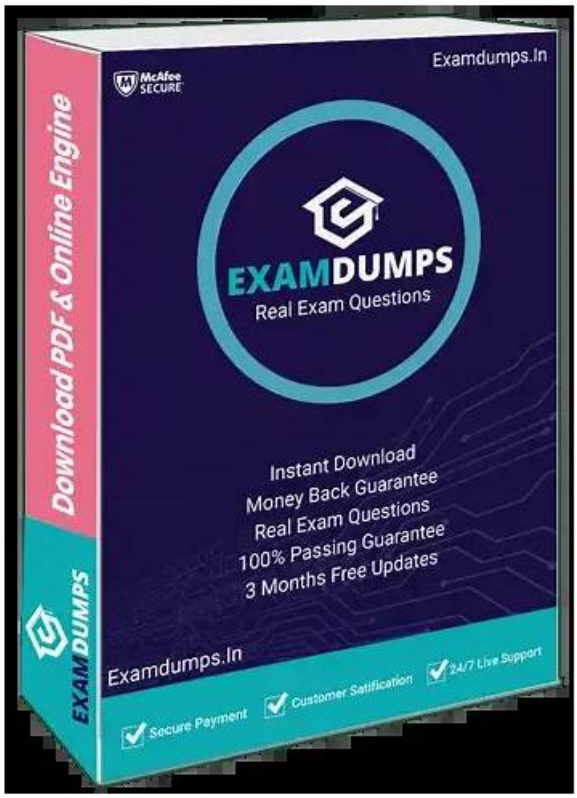
Quiz 2026 The SecOps Group CNSP–Efficient Latest Braindumps Pdf



BONUS!!! Download part of PassExamDumps CNSP dumps for free: https://drive.google.com/open?id=191xN7NWsDx5uze9VtC9o-YMYtqkTQT5t

The pass rate is 99% for CNSP exam materials, and most candidates can pass the exam by using CNSP questions and answers of us. If you choose us, we can ensure you that you can pass the exam just one time. We will give you refund if you fail to pass the exam, you don't need to worry that your money will be wasted. We offer you free demo to have a try before buying CNSP Exam Dumps, so that you can have a better understanding of what will buy. We have online and offline chat service stuff, and if you have any questions about CNSP exam dumps, you can consult us.

We are concentrating on the reform on the CNSP exam material that our candidates try to get aid with. We own the profession experts on compiling the CNSP practice questions and customer service on giving guide on questions from our clients. Our CNSP Preparation materials contain three versions: the PDF, the Software and the APP online. They give you different experience on trying out according to your interests and hobbies. And they can assure your success by precise information.

>> Latest CNSP Braindumps Pdf <<

Valid The SecOps Group - CNSP - Latest Certified Network Security Practitioner Braindumps Pdf

What are you waiting for? Opportunity knocks but once. You can get The SecOps Group CNSP complete as long as you enter PassExamDumps website. You find the best CNSP Exam Training materials, with our exam questions and answers, you will pass the exam.

The SecOps Group CNSP Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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	• 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 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	• 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.
Topic 8	• 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 9	• 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.

The SecOps Group Certified Network Security Practitioner Sample Questions (Q16-Q21):

NEW QUESTION # 16
The application is showing a TLS error message as a result of a website administrator failing to timely renew the TLS certificate. But upon deeper analysis, it appears that the problem is brought on by the expiration of the TLS certificate. Which of the following statements is correct?

- A. The communication between the browser and the server is still over TLS.
- B. The communication between the browser and the server is now no longer over TLS.

Answer: B

Explanation:
TLS (Transport Layer Security) secures communication (e.g., HTTPS) using certificates, per RFC 8446. A certificate includes:
Validity Period: Start and end dates (e.g., "Not After: March 8, 2025").
Purpose: Authenticates the server and encrypts the session.
Scenario: An expired TLS certificate (e.g., past "Not After" date). Modern browsers (e.g., Chrome, Firefox) validate certificates during the handshake:
ClientHello: Browser initiates TLS.
ServerHello: Server sends its certificate.
Validation: Browser checks expiration, CA trust, etc.
If expired, browsers reject the handshake, displaying errors (e.g., "NET::ERR_CERT_DATE_INVALID"). No session key is negotiated, and communication doesn't proceed over TLS. Users may bypass warnings (e.g., "Advanced > Proceed"), but this is unencrypted or uses a fallback (not standard TLS), breaking security guarantees.
Security Implications: Expired certificates expose sites to MITM attacks, as trust is lost. CNSP likely emphasizes certificate management (e.g., automation with Let's Encrypt) to avoid this.
Why other options are incorrect:
B . The communication is still over TLS: False; an expired certificate halts the TLS handshake in compliant browsers. Legacy systems might negotiate insecurely, but this isn't "TLS" per standards.
Real-World Context: The 2019 Equifax breach partially stemmed from expired certificates missing vulnerabilities.

