CAS-002^Q&As

CompTIA Advanced Security Practitioner Exam

QUESTION 1

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 2

Company XYZ has experienced a breach and has requested an internal investigation be conducted by the IT Department. Which of the following represents the correct order of the investigation process?

A. Collection, Identification, Preservation, Examination, Analysis, Presentation.

B. Identification, Preservation, Collection, Examination, Analysis, Presentation.

C. Collection, Preservation, Examination, Identification, Analysis, Presentation.

D. Identification, Examination, Preservation, Collection, Analysis, Presentation.

Correct Answer: B

QUESTION 3

An industry organization has implemented a system to allow trusted authentication between all of its partners. The system consists of a web of trusted RADIUS servers communicating over the Internet. An attacker was able to set up a malicious server and conduct a successful man-in-the-middle attack. Which of the following controls should be implemented to mitigate the attack in the future?

A. Use PAP for secondary authentication on each RADIUS server

B. Disable unused EAP methods on each RADIUS server

C. Enforce TLS connections between RADIUS servers

D. Use a shared secret for each pair of RADIUS servers

Correct Answer: C

QUESTION 4

A storage administrator would like to make storage available to some hosts and unavailable to other hosts. Which of the following would be used?

A. LUN masking

B. Deduplication

C. Multipathing

D. Snapshots

Correct Answer: A

QUESTION 5

A system administrator needs to meet the maximum amount of security goals for a new DNS infrastructure. The administrator deploys DNSSEC extensions to the domain names and infrastructure. Which of the following security goals does this meet? (Select TWO).

A. Availability

B. Authentication

C. Integrity

D. Confidentiality

E. Encryption

Correct Answer: BC

QUESTION 6

A security engineer has inherited an authentication project which integrates 1024-bit PKI certificates into the company infrastructure and now has a new requirement to integrate 2048-bit PKI certificates so that the entire company will be interoperable with its vendors when the project is completed. The project is now 25% complete, with 15% of the company staff being issued 1024-bit certificates. The provisioning of network based accounts has not occurred yet due to other project delays. The project is now expected to be over budget and behind its original schedule. Termination of the existing project and beginning a new project is a consideration because of the change in scope. Which of the following is the security engineer\\'s MOST serious concern with implementing this solution?

A. Succession planning

B. Performance

C. Maintainability

D. Availability

Correct Answer: C

QUESTION 7

Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the proprietary web application before launch. Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of the company\\'s purchased application? (Select TWO).

A. Code review

B. Sandbox

C. Local proxy

D. Fuzzer

E. Web vulnerability scanner

Correct Answer: CD

QUESTION 8

A security engineer is responsible for monitoring company applications for known vulnerabilities. Which of the following is a way to stay current on exploits and information security news?

A. Update company policies and procedures

B. Subscribe to security mailing lists

C. Implement security awareness training

D. Ensure that the organization vulnerability management plan is up-to-date

Correct Answer: B

QUESTION 9

An organization recently upgraded its wireless infrastructure to support 802.1x and requires all clients to use this method. After the upgrade, several critical wireless clients fail to connect because they are only pre-shared key compliant. For the foreseeable future, none of the affected clients have an upgrade path to put them into compliance with the 802.1x requirement. Which of the following provides the MOST secure method of integrating the non-compliant clients into the network?

A. Create a separate SSID and require the use of dynamic encryption keys.

B. Create a separate SSID with a pre-shared key to support the legacy clients and rotate the key at random intervals.

C. Create a separate SSID and pre-shared WPA2 key on a new network segment and only allow required communication paths.

D. Create a separate SSID and require the legacy clients to connect to the wireless network using certificate-based 802.1x.

Correct Answer: B

QUESTION 10

There have been some failures of the company\\'s customer-facing website. A security engineer has analyzed the root cause to be the WAF. System logs show that the WAF has been down for 14 total hours over the past month in four separate situations. One of these situations was a two hour scheduled maintenance activity aimed to improve the stability of the WAF. Which of the following is the MTTR, based on the last month\\'s performance figures?

A. 3 hours

B. 3.5 hours

C. 4 hours

D. 4.666 hours

Correct Answer: C

QUESTION 11

A small company is developing a new Internet-facing web application. The security requirements are:

1.

Users of the web application must be uniquely identified and authenticated.

2.

Users of the web application will not be added to the company\\'s directory services.

3.

Passwords must not be stored in the code. Which of the following meets these requirements?

A. Use OpenID and allow a third party to authenticate users.

B. Use TLS with a shared client certificate for all users.

C. Use SAML with federated directory services.

D. Use Kerberos and browsers that support SAML.

Correct Answer: A

QUESTION 12

A manager who was attending an all-day training session was overdue entering bonus and payroll information for subordinates. The manager felt the best way to get the changes entered while in training was to log into the payroll system, and then activate desktop sharing with a trusted subordinate. The manager granted the subordinate control of the desktop thereby giving the subordinate full access to the payroll system. The subordinate did not have authorization to be in the payroll system. Another employee reported the incident to the security team. Which of the following would be the MOST appropriate method for dealing with this issue going forward?

A. Provide targeted security awareness training and impose termination for repeat violators.

B. Block desktop sharing and web conferencing applications and enable use only with approval.

C. Actively monitor the data traffic for each employee using desktop sharing or web conferencing applications.

D. Permanently block desktop sharing and web conferencing applications and do not allow its use at the company.

Correct Answer: A

QUESTION 13

A system worth $100,000 has an exposure factor of eight percent and an ARO of four. Which of the following figures is the system\\'s SLE?

A. $2,000

B. $8,000

C. $12,000

D. $32,000

Correct Answer: B

QUESTION 14

An administrator is trying to categorize the security impact of a database server in the case of a security event. There are three databases on the server.

Current Financial Data = High level of damage if data is disclosed. Moderate damage if the system goes offline

Archived Financial Data = No need for the database to be online. Low damage for integrity loss

Public Website Data = Low damage if the site goes down. Moderate damage if the data is corrupted

Given these security categorizations of each database, which of the following is the aggregate security categorization of the database server?

A. Database server = {(Confidentiality HIGH),(Integrity High),(Availability High)}

B. Database server = {(Confidentiality HIGH),(Integrity Moderate),(Availability Moderate)}

C. Database server = {(Confidentiality HIGH),(Integrity Moderate),(Availability Low)}

D. Database server = {(Confidentiality Moderate),(Integrity Moderate),(Availability Moderate)}

Correct Answer: B

QUESTION 15

There have been some failures of the company\\'s internal facing website. A security engineer has found the WAF to be the root cause of the failures. System logs show that the WAF has been unavailable for 14 hours over the past month, in four separate situations. One of these situations was a two hour scheduled maintenance time, aimed at improving the stability of the WAF. Using the MTTR based on the last month\\'s performance figures, which of the following calculations is the percentage of uptime assuming there were 722 hours in the month?

A. 92.24 percent

B. 98.06 percent

C. 98.34 percent

D. 99.72 percent

Correct Answer: C

Latest CAS-002 Dumps   CAS-002 Practice Test   CAS-002 Braindumps