Latest The SecOps Group CNSP Exam Registration - CNSP Reliable Test Camp

BTW, DOWNLOAD part of Exam4Docs CNSP dumps from Cloud Storage: https://drive.google.com/open?id=1RvyVaVvgvXR025FysUtbzKl1c9BcI5bw

Because our CNSP actual exam help exam cannonades pass the exam with rate up to 98 to 100 percent. It encourages us to focus more on the quality and usefulness of our CNSP exam questions in the future. And at the same time, we offer free demos before you really choose our three versions of CNSP Practice Guide. Time is flying, hope you can begin your review on our CNSP study engine as quickly as possible.

Our CNSP exam dumps are compiled by our veteran professionals who have been doing research in this field for years. There is no question to doubt that no body can know better than them. The content and displays of the CNSP pass guide Which they have tailor-designed are absolutely more superior than the other providers'. Besides, they update our CNSP Real Exam every day to make sure that our customer can receive the latest CNSP preparation brain dumps.

>> Latest The SecOps Group CNSP Exam Registration <<

The SecOps Group CNSP Reliable Test Camp | Examcollection CNSP Dumps

After the user has purchased our CNSP learning materials, we will discover in the course of use that our product design is extremely scientific and reasonable. Details determine success or failure, so our every detail is strictly controlled. For example, our learning material's Windows Software page is clearly, our CNSP Learning material interface is simple and beautiful. There are no additional ads to disturb the user to use the Certified Network Security Practitioner qualification question. Once you have submitted your practice time, CNSP study tool system will automatically complete your operation.

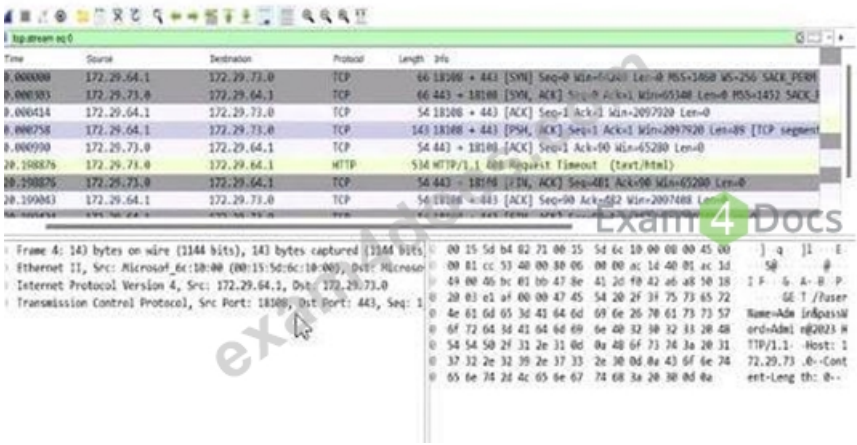
The SecOps Group CNSP Exam Syllabus Topics:

Topic	Details

Topic 1	• 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 2	• 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 3	• 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 4	• Testing Network Services
Topic 5	• 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 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.
Topic 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.
Topic 8	• Network Security Tools and Frameworks (such as Nmap, Wireshark, etc)
Topic 9	• 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 10	• 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 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.

The SecOps Group Certified Network Security Practitioner Sample Questions (Q35-Q40):

NEW QUESTION # 35
According to the screenshot below, which of the following statements are correct?



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

Answer: A

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 # 36
If a hash begins with $2a$, what hashing algorithm has been used?

- A. Blowfish

- B. SHA256
- C. MD5
- D. SHA512

Answer: A

Explanation:
The prefix $2a$ identifies the bcrypt hashing algorithm, which is based on the Blowfish symmetric encryption cipher (developed by Bruce Schneier). Bcrypt is purpose-built for password hashing, incorporating:
Salt: A random string (e.g., 22 Base64 characters) to thwart rainbow table attacks.
Work Factor: A cost parameter (e.g., $2a$10$ means 2