

# CS0-002<sup>Q&As</sup>

CompTIA Cybersecurity Analyst (CySA+)

## Pass CompTIA CS0-002 Exam with 100% Guarantee

Free Download Real Questions & Answers PDF and VCE file from:

https://www.pass2lead.com/cs0-002.html

100% Passing Guarantee 100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA
Official Exam Center

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers



#### https://www.pass2lead.com/cs0-002.html

2024 Latest pass2lead CS0-002 PDF and VCE dumps Download

#### **QUESTION 1**

An analyst has noticed unusual activities in the SIEM to a .cn domain name. Which of the following should the analyst use to identify the content of the traffic?

- A. Log review
- B. Service discovery
- C. Packet capture
- D. DNS harvesting

Correct Answer: C

#### **QUESTION 2**

The director of software development is concerned with recent web application security incidents, including the successful breach of a back-end database server. The director would like to work with the security team to implement a standardized way to design, build, and test web applications and the services that support them. Which of the following meets the criteria?

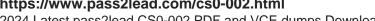
- A. OWASP
- B. SANS
- C. PHP
- D. Ajax

Correct Answer: A

Reference: https://www.synopsys.com/software-integrity/resources/knowledge-database/owasp-top-10.html

### **QUESTION 3**

An organization is conducting penetration testing to identify possible network vulnerabilities. The penetration tester has received the following output from the latest scan:



Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT

Nmap scan report for 192.168.1.13

Host is up (0.00066s latency).

Not shown: 996 closed ports

STATE PORT SERVICE 22/tcp open ssh 80/tcp open http

139/tcp netbios-ssn open 1417/tcp open timbuktu-srv1

MAC Address:01:AA:FB:23:21:45

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds

The penetration tester knows the organization does not use Timbuktu servers and wants to have Nmap interrogate the ports on the target in more detail. Which of the following commands should the penetration tester use NEXT?

A. nmap V 192.168.1.13 1417

B. nmap S 192.168.1.13 1417

C. sudo nmap S 192.168.1.13

D. nmap 192.168.1.13

Correct Answer: A

#### **QUESTION 4**

During the security assessment of a new application, a tester attempts to log in to the application but receives the following message incorrect password for given username. Which of the following can the tester recommend to decrease the likelihood that a malicious attacker will receive helpful information?

- A. Set the web page to redirect to an application support page when a bad password is entered.
- B. Disable error messaging for authentication
- C. Recognize that error messaging does not provide confirmation of the correct element of authentication
- D. Avoid using password-based authentication for the application

Correct Answer: B

#### **QUESTION 5**

An analyst was investigating the attack that took place on the network. A user was able to access the system without proper authentication. Which of the following will the analyst recommend, related to management approaches, in order



https://www.pass2lead.com/cs0-002.html 2024 Latest pass2lead CS0-002 PDF and VCE dumps Download

to control access? (Choose three.)
A. RBAC
B. LEAP
C. DAC
D. PEAP
E. MAC
F. SCAP
G. BCP
Correct Answer: ACE

Latest CS0-002 Dumps

CS0-002 PDF Dumps

CS0-002 Study Guide