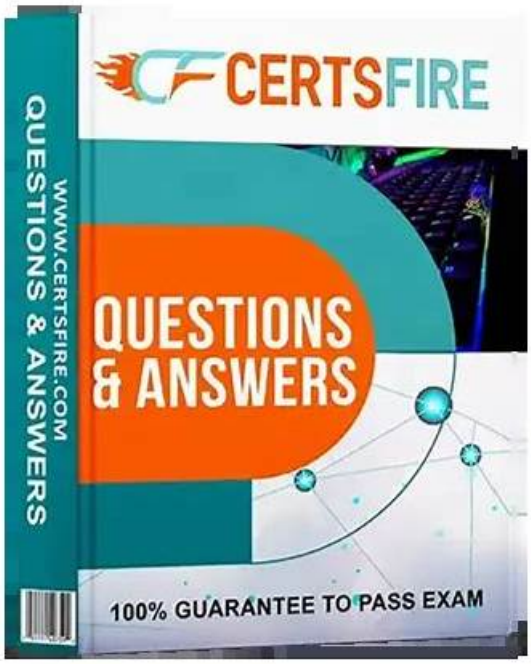
Free PDF Quiz 2026 The SecOps Group CNSP–High-quality Exam Blueprint



DOWNLOAD the newest Exam4Docs CNSP PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1RvyVaVvgvXR025FysUtbzKl1c9BcI5bw

Our Exam4Docs has devoted more time and efforts to develop the CNSP exam software for you to help you successfully obtain CNSP exam certification with less time and efforts. Our promise of "no help, full refund" is not empty talk. No matter how confident we are in our dumps, once our dumps do not satisfy you or have no help for you, we will immediately full refund all your money you purchased our CNSP Exam software. However, we believe that our CNSP exam software will meet your expectation, and wish you success!

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	• 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 3	• 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 4	• 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 5	• Network Security Tools and Frameworks (such as Nmap, Wireshark, etc)
Topic 6	• 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 7	• 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 8	• 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 9	• 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 10	• 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 11	• 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 12	• 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 13	• Testing Network Services
Topic 14	• 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 15	• 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 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.

>> Exam CNSP Blueprint <<

Pass Guaranteed Quiz 2026 Accurate The SecOps Group CNSP: Exam Certified Network Security Practitioner Blueprint

Exam4Docs's CNSP certification is a dispensable part in IT area. So how can we achieve it in a short time? Exam4Docs will be your choice. CNSP test training materials of Exam4Docs are organized by experienced IT experts. If you still worry, you can download CNSP free demo before purchase.

The SecOps Group Certified Network Security Practitioner Sample Questions (Q15-Q20):

NEW QUESTION # 15
If you find the 111/TCP port open on a Unix system, what is the next logical step to take?

- A. None of the above.
- B. Telnet to the port, send "GET / HTTP/1.0" and gather information from the response.
- C. Telnet to the port to look for a banner.
- 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 # 16
Which of the following is true for SNMP?
A) The default community string for read-only access is "public."
B) The default community string for read/write access is "private."

- A. Only A
- B. Only B
- C. None of the above
- D. Both A and B

Answer: D

Explanation:
SNMP community strings authenticate access, with defaults posing security risks if unchanged.
Why C is correct:
A: "public" is the standard read-only default, per SNMP specs and CNSP.
B: "private" is the standard read-write default, also per SNMP and CNSP.
Both are true, making C the answer.
Why other options are incorrect:
1, 2: Exclude one true statement each.
4: Both statements are true, so "none" is wrong.

NEW QUESTION # 17
WannaCry, an attack, spread throughout the world in May 2017 using machines running on outdated Microsoft operating systems. What is WannaCry?

