Free PDF Quiz 2025 Reliable The SecOps Group CNSP: Reliable Certified Network Security Practitioner Braindumps Sheet

BTW, DOWNLOAD part of ActualCollection CNSP dumps from Cloud Storage: https://drive.google.com/open?id=1A0vXWT02EP22yEq6ER58VivqSlPZg-hQ

As the labor market becomes more competitive, a lot of people, of course including students, company employees, etc., and all want to get CNSP authentication in a very short time, this has developed into an inevitable trend. Each of them is eager to have a strong proof to highlight their abilities, so they have the opportunity to change their current status, including getting a better job, have higher pay, and get a higher quality of material, etc. It is not easy to qualify for a qualifying exam in such a short period of time. Our company's CNSP learning material is very good at helping customers pass the exam and obtain a certificate in a short time, and now I'm going to show you our CNSP Learning materials.

The CNSP certification is the way to go in the modern The SecOps Group era. Success in the Certified Network Security Practitioner exam of this certification plays an essential role in an individual's future growth. Nowadays, almost every tech aspirant is taking the test to get CNSP certification and find well-paying jobs or promotions. But the main issue that most of the candidates face is not finding updated The SecOps Group CNSP Practice Questions to prepare successfully for the The SecOps Group CNSP certification exam in a short time.

>> Reliable CNSP Braindumps Sheet <<

100% Pass The SecOps Group - Accurate CNSP - Reliable Certified Network Security Practitioner Braindumps Sheet

If you want to get a desirable opposition and then achieve your career dream, you are a right place now. Our CNSP Study Tool can help you pass the exam. So, don't be hesitate, choose the CNSP test torrent and believe in us. Let's strive to our dreams together. Life is short for us, so we all should cherish our life. Our Certified Network Security Practitioner guide torrent can help you to save your valuable time and let you have enough time to do other things you want to do.

The SecOps Group CNSP Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 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	• 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 6	• 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 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	• 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 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	• Testing Network Services
Topic 11	• Network Security Tools and Frameworks (such as Nmap, Wireshark, etc)
Topic 12	• 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 13	• 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 14	• 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 15	• 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 16	• 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 (Q19-Q24):

NEW QUESTION # 19
Which of the aforementioned SSL/TLS protocols are considered to be unsafe?

- A. SSLv2 and SSLv3
- B. Both A and B
- C. SSLv2, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3
- D. TLSv1.0 and TLSv1.1

Answer: B

Explanation:
SSL/TLS protocols secure network communication, but older versions have vulnerabilities:
SSLv2 (1995): Weak ciphers, no handshake integrity (e.g., MITM via DROWN attack, CVE-2016-0800). Deprecated by RFC 6176 (2011).
SSLv3 (1996): Vulnerable to POODLE (CVE-2014-3566), weak block ciphers (e.g., RC4). Deprecated by RFC 7568 (2015).
TLSv1.0 (1999, RFC 2246): Inherits SSLv3 flaws (e.g., BEAST, CVE-2011-3389), weak CBC ciphers. Deprecated by PCI DSS (2018) and RFC 8996 (2021).
TLSv1.1 (2006, RFC 4346): Improved over 1.0 but lacks modern cipher suites (e.g., AEAD). Deprecated with 1.0 by RFC 8996.
TLSv1.2 (2008, RFC 5246): Secure with strong ciphers (e.g., AES-GCM), widely used today.
TLSv1.3 (2018, RFC 8446): Latest, removes legacy weaknesses, mandatory forward secrecy.
Why other options are incorrect:
A: Correct but incomplete without B.
B: Correct but incomplete without A.
D: Incorrectly includes TLSv1.2 and 1.3, which are secure and recommended.
Real-World Context: POODLE forced mass SSLv3 disablement in 2014; TLS 1.0/1.1 deprecation hit legacy systems in 2021.

NEW QUESTION # 20
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 # 21
What is the response from a closed TCP port which is behind a firewall?

- A. A FIN and an ACK packet
- B. A SYN and an ACK packet
- C. RST and an ACK packet
- D. No response

Answer: D

Explanation:
TCP (Transmission Control Protocol) uses a three-way handshake (SYN, SYN-ACK, ACK) to establish connections, as per RFC 793. When a client sends a SYN packet to a port:
Open Port: The server responds with SYN-ACK.
Closed Port (no firewall): The server sends an RST (Reset) packet, often with ACK, to terminate the attempt immediately.
However, when a firewall is present, its configuration dictates the response. Modern firewalls typically operate in stealth mode, using a "drop" rule for closed ports rather than a "reject" rule:
Drop: Silently discards the packet without replying, resulting in no response. The client experiences a timeout (e.g., 30 seconds), as no feedback is provided.
Reject: Sends an RST or ICMP "Port Unreachable," but this is less common for security reasons, as it confirms the firewall's presence.
For a closed TCP port behind a firewall, "no response" (drop) is the standard behavior in secure configurations, minimizing information leakage to attackers. This aligns with CNSP's focus on firewall best practices to obscure network topology during port scanning (e.g., with Nmap).
Why other options are incorrect:
A . A FIN and an ACK packet: FIN-ACK is used to close an established TCP connection gracefully (e.g., after data transfer), not to respond to an initial SYN on a closed port.
B . RST and an ACK packet: RST-ACK is the host's response to a closed port without a firewall. A firewall's drop rule overrides this by silently discarding the packet.
C . A SYN and an ACK packet: SYN-ACK indicates an open port accepting a connection, the opposite of a closed port scenario.
Real-World Context: Tools like Nmap interpret "no response" as "filtered" (firewall likely present) vs. "closed" (RST received), aiding in firewall detection.

NEW QUESTION # 22
Which of the following services use TCP protocol?

- A. NTP
- B. SNMP
- C. IKE
- D. HTTP

Answer: D

Explanation:
TCP (Transmission Control Protocol) ensures reliable, ordered data delivery via a connection-oriented handshake, contrasting with UDP's lightweight, connectionless approach. Analyzing each service:
C . HTTP (Hypertext Transfer Protocol): Uses TCP (port 80) for web traffic. TCP's reliability ensures HTML, images, etc., arrive intact. HTTPS (TCP 443) extends this with TLS. RFC 2616 mandates TCP.
A . SNMP (Simple Network Management Protocol): Defaults to UDP (port 161) for monitoring devices. UDP's speed suits its lightweight queries, though TCP variants exist (rarely used).
B . NTP (Network Time Protocol): Uses UDP (port 123) per RFC 5905. UDP minimizes latency for time sync, tolerating occasional packet loss.
D . IKE (Internet Key Exchange): Part of IPsec, uses UDP (port 500) per RFC 7296. UDP suits its negotiation phase; TCP isn't standard.
Security Implications: TCP services like HTTP are more prone to state-based attacks (e.g., SYN floods) than UDP counterparts. CNSP likely contrasts TCP vs. UDP in protocol analysis.
Why other options are incorrect:
A, B, D: All default to UDP for efficiency, not TCP's reliability.
Real-World Context: Firewalls prioritize TCP 80/443 rules for HTTP/HTTPS, while UDP 123 is opened for NTP servers.

NEW QUESTION # 23
How many usable TCP/UDP ports are there?

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

Answer: D

Explanation:
TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) port numbers are defined by a 16-bit field in their packet headers, as specified in RFC 793 (TCP) and RFC 768 (UDP). A 16-bit integer ranges from 0 to 65,535, yielding a total of 65,536 possible ports (2