CS0-002$^{Q\&As}$

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

QUESTION 1

Joe, an analyst, has received notice that a vendor who is coming in for a presentation will require access to a server outside the network. Currently, users are only able to access remote sites through a VPN connection. Which of the following should Joe use to BEST accommodate the vendor?

A. Allow incoming IPSec traffic into the vendor\\'s IP address.

B. Set up a VPN account for the vendor, allowing access to the remote site.

C. Turn off the firewall while the vendor is in the office, allowing access to the remote site.

D. Write a firewall rule to allow the vendor to have access to the remote site.

Correct Answer: B

QUESTION 2

Which of the following is MOST important when developing a threat hunting program?

A. Understanding penetration testing techniques

B. Understanding how to build correlation rules within a SIEM

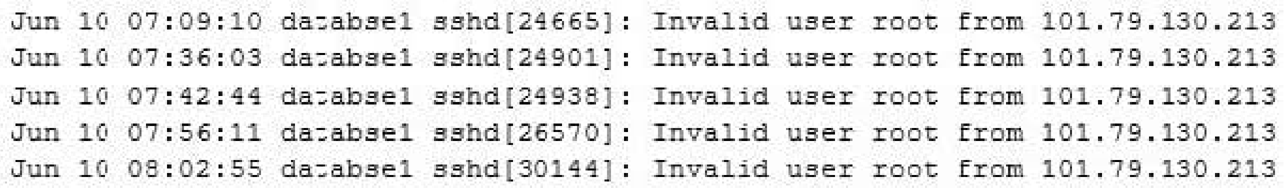
C. Understanding security software technologies

D. Understanding assets and categories of assets

Correct Answer: D

QUESTION 3

An analyst is conducting a log review and identifies the following snippet in one of the logs:



```
Jun 10 07:09:10 databse1 sshd[24665]: Invalid user root from 101.79.130.213
Jun 10 07:36:03 databse1 sshd[24901]: Invalid user root from 101.79.130.213
Jun 10 07:42:44 databse1 sshd[24938]: Invalid user root from 101.79.130.213
Jun 10 07:56:11 databse1 sshd[26570]: Invalid user root from 101.79.130.213
Jun 10 08:02:55 databse1 sshd[30144]: Invalid user root from 101.79.130.213
```

Which of the following MOST likely caused this activity?

A. SQL injection

B. Privilege escalation

C. Forgotten password

D. Brute force

Correct Answer: D

QUESTION 4

Which of the following ICS network protocols has no inherent security functions on TCP port 502?

A. CIP

B. DHCP

C. SSH

D. Modbus

Correct Answer: D

QUESTION 5

A development team signed a contract that requires access to an on-premises physical server. Access must be restricted to authorized users only and cannot be connected to the Internet. Which of the following solutions would meet this requirement?

A. Establish a hosted SSO.

B. Implement a CASB.

C. Virtualize the server.

D. Air gap the server.

Correct Answer: D