CAS-001 Q&As

CompTIA Advanced Security Practitioner

Pass CompTIA CAS-001 Exam with 100% Guarantee

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

https://www.lead4pass.com/CAS-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The Chief Executive Officer (CEO) of a corporation decided to move all email to a cloud computing environment. The Chief Information Security Officer (CISO) was told to research the risk involved in this environment.

Which of the following measures should be implemented to minimize the risk of hosting email in the cloud?

A. Remind users that all emails with sensitive information need be encrypted and physically inspect the cloud computing.

B. Ensure logins are over an encrypted channel and obtain an NDA and an SLA from the cloud provider.

C. Ensure logins are over an encrypted channel and remind users to encrypt all emails that contain sensitive information.

D. Obtain an NDA from the cloud provider and remind users that all emails with sensitive information need be encrypted.

Correct Answer: B

QUESTION 2

The Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router\\'s external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company\\'s external router\\'s IP which is 128.20.176.19:

11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 1400 11:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 1400 11:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 1400 11:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 1400 11:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400

Which of the following describes the findings the senior security engineer should report to the ISO and the BEST solution for service restoration?

A. After the senior engineer used a network analyzer to identify an active Fraggle attack, the company\\'s ISP should be contacted and instructed to block the malicious packets.

B. After the senior engineer used the above IPS logs to detect the ongoing DDOS attack, an IPS filter should be enabled to block the attack and restore communication.

C. After the senior engineer used a mirror port to capture the ongoing amplification attack, a BGP sinkhole should be configured to drop traffic at the source networks.

D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company\\'s external router to block incoming UDP port 19 traffic.

Correct Answer: A

QUESTION 3

A security engineer at a bank has detected a Zeus variant, which relies on covert communication channels to receive new instructions and updates from the malware developers. As a result, NIPS and AV systems did not detect the configuration files received by staff in emails that appeared as normal files.

Which of the following BEST describes the technique used by the malware developers?

A. Perfect forward secrecy

B. Stenography

C. Diffusion

D. Confusion

E. Transport encryption

Correct Answer: B

QUESTION 4

Two storage administrators are discussing which SAN configurations will offer the MOST confidentiality. Which of the following configurations would the administrators use? (Select TWO).

A. Deduplication

B. Zoning

C. Snapshots

D. Multipathing

E. LUN masking

Correct Answer: BE

QUESTION 5

Company XYZ is building a new customer facing website which must access some corporate resources. The company already has an internal facing web server and a separate server supporting an extranet to which suppliers have access. The extranet web server is located in a network DMZ. The internal website is hosted on a laptop on the internal corporate network. The internal network does not restrict traffic between any internal hosts.

Which of the following locations will BEST secure both the intranet and the customer facing website?

A. The existing internal network segment

B. Dedicated DMZ network segments

C. The existing extranet network segment

D. A third-party web hosting company

Correct Answer: B