

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.leads4pass.com/rc0-c02.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

The network administrator at an enterprise reported a large data leak. One compromised server was used to aggregate data from several critical application servers and send it out to the Internet using HTTPS. Upon investigation, there have been no user logins over the previous week and the endpoint protection software is not reporting any issues. Which of the following BEST provides insight into where the compromised server collected the information?

- A. Review the flow data against each server's baseline communications profile.
- B. Configure the server logs to collect unusual activity including failed logins and restarted services.
- C. Correlate data loss prevention logs for anomalous communications from the server.
- D. Setup a packet capture on the firewall to collect all of the server communications.

Correct Answer: A

Network logging tools such as Syslog, DNS, NetFlow, behavior analytics, IP reputation, honeypots, and DLP solutions provide visibility into the entire infrastructure. This visibility is important because signature-based systems are no longer sufficient for identifying the advanced attacker that relies heavily on custom malware and zero-day exploits. Having knowledge of each host's communications, protocols, and traffic volumes as well as the content of the data in question is key to identifying zero-day and APT (advance persistent threat) malware and agents. Data intelligence allows forensic analysis to identify anomalous or suspicious communications by comparing suspected traffic patterns against normal data communication behavioral baselines. Automated network intelligence and next-generation live forensics provide insight into network events and rely on analytical decisions based on known vs. unknown behavior taking place within a corporate network.

QUESTION 2

An organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?

- A. BGP route hijacking attacks
- B. Bogon IP network traffic
- C. IP spoofing attacks
- D. Man-in-the-middle attacks
- E. Amplified DDoS attacks

Correct Answer: C

The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall. This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range. IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host

and alters packet headers so that the legitimate host appears to be the source. When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL `www.loc.gov` would see spoofed content created by the hijacker. If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.

QUESTION 3

A company has noticed recently that its corporate information has ended up on an online forum. An investigation has identified that internal employees are sharing confidential corporate information on a daily basis. Which of the following are the MOST effective security controls that can be implemented to stop the above problem? (Select TWO).

- A. Implement a URL filter to block the online forum
- B. Implement NIDS on the desktop and DMZ networks
- C. Security awareness compliance training for all employees
- D. Implement DLP on the desktop, email gateway, and web proxies
- E. Review of security policies and procedures

Correct Answer: CD

Security awareness compliance training for all employees should be implemented to educate employees about corporate policies and procedures for working with information technology (IT). Data loss prevention (DLP) should be implemented to make sure that users do not send sensitive or critical information outside the corporate network.

QUESTION 4

The senior security administrator wants to redesign the company DMZ to minimize the risks associated with both external and internal threats. The DMZ design must support security in depth, change management and configuration processes, and support incident reconstruction. Which of the following designs BEST supports the given requirements?

- A. A dual firewall DMZ with remote logging where each firewall is managed by a separate administrator.
- B. A single firewall DMZ where each firewall interface is managed by a separate administrator and logging to the cloud.
- C. A SaaS based firewall which logs to the company's local storage via SSL, and is managed by the change control team.
- D. A virtualized firewall, where each virtual instance is managed by a separate administrator and logging to the same hardware.

Correct Answer: A

Security in depth is the concept of creating additional layers of security. The traditional approach of securing the IT infrastructure is no longer enough. Today's threats are multifaceted and often persistent, and traditional network perimeter security controls cannot effectively mitigate them. Organizations need to implement more effective, multi-level security controls that are embedded with their electronic assets. They need to protect key assets from both external and

internal threats. This security in depth approach is meant to sustain attacks even when perimeter and traditional controls have been breached.

In this question, using two firewalls to secure the DMZ from both external and internal attacks is the best approach. Having each firewall managed by a separate administrator will reduce the chance of a configuration error being made on both firewalls. The remote logging will enable incident reconstruction.

QUESTION 5

Company policy requires that all unsupported operating systems be removed from the network. The security administrator is using a combination of network based tools to identify such systems for the purpose of disconnecting them from the network. Which of the following tools, or outputs from the tools in use, can be used to help the security administrator make an approximate determination of the operating system in use on the local company network? (Select THREE).

- A. Passive banner grabbing
- B. Password cracker
- C. `http://www.company.org/documents_private/index.php?search=string#andtopic=windowsandtcp=packet%20captureandcookie=wokdjwalkjcnie61lkasdf2aliser4`
- D. 443/tcp open http
- E. `dig host.company.com`
- F. `09:18:16.262743 IP (tos 0x0, ttl 64, id 9870, offset 0, flags [none], proto TCP (6), length 40) 192.168.1.3.1051 > 10.46.3.7.80: Flags [none], cksum 0x1800 (correct), win 512, length 0`
- G. Nmap

Correct Answer: AFG

Banner grabbing and operating system identification can also be defined as fingerprinting the TCP/IP stack. Banner grabbing is the process of opening a connection and reading the banner or response sent by the application.

The output displayed in option F includes information commonly examined to fingerprint the OS.

Nmap provides features that include host discovery, as well as service and operating system detection.

[Latest RC0-C02 Dumps](#)

[RC0-C02 VCE Dumps](#)

[RC0-C02 Study Guide](#)