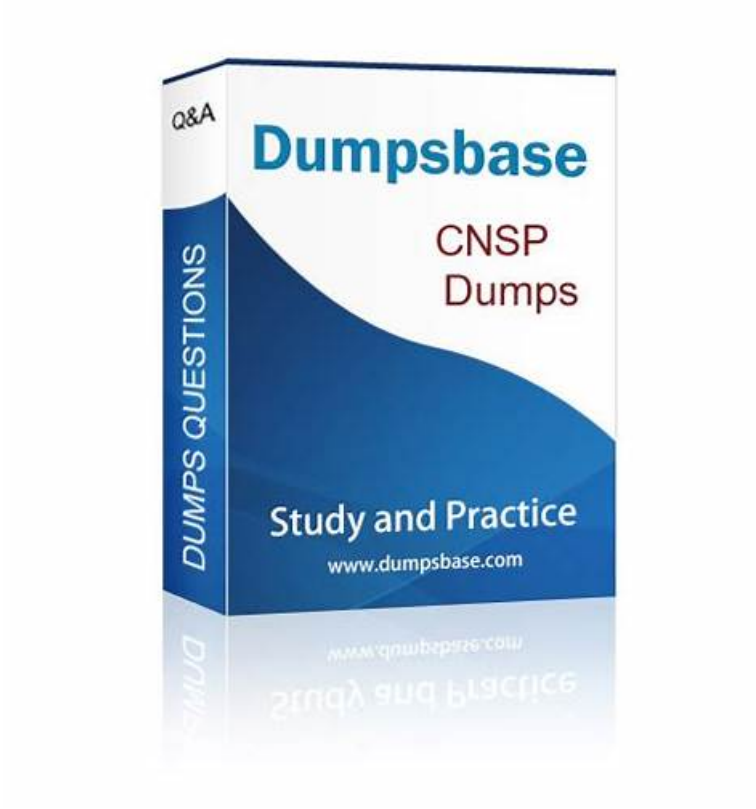
CNSP Dumps & CNSP Übungsmaterialien



Außerdem sind jetzt einige Teile dieser It-Pruefung CNSP Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1kATvKk_PcPJZ34izRdiCRxud77IRmXwN

Die Produkte von It-Pruefung sind von guter Qualität. Sie sind am schnellsten aktualisiert. Wenn Sie die Schulungsunterlagen zur The SecOps Group CNSP Zertifizierungsprüfung kaufen, können Sie die The SecOps Group CNSP Zertifizierungsprüfung sicher bestehen.

The SecOps Group CNSP Prüfungsplan:

Thema	Einzelheiten
Thema 1	• 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.
Thema 2	• 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.
Thema 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.
Thema 4	• 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.

Thema 5	• 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.
Thema 6	• 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.
Thema 7	• 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.
Thema 8	• 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.
Thema 9	• 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.
Thema 10	• Testing Network Services
Thema 11	• 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.
Thema 12	• 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.
Thema 13	• 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.
Thema 14	• 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.
Thema 15	• 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.
Thema 16	• 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.

CNSP Übungsmaterialien, CNSP Vorbereitungsfragen

Machen Sie Sorge um die CNSP von The SecOps Group Prüfung, weil Sie nur noch ein Anfänger sind? Von jetzt an wird It-Pruefung alle Probleme für Sie lösen. Die Lernhilfe von The SecOps Group CNSP Zertifizierung sind umfassend und enthalten

unterschiedliche Ziele, daher können sogar die Anfänger sie leicht erfassen. Sie würden den Schlüssel für den Durchlauf der CNSP Prüfung haben und Selbstsicherheit gewinnen, wenn Sie solche Lernhilfe haben. Dann warum warten Sie noch?

The SecOps Group Certified Network Security Practitioner CNSP Prüfungsfragen mit Lösungen (Q22-Q27):

22. Frage
Which of the following protocols is not vulnerable to address spoofing attacks if implemented correctly?

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

Antwort: A

Begründung:
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.

