The SecOps Group - High Hit-Rate CNSP Latest Dumps Pdf

What's more, part of that PassTestking CNSP dumps now are free: https://drive.google.com/open?id=1yVl4U4d6WvJkmnteDi9fcMyFylJ6LqFH

Our CNSP learning materials are new but increasingly popular choices these days which incorporate the newest information and the most professional knowledge of the practice exam. All points of questions required are compiled into our CNSP Preparation quiz by experts. By the way, the CNSPcertificate is of great importance for your future and education. Our CNSP practice materials cover all the following topics for your reference.

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	• 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 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	• 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 5	- 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 6	- 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 7	- 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 8	- 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 9	- 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 10	- 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 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	- 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	- Testing Network Services
Topic 14	- Network Security Tools and Frameworks (such as Nmap, Wireshark, etc)
Topic 15	- 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 16	- 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 17	- 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 18	- 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.

>> CNSP Latest Dumps Pdf <<

New CNSP Exam Papers | CNSP Vce Format

We have a professional team to collect the first-hand information for the CNSP study materials. We can ensure you that what you receive is the latest version for the CNSP exam dumps. We are strict with quality and answers of exam dumps. Besides, we offer you free update for one year, and you can get the latest information about CNSP Exam Dumps. We also have online and offline chat service stuff to answer all the questions. If you have any questions about CNSP exam materials, just contact us, we will give you reply as soon as we can.

The SecOps Group Certified Network Security Practitioner Sample Questions (Q31-Q36):

NEW QUESTION # 31
If you find the 111/TCP port open on a Unix system, what is the next logical step to take?

- A. Telnet to the port, send "GET / HTTP/1.0" and gather information from the response.
- B. Telnet to the port to look for a banner.
- C. None of the above.
- D. Run "rpcinfo -p <hostname>" to enumerate the RPC services.

Answer: D

Explanation:
Port 111/TCP is the default port for the RPC (Remote Procedure Call) portmapper service on Unix systems, which registers and manages RPC services.
Why A is correct: Running rpcinfo -p <hostname> queries the portmapper to list all registered RPC services, their programs, versions, and associated ports. This is a logical next step during a security audit or penetration test to identify potential vulnerabilities (e.g., NFS or NIS services). CNSP recommends this command for RPC enumeration.
Why other options are incorrect:
B . Telnet to the port to look for a banner: Telnet might connect, but RPC services don't typically provide a human-readable banner, making this less effective than rpcinfo.
C . Telnet to the port, send "GET / HTTP/1.0" and gather information from the response: Port 111 is not an HTTP service, so an HTTP request is irrelevant and will likely fail.
D . None of the above: Incorrect, as A is a valid and recommended step.

NEW QUESTION # 32
Which of the following attacks are associated with an ICMP protocol?

- A. ICMP flooding
- B. All of the following
- C. Smurf attack
- D. Ping of death

Answer: B

Explanation:
ICMP (Internet Control Message Protocol), per RFC 792, handles diagnostics (e.g., ping) and errors in IP networks. It's exploitable in:
A . Ping of Death:
Method: Sends oversized ICMP Echo Request packets (>65,535 bytes) via fragmentation. Reassembly overflows buffers, crashing older systems (e.g., Windows 95).
Fix: Modern OSes cap packet size (e.g., ping -s 65500).
B . Smurf Attack:
Method: Spoofs ICMP Echo Requests to a network's broadcast address (e.g., 192.168.255.255). All hosts reply, flooding the victim.
Amplification: 100 hosts = 100x traffic.
C . ICMP Flooding:
Method: Overwhelms a target with ICMP Echo Requests (e.g., ping -f), consuming bandwidth/CPU.
Variant: BlackNurse attack targets firewalls.
Technical Details:
ICMP Type 8 (Echo Request), Type 0 (Echo Reply) are key.
Mitigation: Rate-limit ICMP, disable broadcasts (e.g., no ip directed-broadcast).
Security Implications: ICMP attacks are DoS vectors. CNSP likely teaches filtering (e.g., iptables -p icmp -j DROP) balanced with

diagnostics need.
Why other options are incorrect:
A, B, C individually: All are ICMP-based; D is comprehensive.
Real-World Context: Smurf attacks peaked in the 1990s; modern routers block them by default.

NEW QUESTION # 33
What is the response from an open TCP port which is not behind a firewall?

- A. A SYN and an ACK packet
- B. A FIN and an ACK packet
- C. A SYN packet
- D. A RST and an ACK packet

Answer: A

Explanation:
TCP's three-way handshake, per RFC 793, establishes a connection:
Client → Server: SYN (Synchronize) packet (e.g., port 80).
Server → Client: SYN-ACK (Synchronize-Acknowledge) packet if the port is open and listening.
Client → Server: ACK (Acknowledge) completes the connection.
Scenario: An open TCP port (e.g., 80 for HTTP) with no firewall. When a client sends a SYN to an open port (e.g., via telnet 192.168.1.1 80), the server responds with a SYN-ACK packet, indicating willingness to connect. No firewall means no filtering alters this standard response.
Packet Details:
SYN-ACK: Sets SYN and ACK flags in the TCP header, with a sequence number and acknowledgment number.
Example: Client SYN (Seq=100), Server SYN-ACK (Seq=200, Ack=101).
Security Implications: Open ports responding with SYN-ACK are easily detected (e.g., Nmap "open" state), inviting exploits if unneeded (e.g., Telnet on 23). CNSP likely stresses port minimization and monitoring.
Why other options are incorrect:
A . A FIN and an ACK packet: FIN-ACK closes an established connection, not a response to a new SYN.
B . A SYN packet: SYN initiates a connection from the client, not a server response.
D . A RST and an ACK packet: RST-ACK rejects a connection (e.g., closed port), not an open one.
Real-World Context: SYN-ACK from SSH (22/TCP) confirms a server's presence during reconnaissance.

NEW QUESTION # 34
How many octets are there in an IPv6 address?

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

Answer: C

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