SY0-601 Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

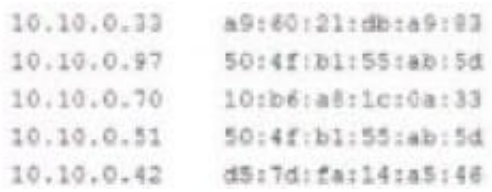
https://www.leads4pass.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A penetration tester successfully gained access to a company\\'s network The investigating analyst determines malicious traffic connected through the WAP despite filtering rules being in place. Logging in to the connected switch, the analyst sees the following m the ARP table:



Which of the following cid the penetration tester MOST liely use?

A. ARP poisoning

B. MAC cloning

C. Man in the middle

D. Evil twin

Correct Answer: C

QUESTION 2

A police department is using the cloud to share information city officials.

Which of the cloud models describes this scenario?

A. Hybrid

B. private

C. pubic

D. Community

Correct Answer: D

A community cloud model describes a scenario where a cloud service is shared among multiple organizations that have common goals, interests, or requirements. A community cloud can be hosted by one of the organizations, a third-party provider, or a combination of both. A community cloud can offer benefits such as cost savings, security, compliance, and collaboration. A police department using the cloud to share information with city officials is an example of a community cloud model.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.ibm.com/cloud/learn/community-cloud

QUESTION 3

Which of the following controls is used to make an organization initially aware of a data compromise?

A. Protective

B. Preventative

C. Corrective

D. Detective

Correct Answer: D

Detective control identifies security events that have already occurred. Intrusion detection systems are detective controls.

==========

Preventative Controls - acts to eliminate or reduce the likelihood that an attack can succeed. A preventative control operates before an attack can take place. They are comparing the configurations to a secure guideline to ensure no gaps.

Meaning they are pre-emptively hardening their systems against future attack vectors.

Corrective Controls - controls that remediate security issues that have already occurred. Restoring backups after a ransomware attack is an example of a corrective control.

https://purplesec.us/security-controls/

QUESTION 4

On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)

A. Data accessibility

B. Legal hold

C. Cryptographic or hash algorithm

D. Data retention legislation

E. Value and volatility of data

F. Right-to-audit clauses

Correct Answer: AE

directly from the link @AspiringScriptKiddie provided:

Note

Before conducting a live acquisition, data acquisition priorities should be identified in terms of data accessibility, as well as the value and volatility of the data.

QUESTION 5

A security analyst is investigating a vulnerability in which a default file permission was set incorrectly. The company uses non-credentialed scanning for vulnerability management.

Which of the following tools can the analyst use to verify the permissions?

A. ssh

B. chmod

C. ls

D. setuid

E. nessus

F. nc

Correct Answer: B

chmod is used to set permissions for the file.

If you use: ls -l