The SecOps Group CNSP Practice Test: Tips and Tricks from Pass4sures

P.S. Free 2025 The SecOps Group CNSP dumps are available on Google Drive shared by Pass4sures: https://drive.google.com/open?id=1v_oBgkQ6klQV57jwAkZsiWvGD1aUBpG8

We have a lot of regular customers for a long-term cooperation now since they have understood how useful and effective our CNSP actual exam is. In order to let you have a general idea about the shining points of our CNSP training materials, we provide the free demos on our website for you to free download. You can check the information and test the functions by the three kinds of the free demos according to our three versions of the CNSP Exam Questions.

The SecOps Group CNSP Exam Syllabus Topics:

Topic	Details
Topic 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.
Topic 2	• 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 3	• 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 4	• 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 5	• Testing Network Services
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	• 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 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	• 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.

Exam CNSP Labs - CNSP Accurate Prep Material

Choosing our CNSP real dumps as your study guide means you choose a smart and fast way to get succeed in the certification exam. There are accurate CNSP test answers and some explanations along with the exam questions that will boost your confidence to solve the difficulty of CNSP Practice Test. You will enjoy great benefits if you buy our CNSP braindumps now and free update your study materials one-year.

The SecOps Group Certified Network Security Practitioner Sample Questions (Q51-Q56):

NEW QUESTION # 51
What is the response from an open UDP port which is not behind a firewall?

- A. A SYN packet
- B. A FIN packet
- C. No response
- D. ICMP message showing Port Unreachable

Answer: C

Explanation:
UDP's connectionless nature means it lacks inherent acknowledgment mechanisms, affecting its port response behavior.
Why B is correct: An open UDP port does not respond unless an application explicitly sends a reply. Without a firewall or application response, the sender receives no feedback, per CNSP scanning guidelines.
Why other options are incorrect:
A: ICMP Port Unreachable indicates a closed port, not an open one.
C: SYN packets are TCP-specific, not UDP.
D: FIN packets are also TCP-specific.

NEW QUESTION # 52
Which of the following algorithms could be used to negotiate a shared encryption key?

- A. AES
- B. SHA1
- C. Diffie-Hellman
- D. Triple-DES

Answer: C

Explanation:
Negotiating a shared encryption key involves a process where two parties agree on a secret key over an insecure channel without directly transmitting it. This is distinct from encryption or hashing algorithms, which serve different purposes.
Why C is correct: The Diffie-Hellman (DH) algorithm is a key exchange protocol that enables two parties to establish a shared secret key using mathematical operations (e.g., modular exponentiation). It's widely used in protocols like TLS and IPsec, as noted in CNSP for secure key negotiation.
Why other options are incorrect:
A: Triple-DES is a symmetric encryption algorithm for data encryption, not key negotiation.
B: SHA1 is a hash function for integrity, not key exchange.
D: AES is a symmetric encryption algorithm, not a key exchange mechanism.

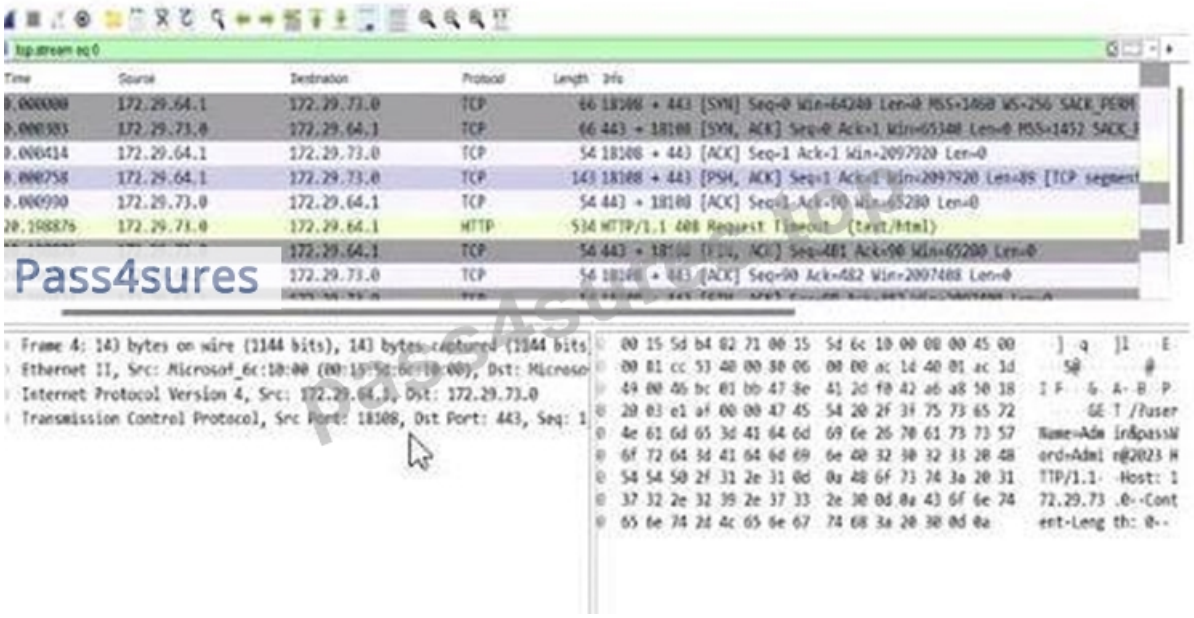
NEW QUESTION # 53
Which of the following services do not encrypt its traffic by default?

