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

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

QUESTION 1

When reviewing network traffic, a security analyst detects suspicious activity:

```
110 172.150.200.129 TCP    1140 > 443 [SYN] Seq=0 Win=15901 Len=0 MSS=1460 SACK_PERM=1
111 172.150.200.129 TCP    1140 > 443 [ACK] Seq=1 ACK=1 Win=15091 Len=0
112 172.150.200.129 SSLv2  Client Hello
113 172.150.200.129 TCP    [TCP Dup ACK 112#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
114 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
115 172.150.200.129 TCP    [TCP Dup ACK 114#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
120 172.150.200.129 TCP    [TCP Dup ACK 114#2] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
122 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
```

Based on the log above, which of the following vulnerability attacks is occurring?

A. ShellShock

B. DROWN

C. Zeus

D. Heartbleed

E. POODLE

Correct Answer: E

QUESTION 2

A recent audit included a vulnerability scan that found critical patches released 60 days prior were not applied to servers in the environment. The infrastructure team was able to isolate the issue and determined it was due to a service being disabled on the server running the automated patch management application. Which of the following would be the MOST efficient way to avoid similar audit findings in the future?

A. Implement a manual patch management application package to regain greater control over the process.

B. Create a patch management policy that requires all servers to be patched within 30 days of patch release.

C. Implement service monitoring to validate that tools are functioning properly.

D. Set services on the patch management server to automatically run on start-up.

Correct Answer: D

QUESTION 3

In system hardening, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

A. SCAP

B. Burp Suite

C. OWASP ZAP

D. Unauthenticated

Correct Answer: D

QUESTION 4

A Chief Executive Officer (CEO) is concerned the company will be exposed lo data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?

A. Data masking procedures

B. Enhanced encryption functions

C. Regular business impact analysis functions

D. Geographic access requirements

Correct Answer: D

Data Sovereignty means that data is subject to the laws and regulations of the geographic location where that data is collected and processed. Data sovereignty is a country-specific requirement that data must remain within the borders of the jurisdiction where it originated. At its core, data sovereignty is about protecting sensitive, private data and ensuring it remains under the control of its owner. You\\'re only worried about that if you\\'re in multiple locations. . https://www.virtru.com/ blog/gdpr-data-sovereignty-matters- globally

QUESTION 5

A security analyst is reviewing existing email protection mechanisms to generate a report. The analysis finds the following DNS records:

Record 1 v=spf1 ip4:192:168.0.0/16 include:_spf.marketing.com include: thirdpartyprovider.com ~all Record 2

“v=DKIM1\ k=rsa\;
p=MIGfMA0GCSqh7d8hyh78Gdg87gd98hag86ga98dhay8gd7ashdca7yg79auhudig7df9ah8g76ag98dhay87ga9”

Record 3 _dmarc.comptia.com TXT v=DMARC1\; p=reject\; pct=100; rua=mailto:dmarc-reports@comptia.com Which of the following options provides accurate information to be included in the report?

A. Record 3 serves as a reference of the security features configured at Record 1 and 2.

B. Record 1 is used as a blocklist mechanism to filter unauthorized senders.

C. Record 2 is used as a key to encrypt all outbound messages sent.

D. The three records contain private information that should not be disclosed.

Correct Answer: A

The DMARC record is what tells us to do with messages that don\\'t properly align to SPF / DKIM. WRONG ANSWERS

- B – this SPF record, as configured, is a softfail. That means it functions as less of a blocklist and more as a quarantine list.
- C – the DKIM key is used to sign, not encrypt, outbound messages.
- D – all 3 records must be in public DNS or e-mail servers outside the organization would be unable to reference them and use them.