SY0-601 Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.leads4pass.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company\\'s final software releases? (Select TWO.)

A. Unsecure protocols

B. Use of penetration-testing utilities

C. Weak passwords

D. Included third-party libraries

E. Vendors/supply chain

F. Outdated anti-malware software

Correct Answer: DE

A. Unsecure protocols

--> Could be correct. This is a vector that could be used shortly before the final release to somehow include malicious code.

B. Use of penetration-testing utilities

--> Makes no sense

C. Weak passwords

--> Is an attack vector and "unauthorized" could match that. Might be correct.

D. Included third-party libraries

--> unintentional would fit. But if there was something wrong with a 3rd party libary, that should have been discovered before the final release.

E. Vendors/supply chain

--> Depends on what these vendors do. If they are developing code that is used in the final release it could contain vulnerabilities that are included unintentionally. But that would be kind of similar to the 3rd party libraries.

F. Outdated anti-malware software

--> With outdated anti-malware, and attacker could gain acces to a developers machine and include vulnerable code. The developer could then commit it unintentionally.

QUESTION 2

Which of the following would BEST provide detective and corrective controls for thermal regulation?

A. A smoke detector

B. A fire alarm

C. An HVAC system

D. A fire suppression system

E. Guards

Correct Answer: C

What are the functions of an HVAC system?

An HVAC system is designed to control the environment in which it works. It achieves this by controlling the temperature (THERMAL) of a room through heating and cooling. It also controls the humidity level in that environment by controlling the movement and distribution of air inside the room. So it provides detective and corrective controls for THERMAL regulation.

QUESTION 3

A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.

Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads.

Which of the following BEST describe this type of attack? (Choose two.)

A. DoS

B. SSL stripping

C. Memory leak

D. Race condition

E. Shimming

F. Refactoring

Correct Answer: AC

A DoS attack is a type of cyber attack that is designed to disrupt the availability of a network, system, or service. In this case, the attacker is using the exploit outlined in the CVE to disrupt the availability of Internet and VoIP services at the university\\'s remote campuses.

A Memory Leak is a type of software bug that occurs when a program or application allocates memory for a task, but fails to release the memory when it is no longer needed. This can lead to a depletion of available memory resources, causing the system to crash or become unstable. The fact that the outages at the university are occurring at random intervals and are being caused by system reloads suggests that a Memory Leak may be present.

QUESTION 4

A large retail store\\'s network was breached recently, and this news was made public. The store did not lose any intellectual property, and no customer information was stolen. Although no fines were incurred as a result, the store lost revenue after the breach. Which of the following is the most likely reason for this issue?

A. Employee training

B. Leadership changes

C. Reputation damage

D. Identity theft

Correct Answer: C

Even though no intellectual property or customer information was stolen, the fact that the breach became public knowledge could have significantly damaged the store\\'s reputation. Customers may lose trust in the store\\'s ability to protect their data and personal information, leading to a decline in sales and customer loyalty. A damaged reputation can result in negative publicity, reduced customer confidence, and a decrease in the store\\'s overall market value, all of which can impact the company\\'s revenue and profitability.

QUESTION 5

The Chief Information Security Officer (CISO) has requested that a third-party vendor provide supporting documents that show proper controls are in place to protect customer data. Which of the following would be BEST for the third-party vendor to provide to the CISO?

A. GDPR compliance attestation

B. Cloud Security Alliance materials

C. SOC 2 Type 2 report

D. NIST RMF workbooks

Correct Answer: C

GDPR related to EU nothing in question to say they are in EU. SOC type 2 : tests security controls in place https://www.itgovernance.co.uk/soc-reporting