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

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 2

Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities After further investigation, a security analyst notices the following

1.

All users share workstations throughout the day

2.

Endpoint protection was disabled on several workstations throughout the network.

3.

Travel times on logins from the affected users are impossible

4.

Sensitive data is being uploaded to external sites

5.

All usee account passwords were forced lo be reset and the issue continued

Which of the following attacks is being used to compromise the user accounts?

A. Brute-force

B. Keylogger

C. Dictionary

D. Rainbow

Correct Answer: B

Enduser protection is disabled and someone installed a keyloggers since workstations are being shared. Changing password doesn\\'t uninstall this keylogger which is likely recording the new changed passwords and sending them out to the attacker.

QUESTION 3

A retail company that is launching @ new website to showcase the company\\'s product line and other information for online shoppers registered the following URLs:

1.

www companysite com

2.

shop companysite com

3.

about-us companysite com

4.

contact-us. companysite com

5.

secure-logon companysite com

Which of the following should the company use to secure its website rf the company is concerned with convenience and cost?

A. A self-signed certificate

B. A root certificate

C. A code-signing certificate

D. A wildcard certificate

E. An extended validation certificate

Correct Answer: D

A wildcard certificate is a digital certificate that is applied to a domain and all its subdomains. Wildcard notation consists of an asterisk and a period before the domain name. Secure

QUESTION 4

During an incident, an EDR system detects an increase in the number of encrypted outbound connections from multiple hosts. A firewall is also reporting an increase in outbound connections that use random high ports. An analyst plans to review the correlated logs to find the source of the incident. Which of the following tools will best assist the analyst?

A. A vulnerability scanner

B. A NGFW

C. The Windows Event Viewer

D. A SIEM

Correct Answer: D

A SIEM is a centralized logging and monitoring solution that collects, analyzes, and correlates log data from various sources within an organization\\'s network and security infrastructure. It helps security analysts to gain visibility into security events and incidents by aggregating and correlating logs from multiple systems and devices.

In the scenario described, the EDR system and firewall are both generating logs that provide valuable information about the incident. By using a SIEM, the analyst can collect and correlate the logs from these different sources to get a comprehensive view of the incident. The SIEM will help the analyst identify patterns, anomalies, and potential indicators of compromise that may not be immediately apparent when reviewing individual logs in isolation.

QUESTION 5

A security analyst has received an alert about being sent via email. The analyst\\'s Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care From which of the following did the alert MOST likely originate?

A. S/MIME

B. DLP

C. IMAP

D. HIDS

Correct Answer: B

Network-based DLP monitors outgoing data looking for sensitive data. Network-based DLP systems monitor outgoing email to detect and block unauthorized data transfers and monitor data stored in the cloud.