



SY0-501^{Q&As}

CompTIA Security+ Certification Exam

Pass CompTIA SY0-501 Exam with 100% Guarantee

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

<https://www.geekcert.com/sy0-501.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

Which of the following describes the maximum amount of time a mission essential function can operate without the systems it depends on before significantly impacting the organization?

- A. MTBF
- B. MTTR
- C. RTO
- D. RPO

Correct Answer: C

QUESTION 2

A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use.

Which of the following should the engineer do to determine the issue? (Select Two)

- A. Perform a site survey.
- B. Deploy an FTK Imager.
- C. Create a heat map.
- D. Scan for rogue access points.
- E. Upgrade the security protocols.
- F. Install a captive portal

Correct Answer: AD

QUESTION 3

Joe notices there are several user accounts on the local network generating spam with embedded malicious code. Which of the following technical control should Joe put in place to BEST reduce these incidents?

- A. Account lockout
- B. Group Based Privileges
- C. Least privilege
- D. Password complexity

Correct Answer: A



QUESTION 4

Which of the following BEST describes the purpose of authorization?

- A. Authorization provides logging to a resource and comes after authentication.
- B. Authorization provides authentication to a resource and comes after identification.
- C. Authorization provides identification to a resource and comes after authentication.
- D. Authorization provides permissions to a resource and comes after authentication.

Correct Answer: D

QUESTION 5

A security analyst investigate a report from an employee in the human resources (HR) department who is issues with Internal access. When the security analyst pull the UTM logs for the IP addresses in the HR group, the following activity is shown:

Host	Destination	Port	Category	User Group	Action
10.1.13.45	165.35.23.129	8080	News/Journalism	General	Block
10.1.13.45	89.23.45.11	443	Banking	General	Allow
10.1.13.46	76.4.3.19	8080	Business	HR Users	Allow
10.1.13.45	145.29.173	8080	Business	General	Block
10.1.13.45	10.1.1.29	443	Internal	General	Allow
10.1.13.46	19.34.1.189	443	Banking	HR Users	Allow
10.1.13.45	45.1.39.118	8080	Job Search	General	Block
10.1.13.46	45.1.39.118	8080	Job Search	HR Users	Allow

Which of the following actions should the security analyst take?

- A. Ensure the HR employee is in the appropriate user group
- B. Allow port 8080 on the UTM for all outgoing traffic
- C. Disable the proxy settings on the HR employee's device.
- D. Edit the last line Of the ACL On the UTM lo: allow any any.

Correct Answer: A