- A. Malware
- B. Ransomware

Answer: B

Explanation:
WannaCry is a ransomware attack that erupted in May 2017, infecting over 200,000 systems across 150 countries. It exploited the EternalBlue vulnerability (MS17-010) in Microsoft Windows SMBv1, targeting unpatched systems (e.g., Windows XP, Server 2003). Developed by the NSA and leaked by the Shadow Brokers, EternalBlue allowed remote code execution.
Ransomware Mechanics:
Encryption: WannaCry used RSA-2048 and AES-128 to encrypt files, appending extensions like .wcry.
Ransom Demand: Displayed a message demanding $300-$600 in Bitcoin, leveraging a hardcoded wallet.
Worm Propagation: Self-replicated via SMB, scanning internal and external networks, unlike typical ransomware requiring user interaction (e.g., phishing).
Malware Context: While WannaCry is malware (malicious software), "ransomware" is the precise subcategory, distinguishing it from viruses, trojans, or spyware. Malware is a broad term encompassing any harmful code; ransomware specifically encrypts data for extortion. CNSP likely classifies WannaCry as ransomware to focus on its payload and mitigation (e.g., patching, backups).
Why other options are incorrect:
B . Malware: Correct but overly generic. WannaCry's defining trait is ransomware behavior, not just maliciousness. Specificity matters in security taxonomy for threat response (e.g., NIST IR 8019).
Real-World Context: WannaCry crippled NHS hospitals, highlighting patch management's criticality. A kill switch (a domain sinkhole) halted it, but variants persist.

NEW QUESTION # 18
Which of the following protocols is not vulnerable to address spoofing attacks if implemented correctly?

- A. TCP
- B. IP
- C. UDP
- D. ARP

Answer: A

Explanation:
Address spoofing fakes a source address (e.g., IP, MAC) to impersonate or amplify attacks. Analyzing protocol resilience:
C . TCP (Transmission Control Protocol):
Mechanism: Three-way handshake (SYN, SYN-ACK, ACK) verifies both endpoints.
Client SYN (Seq=X), Server SYN-ACK (Seq=Y, Ack=X+1), Client ACK (Ack=Y+1).
Spoofing Resistance: Spoofer must predict the server's sequence number (randomized in modern stacks) and receive SYN-ACK, impractical without session hijacking or MITM.
Correct Implementation: RFC 793-compliant, with anti-spoofing (e.g., Linux tcp_syncookies).
A . UDP:
Connectionless (RFC 768), no handshake. Spoofed packets (e.g., source IP 1.2.3.4) are accepted if port is open, enabling reflection attacks (e.g., DNS amplification).
B . ARP (Address Resolution Protocol):
No authentication (RFC 826). Spoofed ARP replies (e.g., fake MAC for gateway IP) poison caches, enabling MITM (e.g., arpspoof).
D . IP:
No inherent validation at Layer 3 (RFC 791). Spoofed source IPs pass unless filtered (e.g., ingress filtering, RFC 2827).
Security Implications: TCP's handshake makes spoofing harder, though not impossible (e.g., blind spoofing with sequence prediction, mitigated since BSD 4.4). CNSP likely contrasts this with UDP/IP's vulnerabilities in DDoS contexts.
Why other options are incorrect:
A, B, D: Lack handshake or authentication, inherently spoofable.
Real-World Context: TCP spoofing was viable pre-1990s (e.g., Mitnick attack); modern randomization thwarts it.

NEW QUESTION # 19
Which is the correct command to change the MAC address for an Ethernet adapter in a Unix-based system?

- A. ifconfig eth0 hw ether AA:BB:CC:DD:EE:FF
- B. ifconfig eth0 hdwr ether AA:BB:CC:DD:EE:FF
- C. ifconfig eth0 hdw ether AA:BB:CC:DD:EE:FF
- D. ifconfig eth0 hwr ether AA:BB:CC:DD:EE:FF

Answer: A

Explanation:
In Unix-based systems (e.g., Linux), the ifconfig command is historically used to configure network interfaces, including changing the Media Access Control (MAC) address of an Ethernet adapter. The correct syntax to set a new MAC address for an interface like eth0 is ifconfig eth0 hw ether AA:BB:CC:DD:EE:FF, where hw specifies the hardware address type (ether for Ethernet), followed by the new MAC address in colon-separated hexadecimal format.
Why A is correct: The hw ether argument is the standard and correct syntax recognized by ifconfig to modify the MAC address. This command temporarily changes the MAC address until the system reboots or the interface is reset, assuming the user has sufficient privileges (e.g., root). CNSP documentation on network configuration and spoofing techniques validates this syntax for testing network security controls.
Why other options are incorrect:
B: hdw is not a valid argument; it's a typographical error and unrecognized by ifconfig.
C: hdwr is similarly invalid; no such shorthand exists in the command structure.
D: hwr is incorrect; the full keyword hw followed by ether is required for proper parsing.

NEW QUESTION # 20
.....