CS0-002 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.passapply.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

A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic. Which of the following would BEST accomplish this goal?

A. Continuous integration and deployment

B. Automation and orchestration

C. Static and dynamic analysis

D. Information sharing and analysis

Correct Answer: B

QUESTION 2

A cybersecurity analyst has received an alert that well-known "call home" messages are continuously observed by network sensors at the network boundary. The proxy firewall successfully drops the messages. After determining the alert was a true positive, which of the following represents the MOST likely cause?

A. Attackers are running reconnaissance on company resources.

B. An outside command and control system is attempting to reach an infected system.

C. An insider is trying to exfiltrate information to a remote network.

D. Malware is running on a company system.

Correct Answer: B

QUESTION 3

A web application has a newly discovered vulnerability in the authentication method used to validate known company users. The user ID of Admin with a password of "password" grants elevated access to the application over the Internet. Which of the following is the BEST method to discover the vulnerability before a production deployment?

A. Manual peer review

B. User acceptance testing

C. Input validation

D. Stress test the application

Correct Answer: C

QUESTION 4

A new policy requires the security team to perform web application and OS vulnerability scans. All of the company\\'s web applications use federated authentication and are accessible via a central portal. Which of the following should be implemented to ensure a more thorough scan of the company\\'s web application, while at the same time reducing false positives?

A. The vulnerability scanner should be configured to perform authenticated scans.

B. The vulnerability scanner should be installed on the web server.

C. The vulnerability scanner should implement OS and network service detection.

D. The vulnerability scanner should scan for known and unknown vulnerabilities.

Correct Answer: A

QUESTION 5

A security analyst is reviewing packet captures for a specific server that is suspected of containing malware and discovers the following packets:

```
138.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [SYN] Seq=0 Win=4128 Len=0 MSS=1460
73.252.34.101 138.23.45.201 TCP dns (53) -> 56712 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0
138.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [ACK] Seq=1 Ack=1 Win=4128 Len=0
73.252.34.101 138.23.45.201 SSH Server: Protocol (SSH-2.0-Cisco-1.25)
138.23.45.201 73.252.34.101 SSH Client: Protocol (SSH-1.99-Cisco-1.25)
73.252.34.101 138.23.45.201 SSHv2 Server: Key Exchange Init
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [SYN] Seq=0 Win=65535 Len=0
73.252.34.101 103.34.243.12 TCP ftp (21) -> 62014 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [ACK] Seq=1 Ack=1 Win=65535 Len=0
73.252.34.101 103.34.243.12 FTP Response: 220 ProFTPD 1.3.0a Server
103.34.243.12 73.252.34.101 FTP Request: User FTP
73.252.34.101 103.34.243.12 FTP Response: 331 Anonymous login ok, send your complete email address
as your password.
103.34.243.12 73.252.34.101 FTP Request: Pass ftp
73.252.34.101 103.34.243.12 FTP Response: 230 Anonymous access granted, restrictions apply,
202.53.245.78 73.252.34.101 TCP 57678 -> 8080[SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=
835172936 TSecr=2216538 WS=64
73.252.34.101 202.53.245.78 TCP 8080 -> 57678[SYN, ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=2216543
TSecr=835172936
202.53.245.78 73.252.34.101 HTTP GET /images/layout/logo.png HTTP/1.0
202.53.245.78 73.252.34.101 TCP 57678 -> 8080[ACK] Seq=135 Ack=2897 Win=11648 Len=0 TSval=2216543
TSecr=835172936
```

Which of the following traffic patterns or data would be MOST concerning to the security analyst?

A. Port used for SMTP traffic from 73.252.34.101

B. Unencrypted password sent from 103.34.243.12

C. Anonymous access granted by 103.34.243.12

D. Ports used for HTTP traffic from 202.53.245.78

Correct Answer: C