Hottest The SecOps Group CNSP Certification & CNSP Labs

BTW, DOWNLOAD part of GuideTorrent CNSP dumps from Cloud Storage: https://drive.google.com/open?id=1YkTzUeGQ2_m1yrmz8HDSsJ358D4hpDyp

The CNSP examination time is approaching. Faced with a lot of learning content, you may be confused and do not know where to start. CNSP study materials simplify the complex concepts and add examples, simulations, and diagrams to explain anything that may be difficult to understand. You can more easily master and simplify important test sites with CNSP study materials. In addition, are you still feeling uncomfortable about giving up a lot of time to entertain, work or accompany your family and friends in preparation for the exam? Using CNSP Learning Materials, you can spend less time and effort reviewing and preparing, which will help you save a lot of time and energy. Then you can do whatever you want. Actually, if you can guarantee that your effective learning time with CNSP study materials is up to 20-30 hours, you can pass the exam.

Our CNSP test guide is suitable for you whichever level you are in right now. Whether you are in entry-level position or experienced exam candidates who have tried the exam before, this is the perfect chance to give a shot. A growing number of exam candidates are choosing our CNSP Exam Questions, why are you still hesitating? As long as you have make up your mind, our Certified Network Security Practitioner study question is available in five minutes, so just begin your review now! This could be a pinnacle in your life.

>> Hottest The SecOps Group CNSP Certification <<

Customizable Practice Test for Improved Success in The SecOps Group CNSP Certification Exam

To cope with the fast growing market, we will always keep advancing and offer our clients the most refined technical expertise and excellent services about our CNSP exam questions. In the meantime, all your legal rights will be guaranteed after buying our CNSP Study Materials. For many years, we have always put our customers in top priority. Not only we offer the best CNSP training prep, but also our sincere and considerate attitude is praised by numerous of our customers.

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	• Network Security Tools and Frameworks (such as Nmap, Wireshark, etc)
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	• 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 5	• 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 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	• 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 8	• Testing Network Services
Topic 9	• 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 10	• 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 11	• 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 12	• 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 13	• 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 14	• 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 15	• 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 16	• 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 17	• 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.

The SecOps Group Certified Network Security Practitioner Sample Questions (Q42-Q47):

NEW QUESTION # 42
Which one of the following is not an online attack?

- A. Phishing attack
- B. Password spraying attack
- C. Brute force attack
- D. Rainbow table attack

Answer: D

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 # 43
Where are the password hashes stored in a Microsoft Windows 64-bit system?

- A. C:\Windows\System64\config\SAM
- B. C:\System64\config\SAM
- C. C:\Windows\config\System32\SAM
- D. C:\Windows\System32\config\SAM

Answer: D

Explanation:
Windows stores password hashes in the SAM (Security Account Manager) file, with a consistent location across 32-bit and 64-bit systems.
Why B is correct: The SAM file resides at C:\Windows\System32\config\SAM, locked during system operation for security. CNSP notes this for credential extraction risks.
Why other options are incorrect:
A: System64 does not exist; System32 is used even on 64-bit systems.
C: C:\System64 is invalid; the path starts with Windows.

D: config\System32 reverses the correct directory structure.

NEW QUESTION # 44
In the context of a Unix-based system, where does a daemon process execute in the memory?

- A. Kernel space
- B. User space

Answer: B

Explanation:
In Unix-based systems, memory is divided into two primary regions: kernel space and user space, each serving distinct purposes for process execution and system stability.
Why B is correct: Daemon processes are background services (e.g., sshd, cron) that run with elevated privileges but operate in user space. User space is the memory area allocated for user applications and processes, isolated from kernel space to prevent direct hardware access or system crashes. CNSP highlights that daemons run in user space to maintain system integrity, interacting with the kernel via system calls.
Why other option is incorrect:
A . Kernel space: Kernel space is reserved for the operating system kernel and device drivers, which have unrestricted access to hardware. Running daemons in kernel space would pose significant security and stability risks, and it is not the standard practice in Unix systems.

NEW QUESTION # 45
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 is an insecure method used to encrypt data transmitted over transmission media.
- B. A symmetric encryption algorithm uses different keys to encrypt and decrypt data at both ends of the transmission media.
- C. A symmetric encryption algorithm uses the same key to encrypt and decrypt data at both ends of the transmission media.
- D. A symmetric encryption algorithm does not use keys to encrypt and decrypt data at both ends of the transmission media.

Answer: C

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 # 46
You are performing a security audit on a company's infrastructure and have discovered that the domain name system (DNS) server is vulnerable to a DNS cache poisoning attack. What is the primary security risk?

- A. The primary risk is that an attacker could redirect traffic to a malicious website and steal sensitive information.
- B. The primary risk is that an attacker could manipulate the cache of the web server or proxy server to return incorrect content for a specific URL or web page.

Answer: A

Explanation:
DNS cache poisoning, also known as DNS spoofing, involves an attacker injecting false DNS records into a resolver's cache, altering how domain names resolve.
Why A is correct: The primary risk is that an attacker can redirect users to malicious websites (e.g., phishing or malware sites) by poisoning the DNS cache with fake IP addresses. This can lead to credential theft, data exfiltration, or malware distribution. CNSP identifies this as the core threat of DNS cache poisoning, aligning with real-world attack vectors.
Why other option is incorrect:
B . Manipulate the cache of the web server or proxy server: This describes web cache poisoning, a different attack targeting HTTP caches, not DNS servers. DNS cache poisoning affects DNS resolution, not web or proxy server caches directly.

NEW QUESTION # 47
.....

Once you enter into our interface, nothing will disturb your learning the CNSP training engine except the questions and answers. So all you attention will be concentrated on study. At the same time, each process is easy for you to understand. There will have small buttons on the CNSP Exam simulation to help you switch between the different pages. It does not matter whether you can operate the computers well. Our CNSP training engine will never make you confused.

What's more, part of that GuideTorrent CNSP dumps now are free: https://drive.google.com/open?id=1YkTzUeGQ2_ml yrmz8HDSsJ358D4hpDyp