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.passapply.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 help desk technician receives a phone call from someone claiming to be a part of the organization\\'s cybersecurity modem response team The caller asks the technician to verify the network\\'s internal firewall IP address

Which of the following 15 the technician\\'s BEST course of action?

A. Direct the caller to stop by the help desk in person and hang up declining any further requests from the caller

B. Ask for the callers name, verify the persons identity in the email directory and provide the requested information over the phone

C. Write down the phone number of the carter if possible, the name of the person requesting the information hang up. and notify the organization\\'s cybersecurity officer

D. Request the caller send an email for identity verification and provide the requested information via email to the caller

Correct Answer: C

Write down the phone number of the caller if possible, the name of the person requesting the information, hang up, and notify the organization\\'s cybersecurity officer.

In this scenario, the help desk technician should be wary of the person\\'s request as help desk technicians would not have this information. Also, if the person claimed to be from the cybersecurity incident response team, they would more likely to have access to this information anyway, or at least know who to contact.

For the sake of the technician, it would be best to get as much information as possible and delegate the task of confirming the person\\'s identity to the cybersecurity officer. Even in the very slim chance that it was a legitimate request, it would still be best for the cyber security officer to provide this information instead of a tech.

QUESTION 2

All security analysts\\' workstations at a company have network access to a critical server VLAN. The information security manager wants to further enhance the controls by requiring that all access to the secure VLAN be authorized only from a given single location. Which of the following will the information security manager most likely implement?

A. A forward proxy server

B. A jump server

C. A reverse proxy server

D. A stateful firewall server

Correct Answer: B

A jump server, also known as a bastion host or a secure access server, is a dedicated server that serves as a single access point for administrators or authorized users to connect to other systems within a network. By requiring all access to the secure VLAN to go through the jump server, the information security manager can enforce a centralized and controlled access point. This ensures that all access to the secure VLAN is authorized and can be monitored or logged for security purposes. A jump server provides an additional layer of security and helps protect against unauthorized access.

QUESTION 3

Which of the following components can be used to consolidate and forward inbound Internet traffic to multiple cloud environments though a single firewall?

A. Transit gateway

B. Cloud hot site

C. Edge computing

D. DNS sinkhole

Correct Answer: A

VPC peering relationships can quickly become difficult to manage, especially if each VPC must interconnect in a mesh-like structure. A transit gateway is a simpler means of managing these interconnections. Essentially, a transit gateway is a virtual router that handles routing between the subnets in each attached VPC and any attached VPN gateways (aws.amazon.com/transit-gateway).

QUESTION 4

An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner\\'s account. Which of the following would be BEST to minimize this risk?

A. Require a complex, eight-character password that is updated every 90 days.

B. Perform only non-intrusive scans of workstations.

C. Use non-credentialed scans against high-risk servers.

D. Log and alert on unusual scanner account logon times.

Correct Answer: A

QUESTION 5

A security engi is cor that the gy tor on endpoints ts too heavily dependent on previously defined attacks. The engineer would like a tool to monitor for changes to key Mes and network traffic on the device. Which of the following tools BEST addresses both detection and prevention?

A. NIDS

B. HIPS

C. AV

D. NGFW

Correct Answer: B

A host-based intrusion detection and prevention system (HIPS) is a tool that monitors for changes to key files and network traffic on a device