CNSP Paper - CNSP Interactive Practice Exam

P.S. Free & New CNSP dumps are available on Google Drive shared by TestPassKing: https://drive.google.com/open?id=1s59XzNz0u5xdZkkV-96_o5Y3r6josJZf

I think these smart tips will help you to study well for the exam and get a brilliant score without any confusion. To get the Certified Network Security Practitioner CNSP practice test, find a reliable source that provides the CNSP Exam Dumps to their clients. Certified Network Security Practitioner CNSP certification exams are not easy but quite tricky to know whether the applicant has complete knowledge regarding the subject or not.

The SecOps Group CNSP Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• Network Security Tools and Frameworks (such as Nmap, Wireshark, etc)
Topic 4	• 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 5	• 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 6	• 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 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	• 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 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	• 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 12	• 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.

CNSP Interactive Practice Exam - CNSP Valid Test Review

The CNSP would assist applicants in preparing for the The SecOps Group CNSP exam successfully in one go CNSP would provide CNSP candidates with accurate and real Certified Network Security Practitioner (CNSP) Dumps which are necessary to clear the CNSP test quickly. Students will feel at ease since the content they are provided with is organized rather than dispersed.

The SecOps Group Certified Network Security Practitioner Sample Questions (Q18-Q23):

NEW QUESTION # 18
Which is the correct command to change the MAC address for an Ethernet adapter in a Unix-based system?

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

Answer: D

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

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

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
A system encrypts data prior to transmitting it over a network, and the system on the other end of the transmission media decrypts it. If the systems are using a symmetric encryption algorithm for encryption and decryption, which of the following statements is true?

- A. A symmetric encryption algorithm uses different keys to encrypt and decrypt data at both ends of the transmission media.
- B. A symmetric encryption algorithm does not use keys to encrypt and decrypt data at both ends of the transmission media.
- C. A symmetric encryption algorithm is an insecure method used to encrypt data transmitted over transmission media.
- D. A symmetric encryption algorithm uses the same key to encrypt and decrypt data at both ends of the transmission media.

Answer: D

Explanation:
Symmetric encryption is a cryptographic technique where the same key is used for both encryption and decryption processes. In the context of network security, when data is encrypted prior to transmission and decrypted at the receiving end using a symmetric encryption algorithm (e.g., AES or Triple-DES), both the sender and receiver must share and utilize an identical secret key. This key is applied by the sender to transform plaintext into ciphertext and by the receiver to reverse the process, recovering the original plaintext. The efficiency of symmetric encryption makes it ideal for securing large volumes of data transmitted over networks, provided the key is securely distributed and managed.
Why A is correct: Option A accurately describes the fundamental property of symmetric encryption-using a single shared key for both encryption and decryption. This aligns with CNSP documentation, which emphasizes symmetric encryption's role in securing data in transit (e.g., via VPNs or secure file transfers).
Why other options are incorrect:
B: This describes asymmetric encryption (e.g., RSA), where different keys (public and private) are used for encryption and decryption, not symmetric encryption.
C: Symmetric encryption inherently relies on keys; the absence of keys contradicts its definition and operational mechanism.
D: Symmetric encryption is not inherently insecure; its security depends on key strength and management practices, not the algorithm itself. CNSP highlights that algorithms like AES are widely regarded as secure when implemented correctly.

NEW QUESTION # 21
The Active Directory database file stores the data and schema information for the Active Directory database on domain controllers in Microsoft Windows operating systems. Which of the following file is the Active Directory database file?

- A. NTDS.DIT
- B. NTDS.MDB
- C. NTDS.DAT
- D. MSAD.MDB

Answer: A

Explanation:
The Active Directory (AD) database on Windows domain controllers contains critical directory information, stored in a specific file

format.
Why D is correct: The NTDS.DIT file (NT Directory Services Directory Information Tree) is the Active Directory database file, located in C:\Windows\NTDS\ on domain controllers. It stores all AD objects (users, groups, computers) and schema data in a hierarchical structure. CNSP identifies NTDS.DIT as the key file for AD data extraction in security audits.
Why other options are incorrect:
A . NTDS.DAT: Not a valid AD database file; may be a confusion with other system files.
B . NTDS.MDB: Refers to an older Microsoft Access database format, not used for AD.
C . MSAD.MDB: Not a recognized file for AD; likely a misnomer.