- A. FTPS
- B. DNS
- C. SSH
- D. All of these

Answer: B

Explanation:
Encryption ensures confidentiality and integrity of network traffic. Analyzing defaults:
A . DNS (Domain Name System):
Default: Unencrypted (UDP/TCP 53), per RFC 1035. Queries/responses (e.g., "google.com → 142.250.190.14") are plaintext.
Modern Options: DNS over HTTPS (DoH, TCP 443) or DNS over TLS (DoT, TCP 853) encrypt, but aren't default in most systems (e.g., pre-2020 Windows).
B . SSH (Secure Shell):
Default: Encrypted (TCP 22), per RFC 4251. Uses asymmetric (e.g., RSA) and symmetric (e.g., AES) crypto for all sessions.
C . FTPS (FTP Secure):
Default: Encrypted (TCP 21 control, dynamic data ports). Extends FTP with SSL/TLS (e.g., RFC 4217), securing file transfers.
Technical Details:
DNS: Plaintext exposes queries to eavesdropping (e.g., ISP snooping) or spoofing (e.g., cache poisoning).
SSH/FTPS: Encryption is baked into their standards; disabling it requires explicit misconfiguration.
Security Implications: Unencrypted DNS risks privacy and integrity (e.g., Kaminsky attack). CNSP likely pushes DoH/DoT adoption.
Why other options are incorrect:
B, C: Encrypt by default.
D: False, as only DNS lacks default encryption.
Real-World Context: The 2013 Snowden leaks exposed DNS monitoring; DoH uptake (e.g., Cloudflare 1.1.1.1) counters this.

NEW QUESTION # 54
According to the screenshot below, which of the following statements are correct?



- A. The application is running on port 80 and the HTTP protocol.
- B. The credentials have been submitted over the HTTP protocol.
- C. The application is running on port 443 and the HTTPS protocol.
- D. The credentials have been submitted over the HTTPS protocol.

Answer: C

Explanation:
The screenshot is from Wireshark, a network protocol analyzer, displaying captured network traffic. The relevant columns include the source and destination IP addresses, ports, protocol, and additional information about the packets. Let's break down the details:
Destination Port Analysis: The screenshot shows multiple packets with a destination port of 443 (e.g., in the "Destination" column, entries like "172.72.61.9:443"). Port 443 is the default port for HTTPS (HTTP Secure), which is HTTP traffic encrypted using SSL/TLS. This indicates that the application is communicating over HTTPS.
Protocol Analysis: The "Protocol" column lists "TLSv1.2" for most packets (e.g., frame numbers 2000084, 2000086). TLS (Transport Layer Security) is the cryptographic protocol used by HTTPS to secure HTTP communications. This confirms that the traffic is HTTPS, not plain HTTP.
Packet Details: The "Info" column provides additional context, such as "Application Data" for TLS packets, indicating encrypted application-layer data (typical of HTTPS). There are also HTTP packets (e.g., frame 2000088), but these are likely part of the HTTPS session (e.g., HTTP/2 over TLS, as noted by "HTTP2").
Now, let's evaluate the options:
Option A: "The application is running on port 443 and the HTTPS protocol." This is correct. The destination port 443 and the use of TLSv1.2 confirm that the application is using HTTPS. HTTPS is the standard protocol for secure web communication, and port 443 is its designated port. CNSP documentation emphasizes that HTTPS traffic on port 443 indicates a secure application-layer protocol, often used for web applications handling sensitive data.
Option B: "The credentials have been submitted over the HTTP protocol." This is incorrect. HTTP typically uses port 80, but the screenshot shows traffic on port 443 with TLS, indicating HTTPS. Credentials submitted over this connection would be encrypted via HTTPS, not sent in plaintext over HTTP. CNSP highlights the security risks of HTTP for credential submission due to lack of encryption, which isn't the case here.
Option C: "The credentials have been submitted over the HTTPS protocol." While this statement could be true (since HTTPS is in use, any credentials would likely be submitted securely), the question asks for the "correct" statement based on the screenshot. The screenshot doesn't explicitly show credential submission (e.g., a POST request with form data); it only shows the protocol and port. Option A is more directly supported by the screenshot as it focuses on the application's protocol and port, not the specific action of credential submission. CNSP notes that HTTPS ensures confidentiality, but this option requires more specific evidence of credentials.
Option D: "The application is running on port 80 and the HTTP protocol." This is incorrect. Port 80 is the default for HTTP, but the screenshot clearly shows port 443 and TLS, indicating HTTPS. CNSP documentation contrasts HTTP (port 80, unencrypted) with HTTPS (port 443, encrypted), making this option invalid.
Conclusion: Option A is the most accurate and comprehensive statement directly supported by the screenshot, confirming the application's use of port 443 and HTTPS. While Option C might be true in a broader context, it's less definitive without explicit evidence of credential submission in the captured packets.

NEW QUESTION # 55
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 # 56
.....

- CNSP Exam Pattern □ Test CNSP Sample Questions □ CNSP Exam Answers □ Easily obtain free download of ➤ CNSP □ by searching on ☀ www.prep4pass.com □☀□ □CNSP Valid Exam Labs
- www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, tinnitusheal.com, www.stes.tyc.edu.tw, thesmartcoders.tech, www.stes.tyc.edu.tw, Disposable vapes

2025 Latest Pass4sures CNSP PDF Dumps and CNSP Exam Engine Free Share: https://drive.google.com/open?id=1v_oBgkQ6klQV57jwAkZsiWvGD1aUBpG8