# SY0-601 Q&As

CompTIA Security+

## Pass CompTIA SY0-601 Exam with 100% Guarantee

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

**QUESTION 1**

The security team installed video cameras in a prominent location in the building lobby. Which of the following best describe this type of control? (Choose two.)

A. Technical

B. Detective

C. Deterrent

D. Managerial

E. Compensating

F. Corrective

Correct Answer: BC

**QUESTION 2**

A company\\'s public-facing website, https://www.organization.com, has an IP address of 166.18.75.6. However, over the past hour the SOC has received reports of the site\\'s homepage displaying incorrect information. A quick nslookup search shows https://;www.organization.com is pointing to 151.191.122.115.

Which of the following is occurring?

A. DoS attack

B. ARP poisoning

C. DNS spoofing

D. NXDOMAIN attack

Correct Answer: C

Domain Name Server (DNS) spoofing, or DNS cache poisoning, is an attack involving manipulating DNS records to redirect users toward a fraudulent, malicious website that may resemble the user\\'s intended destination.

**QUESTION 3**

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

A. Insurance

B. Patching

C. Segmentation

D. Replacement

Correct Answer: C

If support from the manufacturer is not available, and the vulnerability is in the OS of legacy IoT devices, the best option to quickly mitigate the vulnerability is C. Segmentation. Since patching may not be feasible without manufacturer support, segmentation can help isolate the vulnerable devices from the rest of the network. This can limit the potential attack surface and reduce the risk of exploitation, even if the devices themselves cannot be patched or updated. Segmentation can be an effective short-term strategy to enhance security when dealing with unsupported legacy IoT devices.If support from the manufacturer is not available, and the vulnerability is in the OS of legacy IoT devices, the best option to quickly mitigate the vulnerability is C. Segmentation.

Since patching may not be feasible without manufacturer support, segmentation can help isolate the vulnerable devices from the rest of the network. This can limit the potential attack surface and reduce the risk of exploitation, even if the devices themselves cannot be patched or updated.

**QUESTION 4**

A company is currently utilizing usernames and passwords, and it wants to integrate an MFA method that is seamless, can integrate easily into a user\\'s workflow, and can utilize employee-owned devices. Which of the following will meet these requirements?

A. Push notifications

B. Phone call

C. Smart card

D. Offline backup codes

Correct Answer: A

**QUESTION 5**

A security analyst receives an alert from trie company\\'s SIEM that anomalous activity is coming from a local source IP address of 192.168.34.26. The Chief Information Security Officer asks the analyst to block the originating source Several days later, another employee opens an internal ticket stating that vulnerability scans are no longer being performed properly. The IP address the employee provides is 192 168.3426. Which of the following describes this type of alert?

A. True positive

B. True negative

C. False positive

D. False negative

Correct Answer: C

True Positive: A legitimate attack which triggers to produce an alarm. You have a brute force alert, and it triggers. You investigate the alert and find out that somebody was indeed trying to break into one of your systems via brute force methods.

False Positive: An event signalling to produce an alarm when no attack has taken place. You investigate another of these brute force alerts and find out that it was just some user who mistyped their password a bunch of times, not a real

attack.

False Negative: When no alarm is raised when an attack has taken place. Someone was trying to break into your system, but they did so below the threshold of your brute force attack logic. For example, you set your rule to look for ten failed

login in a minute, and the attacker did only 9. The attack occurred, but your control was unable to detect it.

True Negative: An event when no attack has taken place and no detection is made. No attack occurred, and your rule didn\\'t make fire.

SY0-601 PDF Dumps SY0-601 VCE Dumps SY0-601 Braindumps