CAS-003^{Q&As}

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee\\' PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the following is MOST likely the problem?

A. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.

B. The DHCP server has a reservation for the PC\\'s MAC address for the wired interface.

C. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.

D. The DHCP server is unavailable, so no IP address is being sent back to the PC.

Correct Answer: A

QUESTION 2

A security analyst, who is working in a Windows environment, has noticed a significant amount of IPv6 traffic originating from a client, even though IPv6 is not currently in use. The client is a stand-alone device, not connected to the AD that manages a series of SCADA devices used for manufacturing.

Which of the following is the appropriate command to disable the client\\'s IPv6 stack?

```
A. C:\>netah ipsec static set policy name=MYIPPolicy /v Disable TCPIP6
B. C:\>reg add "HRCU\Software\Microsoft\Windows\CurrentVersion\Policies\IPV6/v
   disallowRun /t REG_DWORD /d "0000001" /f
C. C:\>reg add HRLM\system\CurrentControlSet\services\TCPIP6\Parameters /v
   DisabledComponents /t REG_DWORD /d 255 /f
D. C:\>reg add 'HRLM\SYSTEM\CurrentControlSet\IPV6" /f /v fDenyIPV6Connections /t
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

QUESTION 3

An analyst connects to a company web conference hosted on www.webconference.com/meetingID#01234 and observes that numerous guests have been allowed to join, without providing identifying information. The topics covered during the web conference are considered proprietary to the company. Which of the following security concerns does

the analyst present to management?

A. Guest users could present a risk to the integrity of the company\\\'s information.

B. Authenticated users could sponsor guest access that was previously approved by management.

C. Unauthenticated users could present a risk to the confidentiality of the company\\\'s information.

D. Meeting owners could sponsor guest access if they have passed a background check.

Correct Answer: C

The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with unauthorized users.

QUESTION 4

Following a recent data breach, a company has hired a new Chief Information Security Officer (CISO). The CISO is very concerned about the response time to the previous breach and wishes to know how the security team expects to react to a future attack. Which of the following is the BEST method to achieve this goal while minimizing disruption?

A. Perform a black box assessment

B. Hire an external red team audit

C. Conduct a tabletop exercise.

D. Recreate the previous breach.

E. Conduct an external vulnerability assessment.

Correct Answer: C

QUESTION 5

An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, report come In that a previously vulnerability has returned. Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

A. Peer review

B. Regression testing

C. User acceptance

D. Dynamic analysis

Correct Answer: A