NEW QUESTION # 22
Which of the following is an example of a SUID program?

- A. /bin/ls
- B. /usr/bin/passwd
- C. /usr/bin/curl
- D. None of the above

Answer: B

Explanation:
In Linux/Unix, the SUID (Set User ID) bit allows a program to execute with the owner's permissions, typically root, rather than the caller's. It's denoted by an s in the user execute field (e.g., -rwsr-xr-x). Common SUID programs perform privileged tasks requiring temporary elevation.
Analysis:
C . /usr/bin/passwd:
Purpose: Updates user passwords in /etc/shadow (root-owned, 0600 perms).
Permissions: Typically -rwsr-xr-x, owned by root. The SUID bit lets non-root users modify shadow securely.
Command: ls -l /usr/bin/passwd confirms SUID (s in user execute).
A . /bin/ls:
Purpose: Lists directory contents, no privileged access needed.
Permissions: -rwxr-xr-x (no SUID). Runs as the calling user.
B . /usr/bin/curl:
Purpose: Transfers data over HTTP/FTP, no root privileges required by default.
Permissions: -rwxr-xr-x (no SUID).
Technical Details:
SUID Bit: Set via chmod u+s <file> or chmod 4755.
Security: SUID binaries are audited (e.g., find / -perm -u=s) due to escalation risks if writable or poorly coded (e.g., buffer overflows).
Security Implications: CNSP likely highlights SUID as an attack vector (e.g., CVE-1996-0095 exploited passwd flaws). Hardening removes unnecessary SUID bits.
Why other options are incorrect:
A, B: Lack SUID; no privileged operations.
D: Incorrect, as /usr/bin/passwd is a SUID example.
Real-World Context: SUID on /bin/su or /usr/bin/sudo similarly enables privilege escalation, often targeted in exploits.

NEW QUESTION # 23
.....

CNSP] on ▸ www.real4dumps.com ◂ will open immediately □Dump CNSP File

- CNSP Latest Learning Material □ Trustworthy CNSP Source □ Latest CNSP Braindumps □ Go to website （ www.pdfvce.com ） open and search for 【 CNSP 】 to download for free ↔Online CNSP Training Materials
- Quiz CNSP - Certified Network Security Practitioner –Efficient Paper □ Copy URL ☀ www.exams4collection.com □☀□ open and search for 「 CNSP 」 to download for free □Regualer CNSP Update
- Trustworthy CNSP Source □ Test CNSP Score Report □ Study CNSP Dumps □ Open website ➤ www.pdfvce.com □ and search for □ CNSP □ for free download □Online CNSP Training Materials
- CNSP Valid Test Testking □ Dump CNSP File ⤴ CNSP Free Practice □ Easily obtain { CNSP } for free download through ➽ www.pass4leader.com □ □Trustworthy CNSP Source
- Latest CNSP Exam Papers □ Authorized CNSP Certification □ CNSP Exam Vce □ Download 「 CNSP 」 for free by simply searching on ➥ www.pdfvce.com □ □Latest CNSP Exam Papers
- Test CNSP Score Report □ Test CNSP Score Report □ Regualer CNSP Update □ Search on [www.passtestking.com] for ☀ CNSP □☀□ to obtain exam materials for free download □Regualer CNSP Update
- 100% Pass Quiz 2025 The SecOps Group Realistic CNSP Paper □ Enter □ www.pdfvce.com □ and search for ➽ CNSP □ to download for free □CNSP Pdf Pass Leader
- Pass Guaranteed Quiz The SecOps Group - CNSP - Certified Network Security Practitioner Newest Paper □ The page for free download of ➠ CNSP □ on ✔ www.getvalidtest.com □✔□ will open immediately □Training CNSP For Exam
- dougwar742.blogocial.com, artofmanmaking.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, rocourses.in, pct.edu.pk, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, yu856.com, www.latifaalkurd.com, rickwal443.full-design.com, ncon.edu.sa, Disposable vapes

What's more, part of that TestPassKing CNSP dumps now are free: https://drive.google.com/open?id=1s59XzNz0u5xdZkkV-96_o5Y3r6josJZf