RC0-C02 Q&As

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

Pass CompTIA RC0-C02 Exam with 100% Guarantee

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

https://www.passapply.com/rc0-c02.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A senior network security engineer has been tasked to decrease the attack surface of the corporate network. Which of the following actions would protect the external network interfaces from external attackers performing network scanning?

A. Remove contact details from the domain name registrar to prevent social engineering attacks.

B. Test external interfaces to see how they function when they process fragmented IP packets.

C. Enable a honeynet to capture and facilitate future analysis of malicious attack vectors.

D. Filter all internal ICMP message traffic, forcing attackers to use full-blown TCP port scans against external network interfaces.

Correct Answer: B

Fragmented IP packets are often used to evade firewalls or intrusion detection systems.

Port Scanning is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a Local Area Network (LAN) or Internet run many services that listen at well-known and

not so well known ports. A port scan helps the attacker find which ports are available (i.e., what service might be listing to a port).

One problem, from the perspective of the attacker attempting to scan a port, is that services listening on these ports log scans. They see an incoming connection, but no data, so an error is logged. There exist a number of stealth scan

techniques to avoid this. One method is a fragmented port scan.

Fragmented packet Port Scan

The scanner splits the TCP header into several IP fragments. This bypasses some packet filter firewalls because they cannot see a complete TCP header that can match their filter rules. Some packet filters and firewalls do queue all IP

fragments, but many networks cannot afford the performance loss caused by the queuing.

QUESTION 2

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 3

A company runs large computing jobs only during the overnight hours. To minimize the amount of capital investment in equipment, the company relies on the elastic computing services of a major cloud computing vendor. Because the virtual resources are created and destroyed on the fly across a large pool of shared resources, the company never knows which specific hardware platforms will be used from night to night. Which of the following presents the MOST risk to confidentiality in this scenario?

A. Loss of physical control of the servers

B. Distribution of the job to multiple data centers

C. Network transmission of cryptographic keys

D. Data scraped from the hardware platforms

Correct Answer: D

QUESTION 4

A member of the software development team has requested advice from the security team to implement a new secure lab for testing malware. Which of the following is the NEXT step that the security team should take?

A. Purchase new hardware to keep the malware isolated.

B. Develop a policy to outline what will be required in the secure lab.

C. Construct a series of VMs to host the malware environment.

D. Create a proposal and present it to management for approval.

Correct Answer: D

Before we can create a solution, we need to motivate why the solution needs to be created and plan the best implementation with in the company\\'s business operations. We therefore need to create a proposal that explains the intended implementation and allows for the company to budget for it.

QUESTION 5

In a situation where data is to be recovered from an attacker\\'s location, which of the following are the FIRST things to capture? (Select TWO).

A. Removable media

B. Passwords written on scrap paper

C. Snapshots of data on the monitor

D. Documents on the printer

E. Volatile system memory

F. System hard drive

Correct Answer: CE

An exact copy of the attacker\\'s system must be captured for further investigation so that the original data can remain unchanged. An analyst will then start the process of capturing data from the most volatile to the least volatile. The order of volatility from most volatile to least volatile is as follows: Data in RAM, including CPU cache and recently used data and applications Data in RAM, including system and network processes Swap files (also known as paging files) stored on local disk drives Data stored on local disk drives Logs stored on remote systems Archive media