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

In order to reduce cost and improve employee satisfaction, a large corporation has decided to allow personal communication devices to access email and to remotely connect to the corporate network. Which of the following security measures should the IT organization implement? (Select TWO).

A. A device lockdown according to policies

B. An IDS on the internal networks

C. A data disclosure policy

D. A privacy policy

E. Encrypt data in transit for remote access

Correct Answer: AE

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 new company requirement mandates the implementation of multi-factor authentication to access network resources. The security administrator was asked to research and implement the most cost-effective solution that would allow for the authentication of both hardware and users. The company wants to leverage the PKI infrastructure which is already well established.

Which of the following solutions should the security administrator implement?

A. Issue individual private/public key pairs to each user, install the private key on the central authentication system, and protect the private key with the user\\'s credentials. Require each user to install the public key on their computer.

B. Deploy USB fingerprint scanners on all desktops, and enable the fingerprint scanner on all laptops. Require all network users to register their fingerprint using the reader and store the information in the central authentication system.

C. Issue each user one hardware token. Configure the token serial number in the user properties of the central authentication system for each user and require token authentication with PIN for network logon.

D. Issue individual private/public key pairs to each user, install the public key on the central authentication system, and require each user to install the private key on their computer and protect it with a password.

Correct Answer: D

QUESTION 4

A security manager is developing new policies and procedures. Which of the following is a best practice in end user security?

A. Employee identity badges and physical access controls to ensure only staff are allowed onsite.

B. A training program that is consistent, ongoing, and relevant.

C. Access controls to prevent end users from gaining access to confidential data.

D. Access controls for computer systems and networks with two-factor authentication.

Correct Answer: B

QUESTION 5

Which of the following refers to programs running in an isolated space to run untested code and prevents the code from making permanent changes to the OS kernel and other data on the host machine?

A. Input Validation

B. Application hardening

C. Code signing

D. Application sandboxing

Correct Answer: D