23. Frage
What is the response from a closed TCP port which is not behind a firewall?

- A. ICMP message showing Port Unreachable
- B. A FIN and an ACK packet
- C. A RST and an ACK packet
- D. A SYN and an ACK packet

Antwort: C

Begründung:
TCP uses a structured handshake, and its response to a connection attempt on a closed port follows a specific protocol when unobstructed by a firewall.
Why C is correct: A closed TCP port responds with a RST (Reset) and ACK (Acknowledgment) packet to terminate the connection attempt immediately. CNSP highlights this as a key scanning indicator.
Why other options are incorrect:
A: ICMP Port Unreachable is for UDP, not TCP.
B: FIN/ACK is for closing active connections, not rejecting new ones.
D: SYN/ACK indicates an open port during the TCP handshake.

24. Frage
Which of the following files has the SGID permission set?
-rwxr-sr-x 1 root root 4096 Jan 1 08:00 myfile
-rwsr-xr-x 1 root root 4096 Jan 1 00:08 myprogram
-rw-r--r-s 1 root root 4896 Jan 1 00:00 anotherfile

- A. myfile
- B. anotherfile
- C. myprogram
- D. All of the above

Antwort: A

Begründung:
In Linux, the SGID (Set Group ID) bit alters execution or directory behavior:
On executables: Runs with the group owner's permissions (e.g., s in group execute position).
On directories: New files inherit the directory's group ownership.
Notation: s in group execute field (e.g., -rwxr-sr-x), or S if no execute (e.g., -rwxr-Sr-x).
Analysis:
-rwxr-sr-x (myfile): User: rwx, Group: r-s (SGID), Others: r-x. The s in group execute confirms SGID.
-rwsr-xr-x (myprogram): User: rws (SUID), Group: r-x, Others: r-x. The s is in user execute, not group-no SGID.
-rw-r--r-s (anotherfile): User: rw-, Group: r--, Others: r-s. The s is in others execute, but no x exists, rendering it meaningless (not SGID; could be a typo or sticky bit misapplied).
Security Implications: SGID executables (e.g., /usr/bin/wall) or directories (e.g., /var/local) manage group access. Misuse risks privilege escalation. CNSP likely teaches auditing with find / -perm -g=s.
Why other options are incorrect:
B: SUID, not SGID.
C: No valid SGID; s in others is irrelevant without execute.
D: Only A has SGID.
Real-World Context: SGID on /var/mail ensures mail files inherit the mail group.

25. Frage
Which built-in Windows utility can be used to verify the validity of a Kerberos ticket?

- A. Kerberos Manager
- B. Kerbtray
- C. Netsh
- D. Klist

Antwort: D

Begründung:
Kerberos is the default authentication protocol in Windows Active Directory environments, and tickets are used to prove identity. Verifying ticket validity involves checking their status, expiration, and attributes, which requires a built-in tool available in modern Windows systems.
Why A is correct: Klist is a command-line utility included in Windows (since Vista/2008) that lists cached Kerberos tickets and their details, such as validity period and renewal status. CNSP recognizes it as the standard tool for Kerberos ticket management in security audits.
Why other options are incorrect:
B: Kerbtray is a graphical tool from the Windows Resource Kit, not a built-in utility, and is outdated.
C: Netsh manages network configurations, not Kerberos tickets.
D: "Kerberos Manager" is not a recognized built-in Windows utility; it's a fictitious name.

26. Frage
WannaCry, an attack, spread throughout the world in May 2017 using machines running on outdated Microsoft operating systems. What is WannaCry?

- A. Ransomware
- B. Malware

Antwort: A

Begründung:
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.

27. Frage
.....

Die The SecOps Group CNSP (Certified Network Security Practitioner)Schulungsunterlagen von It-Pruefung sind den echten Prüfungen ähnlich. Durch die kurze Sonderausbildung können Sie schnell die Fachkenntnisse beherrschen und sich gut auf die The SecOps Group CNSP (Certified Network Security Practitioner)Prüfung vorbereiten. Wir versprechen, dass wir alles tun würden, um Ihnen beim Bestehen der The SecOps Group CNSP Zertifizierungsprüfung helfen.