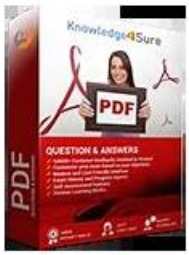
CNSP Relevant Questions, New CNSP Test Pdf



DOWNLOAD the newest Actual4test CNSP PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1Q840bqCSVpYdlZQu1AC7e5JUzUelj7hb

CNSP study engine is very attentive to provide a demo for all customers who concerned about our products, whose purpose is to allow customers to understand our product content before purchase. Many students suspect that if CNSP learning material is really so magical? Does it really take only 20-30 hours to pass such a difficult certification exam successfully? It is no exaggeration to say that you will be able to successfully pass the exam with our CNSP Exam Questions.

The SecOps Group CNSP Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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 5	• 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 6	• 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 7	• Testing Network Services
Topic 8	• 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 9	• 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 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	• 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	• 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 13	• 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 14	• Network Security Tools and Frameworks (such as Nmap, Wireshark, etc)
Topic 15	• 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 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	• 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.

>> CNSP Relevant Questions <<

New CNSP Test Pdf, CNSP PDF Question

All knowledge contained in our CNSP Practice Engine is correct. Our workers have checked for many times. Also, we will accept annual inspection of our CNSP exam simulation from authority. The results show that our CNSP study materials completely have no problem. Our company is rated as outstanding enterprise. And at the same time, our website have became a famous brand in the market. We also find that a lot of the fake websites are imitating our website, so you have to be careful.

The SecOps Group Certified Network Security Practitioner Sample Questions (Q24-Q29):

NEW QUESTION # 24
Which of the following commands will work on a Microsoft operating system to add a new domain admin user?

- A. net group "Administrator" John /add
- B. net user John /add /domain /admin
- C. net user John "Domain Admins" /add /domain
- D. net group "Domain Admins" John /add /domain

Answer: D

Explanation:
Adding a user to a domain group like "Domain Admins" requires the correct command and scope (domain vs. local).
Why A is correct: net group "Domain Admins" John /add /domain adds user John to the domain-level "Domain Admins" group, per CNSP's domain privilege management.
Why other options are incorrect:
B: net user creates users, not group memberships; syntax is wrong.
C: /admin is invalid; correct group specification is missing.
D: Targets local "Administrator" group, not domain "Domain Admins".

NEW QUESTION # 25
Which of the following services do not encrypt its traffic by default?

- A. DNS
- B. SSH
- C. FTPS
- D. All of these

Answer: A

Explanation:
Encryption ensures confidentiality and integrity of network traffic. Analyzing defaults:
A . DNS (Domain Name System):
Default: Unencrypted (UDP/TCP 53), per RFC 1035. Queries/responses (e.g., "google.com → 142.250.190.14") are plaintext.
Modern Options: DNS over HTTPS (DoH, TCP 443) or DNS over TLS (DoT, TCP 853) encrypt, but aren't default in most systems (e.g., pre-2020 Windows).
B . SSH (Secure Shell):
Default: Encrypted (TCP 22), per RFC 4251. Uses asymmetric (e.g., RSA) and symmetric (e.g., AES) crypto for all sessions.
C . FTPS (FTP Secure):
Default: Encrypted (TCP 21 control, dynamic data ports). Extends FTP with SSL/TLS (e.g., RFC 4217), securing file transfers.
Technical Details:
DNS: Plaintext exposes queries to eavesdropping (e.g., ISP snooping) or spoofing (e.g., cache poisoning).
SSH/FTPS: Encryption is baked into their standards; disabling it requires explicit misconfiguration.
Security Implications: Unencrypted DNS risks privacy and integrity (e.g., Kaminsky attack). CNSP likely pushes DoH/DoT adoption.
Why other options are incorrect:
B, C: Encrypt by default.

D: False, as only DNS lacks default encryption.
Real-World Context: The 2013 Snowden leaks exposed DNS monitoring; DoH uptake (e.g., Cloudflare 1.1.1.1) counters this.

NEW QUESTION # 26
Which Kerberos ticket is required to generate a Silver Ticket?

