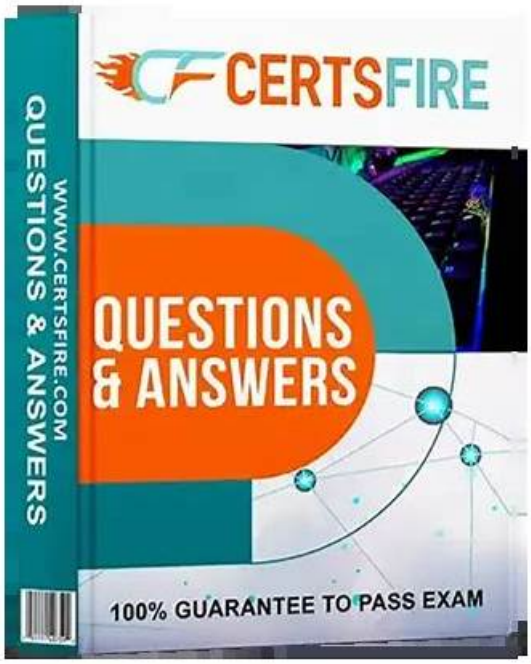
Why do you need to get help from PrepAwayPDF The SecOps Group CNSP Exam Questions?



BONUS!!! Download part of PrepAwayPDF CNSP dumps for free: https://drive.google.com/open?id=1projC2YxbMByeMYcCxa8sGqDL_GiLIsj

For some difficult points of the CNSP exam questions which you may feel hard to understand or easy to confuse for too similar with the others. In order to help you memorize the CNSP guide materials better, we have detailed explanations of the difficult questions such as illustration, charts and referring website. Every year some knowledge of the CNSP Practice Braindumps is reoccurring over and over. You must ensure that you master them completely.

The Internet is increasingly becoming a platform for us to work and learn, while many products are unreasonable in web design, and too much information is not properly classified. It's disorganized. Our CNSP study materials draw lessons from the experience of failure, will all kinds of qualification examination has carried on the classification of clear layout, at the same time the user when they entered the CNSP Study Materials page in the test module classification of clear, convenient to use a very short time to find what they want to study, which began the next exercise.

>> Exams CNSP Torrent <<

Reliable CNSP Test Preparation & Exam CNSP Cram Review

Our PrepAwayPDF website has a long history of providing CNSP test training materials. With many years'hard work, our passing rate of PrepAwayPDF's CNSP exam has achieved 100%. In order to make sure that the accuracy of CNSP test of PrepAwayPDF, our CNSP test training materials are continuing update. If you purchase our CNSP exam dumps, we will offer one year-free update service.

The SecOps Group CNSP Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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 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	• Testing Network Services
Topic 7	• 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 8	• 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 9	• 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 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	• 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 12	• Network Security Tools and Frameworks (such as Nmap, Wireshark, etc)
Topic 13	• 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 14	• 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 15	• 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.

The SecOps Group Certified Network Security Practitioner Sample Questions (Q39-Q44):

NEW QUESTION # 39
What kind of files are "Dotfiles" in a Linux-based architecture?

- A. Hidden files
- B. Library files
- C. Driver files
- D. System files

Answer: A

Explanation:
In Linux, file visibility is determined by naming conventions, impacting how files are listed or accessed in the file system.
Why D is correct: "Dotfiles" are files or directories with names starting with a dot (e.g., .bashrc), making them hidden by default in directory listings (e.g., ls requires -a to show them). They are commonly used for user configuration, as per CNSP's Linux security overview.
Why other options are incorrect:
A: Library files (e.g., in /lib) aren't inherently hidden.
B: Driver files (e.g., kernel modules in /lib/modules) aren't dotfiles by convention.
C: System files may or may not be hidden; "dotfiles" specifically denotes hidden status.

NEW QUESTION # 40
The Management Information Base (MIB) is a collection of object groups that is managed by which service?

- A. SNMP
- B. SMTP
- C. TACACS
- D. NTP

Answer: A

Explanation:
The Management Information Base (MIB) is a structured database defining manageable objects (e.g., CPU usage, interface status) in a network device. It's part of the SNMP (Simple Network Management Protocol) framework, per RFC 1157, used for monitoring and managing network devices (e.g., routers, switches).
SNMP Mechanics:
MIB Structure: Hierarchical, with Object Identifiers (OIDs) like 1.3.6.1.2.1.1.1.0 (sysDescr).
Ports: UDP 161 (agent), 162 (traps).
Operation: Agents expose MIB data; managers (e.g., Nagios) query it via GET/SET commands.
MIB files (e.g., IF-MIB, HOST-RESOURCES-MIB) are vendor-specific or standardized, parsed by SNMP tools (e.g., snmpwalk). CNSP likely covers SNMP for network monitoring and securing it against enumeration (e.g., weak community strings like "public").
Why other options are incorrect:
A . SMTP (Simple Mail Transfer Protocol): Email delivery (TCP 25), unrelated to MIB or device management.
C . NTP (Network Time Protocol): Time synchronization (UDP 123), not MIB-related.
D . TACACS (Terminal Access Controller Access-Control System): Authentication/authorization (TCP 49), not MIB management.
Real-World Context: SNMP misconfiguration led to the 2018 Cisco switch exploits via exposed MIB data.

NEW QUESTION # 41
Which of the following is a valid DNS record type?

- A. NAPTR record
- B. SRV record
- C. TXT record
- D. All of the above

Answer: D

Explanation:
DNS (Domain Name System) records define how domain names are mapped to various types of data, each serving a specific purpose in network operations. The question asks for valid DNS record types, and all listed options are recognized.
Why D is correct:
A . NAPTR record: The Naming Authority Pointer (NAPTR) record is used for service discovery and mapping domain names to services, protocols, and ports (e.g., in SIP or ENUM systems).
B . SRV record: The Service (SRV) record specifies the hostname and port for specific services (e.g., LDAP, XMPP), aiding in service location.
C . TXT record: The Text (TXT) record stores arbitrary text data, often for SPF, DKIM, or domain verification.
All are valid DNS record types per RFC standards and CNSP documentation, making "All of the above" the correct answer.
Why other options are incomplete: A, B, or C alone exclude other valid types listed, so D is the most comprehensive response.

NEW QUESTION # 42
How many octets are there in an IPv6 address?

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

Answer: D

Explanation:
An IPv6 address, defined in RFC 4291, is a 128-bit address designed to replace IPv4's 32-bit scheme, vastly expanding address space (2