic 13	- 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 14	- 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 15	• 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 16	• 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 17	• TLS Security Basics: This section of the exam measures the skills of Security Analysts and outlines the process of securing network communication through encryption. It highlights how TLS ensures data integrity and confidentiality, emphasizing certificate management and secure configurations.

The SecOps Group Certified Network Security Practitioner Sample Questions (Q18-Q23):

NEW QUESTION # 18
Which is the correct command to change the MAC address for an Ethernet adapter in a Unix-based system?

- A. ifconfig eth0 hdw ether AA:BB:CC:DD:EE:FF
- B. ifconfig eth0 hdwr ether AA:BB:CC:DD:EE:FF
- C. ifconfig eth0 hw ether AA:BB:CC:DD:EE:FF
- D. ifconfig eth0 hwr ether AA:BB:CC:DD:EE:FF

Answer: C

Explanation:
In Unix-based systems (e.g., Linux), the ifconfig command is historically used to configure network interfaces, including changing the Media Access Control (MAC) address of an Ethernet adapter. The correct syntax to set a new MAC address for an interface like eth0 is ifconfig eth0 hw ether AA:BB:CC:DD:EE:FF, where hw specifies the hardware address type (ether for Ethernet), followed by the new MAC address in colon-separated hexadecimal format.
Why A is correct: The hw ether argument is the standard and correct syntax recognized by ifconfig to modify the MAC address. This command temporarily changes the MAC address until the system reboots or the interface is reset, assuming the user has sufficient privileges (e.g., root). CNSP documentation on network configuration and spoofing techniques validates this syntax for testing network security controls.
Why other options are incorrect:
B: hdw is not a valid argument; it's a typographical error and unrecognized by ifconfig.
C: hdwr is similarly invalid; no such shorthand exists in the command structure.
D: hwr is incorrect; the full keyword hw followed by ether is required for proper parsing.

NEW QUESTION # 19
Which of the following is not a DDoS attack?

- A. NTP Amplification
- B. UDP Flood
- C. SYN Flood
- D. Brute Force

Answer: D

Explanation:
DDoS (Distributed Denial of Service) attacks aim to overwhelm a target's resources with excessive traffic, disrupting availability, whereas other attack types target different goals.
Why D is correct: Brute force attacks focus on guessing credentials (e.g., passwords) to gain unauthorized access, not on denying service. CNSP classifies it as an authentication attack, not a DDoS method.
Why other options are incorrect:
A: SYN Flood exhausts TCP connection resources, a classic DDoS attack.
B: NTP Amplification leverages amplified responses to flood targets, a DDoS technique.
C: UDP Flood overwhelms a system with UDP packets, another DDoS method.

NEW QUESTION # 20
What types of attacks are phishing, spear phishing, vishing, scareware, and watering hole?

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

Answer: D

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 # 21
If a hash begins with $2a$, what hashing algorithm has been used?

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

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