NEW QUESTION # 17
What RID is given to an Administrator account on a Microsoft Windows machine?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: B

Explanation:
In Windows, security principals (users, groups) are identified by a Security Identifier (SID), formatted as S-1-<authority>-<domain>-<RID>. The RID (Relative Identifier) is the final component, unique within a domain or machine. For local accounts:
RID 500: Assigned to the built-in Administrator account on every Windows machine (e.g., S-1-5-21-<machine>-500).
Created during OS install, with full system privileges.
Disabled by default in newer Windows versions (e.g., 10/11) unless explicitly enabled.
RID 501: Guest account (e.g., S-1-5-21-<machine>-501), limited access.
Technical Details:
Stored in SAM (C:\Windows\System32\config\SAM).
Enumeration: Tools like wmic useraccount or net user reveal RIDs.
Domain Context: Domain Admins use RID 512, but the question specifies a local machine.
Security Implications: RID 500 is a prime target for brute-forcing or pass-the-hash attacks (e.g., Mimikatz). CNSP likely advises renaming/disabling it (e.g., via GPO).
Why other options are incorrect:
A . 0: Reserved (e.g., Null SID, S-1-0-0), not a user RID.
C . 501: Guest, not Administrator.
D . 100: Invalid; local user RIDs start at 1000 (e.g., custom accounts).
Real-World Context: Post-compromise, attackers query RID 500 (e.g., net user Administrator) for privilege escalation.

NEW QUESTION # 18
Which of the following represents a valid Windows Registry key?

- A. HKEY_LOCAL_USER
- B. HKEY_INTERNAL_CONFIG
- C. HKEY_LOCAL_MACHINE
- D. HKEY_ROOT_CLASSES

Answer: C

Explanation:

The Windows Registry is a hierarchical database storing system and application settings, organized into predefined root keys (hives). Only specific names are valid as top-level keys.
Why A is correct: HKEY_LOCAL_MACHINE (HKLM) is a standard root key containing hardware and system-wide configuration data. CNSP references it for security settings analysis (e.g., auditing policies).
Why other options are incorrect:
B: HKEY_INTERNAL_CONFIG is not a valid key; no such hive exists.
C: HKEY_ROOT_CLASSES is a misspelling; the correct key is HKEY_CLASSES_ROOT (HKCR).
D: HKEY_LOCAL_USER is incorrect; the valid key is HKEY_CURRENT_USER (HKCU).

NEW QUESTION # 19
Which SMB (Server Message Block) network protocol version introduced support for encrypting SMB traffic?

- A. SMBv1
- B. SMBv3
- C. None of the above
- 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 # 20
On a Microsoft Windows Operating System, what does the following command do?
net localgroup administrators

- A. Displays the local administrators group on the computer
- B. List domain admin users for the current domain

Answer: A

Explanation:
The net command in Windows is a legacy tool for managing users, groups, and network resources. The subcommand net localgroup <groupname> displays information about a specified local group on the machine where it's run. Specifically:
net localgroup administrators lists all members (users and groups) of the local Administrators group on the current computer.
The local Administrators group grants elevated privileges (e.g., installing software, modifying system files) on that machine only, not domain-wide.
Output Example:
Alias name administrators
Comment Administrators have complete and unrestricted access to the computer Members
---------- Administrator Domain Admins The command completed successfully.
Technical Details:
Local groups are stored in the Security Accounts Manager (SAM) database (e.g., C:\Windows\System32\config\SAM).
This differs from domain groups (e.g., Domain Admins), managed via Active Directory.
Security Implications: Enumerating local admins is a reconnaissance step in penetration testing (e.g., to escalate privileges). CNSP likely covers this command for auditing and securing Windows systems.
Why other options are incorrect:
A . List domain admin users for the current domain: This requires net group "Domain Admins" /domain, which queries the domain controller, not the local SAM. net localgroup is strictly local.
Real-World Context: Attackers use this command post-compromise (e.g., via PsExec) to identify privilege escalation targets.

NEW QUESTION # 21
......

Obtaining this CNSP certificate is not an easy task, especially for those who are busy every day. However, if you use our CNSP exam torrent, we will provide you with a comprehensive service to overcome your difficulties and effectively improve your ability. If you can take the time to learn about our CNSP Quiz prep, I believe you will be interested in our CNSP exam questions. Our CNSP learning materials are practically tested, choosing our CNSP exam guide, you will get unexpected surprise.

CNSP Latest Study Guide: https://www.passexamdumps.com/CNSP-valid-exam-dumps.html