- A. Ticket-Granting Ticket
- B. Service Account Ticket
- C. There is no specific ticket required for generating a Silver Ticket
- D. Session Ticket

Answer: B

Explanation:
A Silver Ticket is a forged Kerberos Service Ticket (TGS - Ticket Granting Service) in Active Directory, granting access to a specific service (e.g., MSSQL, CIFS) without KDC interaction. Unlike a Golden Ticket (TGT forgery), it requires:
Service Account's NTLM Hash: The target service's account (e.g., MSSQLSvc) hash, not a ticket.
Forgery: Tools like Mimikatz craft the TGS (e.g., kerberos::golden /service:<spn> /user:<user> /ntlm:<hash>).
Kerberos Flow (RFC 4120):
TGT (Ticket-Granting Ticket): Obtained via AS (Authentication Service) with user creds.
TGS: Requested from TGS (Ticket Granting Service) using TGT for service access.
Silver Ticket Process:
No TGT needed; the attacker mimics the TGS step using the service account's stolen hash (e.g., from a compromised host).
C . Service Account Ticket: Misnomer-it's the hash of the service account (e.g., MSSQLSvc) that enables forgery, not a pre-existing ticket. CNSP's phrasing likely tests this nuance.
Security Implications: Silver Tickets are stealthier than Golden Tickets (service-specific, shorter-lived). CNSP likely stresses hash protection (e.g., LAPS) and Kerberos monitoring.
Why other options are incorrect:
A . Session Ticket: Not a Kerberos term; confuses session keys.
B . TGT: Used for Golden Tickets, not Silver.
D: Incorrect; the service account's hash (implied by "ticket") is essential.
Real-World Context: Silver Tickets exploited in APT29 attacks (2020 SolarWinds) for lateral movement.

NEW QUESTION # 27
Which SMB (Server Message Block) network protocol version introduced support for encrypting SMB traffic?

- A. None of the above
- B. SMBv3
- C. SMBv1
- D. SMBv2

Answer: B

Explanation:
The SMB protocol, used for file and printer sharing, has evolved across versions, with significant security enhancements in later iterations.
Why C is correct: SMBv3, introduced with Windows 8 and Server 2012, added native support for encrypting SMB traffic. This feature uses AES-CCM encryption to protect data in transit, addressing vulnerabilities in earlier versions. CNSP notes SMBv3's encryption as a critical security improvement.
Why other options are incorrect:
A . SMBv1: Lacks encryption support and is considered insecure, often disabled due to vulnerabilities like WannaCry exploitation.
B . SMBv2: Introduces performance improvements but does not support encryption natively.
D . None of the above: Incorrect, as SMBv3 is the version that introduced encryption.

NEW QUESTION # 28
Where are the password hashes stored in the Linux file system?

- A. /etc/passwd
- B. /etc/password
- C. /etc/shadow
- D. /usr/bin/shadow

Answer: C

Explanation:
In Linux, password hashes are stored in a secure file to protect user authentication data. The evolution of Linux security practices moved password storage from plaintext or weakly protected files to a more secure location.
Why C is correct: The /etc/shadow file is the standard location for storing password hashes in modern Linux systems. This file is readable only by the root user, enhancing security by restricting access. It contains encrypted password hashes (typically using algorithms like SHA-512), along with user details such as password expiration policies. CNSP documentation on Linux security emphasizes /etc/shadow as the authoritative source for password hashes, replacing older methods.
Why other options are incorrect:
A . /etc/passwd: Historically, /etc/passwd stored passwords in plaintext or weakly hashed forms (e.g., using DES), but modern systems use it only for user account information (e.g., UID, GID, home directory) and reference /etc/shadow for hashes.
B . /etc/password: This is not a valid file in the Linux file system; it appears to be a typographical error or misunderstanding, with no recognized role in password storage.
D . /usr/bin/shadow: /usr/bin contains executable binaries, not configuration or data files like password hashes. /etc/shadow is the correct path.

NEW QUESTION # 29
.....

id=1Q840bqCSVpYdlZQu1AC7e5JUzUelj7hb