350-201^{Q&As}

350-201^{Q&As}

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

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

https://www.passapply.com/350-201.html
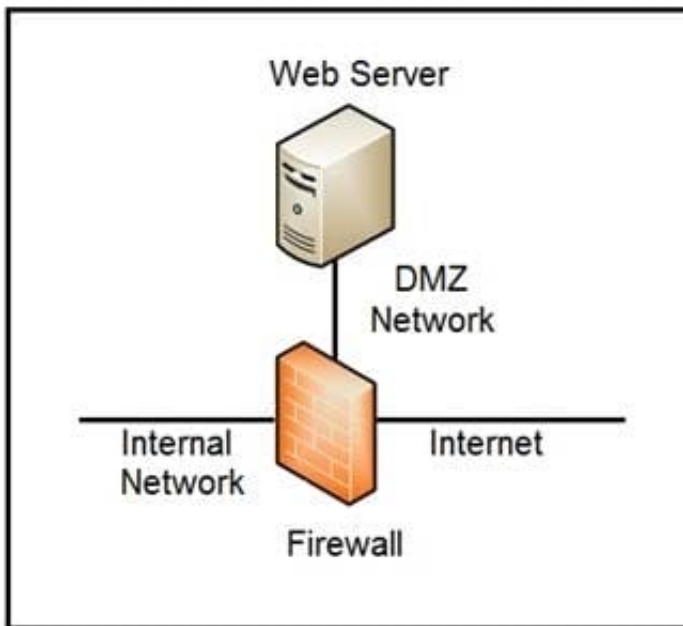
100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit. Which two steps mitigate attacks on the webserver from the Internet? (Choose two.)

A. Create an ACL on the firewall to allow only TLS 1.3

B. Implement a proxy server in the DMZ network

C. Create an ACL on the firewall to allow only external connections

D. Move the webserver to the internal network

Correct Answer: BD

QUESTION 2

What is a principle of Infrastructure as Code?

A. System maintenance is delegated to software systems

B. Comprehensive initial designs support robust systems

C. Scripts and manual configurations work together to ensure repeatable routines

D. System downtime is grouped and scheduled across the infrastructure

Correct Answer: B

QUESTION 3

According to GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?

A. Perform a vulnerability assessment

B. Conduct a data protection impact assessment

C. Conduct penetration testing

D. Perform awareness testing

Correct Answer: B

Reference: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/DPIA-Guide.pdf

QUESTION 4

The SIEM tool informs a SOC team of a suspicious file. The team initializes the analysis with an automated sandbox tool, sets up a controlled laboratory to examine the malware specimen, and proceeds with behavioral analysis. What is the next step in the malware analysis process?

A. Perform static and dynamic code analysis of the specimen.

B. Unpack the specimen and perform memory forensics.

C. Contain the subnet in which the suspicious file was found.

D. Document findings and clean-up the laboratory.

Correct Answer: B

QUESTION 5

A logistic company must use an outdated application located in a private VLAN during the migration to new technologies. The IPS blocked and reported an unencrypted communication. Which tuning option should be applied to IPS?

A. Allow list only authorized hosts to contact the application\\'s IP at a specific port.

B. Allow list HTTP traffic through the corporate VLANS.

C. Allow list traffic to application\\'s IP from the internal network at a specific port.

D. Allow list only authorized hosts to contact the application\\'s VLAN.

Correct Answer: D