

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.pass2lead.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

Joe, the Chief Executive Officer (CEO), was an Information security professor and a Subject Matter Expert for over 20 years. He has designed a network defense method which he says is significantly better than prominent international standards. He has recommended that the company use his cryptographic method. Which of the following methodologies should be adopted?

- A. The company should develop an in-house solution and keep the algorithm a secret.
- B. The company should use the CEO's encryption scheme.
- C. The company should use a mixture of both systems to meet minimum standards.
- D. The company should use the method recommended by other respected information security organizations.

Correct Answer: D

In this question, we have one person's opinion about the best way to secure the network. His method may be more secure than other systems. However, for consensus of opinion, it is better to use the method recommended by other respected information security organizations. If the CEO's methods were the best methods, it is likely that the other respected information security organizations would have thought about them and would be using them. In other words, the methods recommended by other respected information security organizations are probably the best methods. Furthermore, if the company's systems need to communicate with external systems, the systems will need to use a 'standard' method otherwise the external system may not be able to decipher the communications from the company's systems.

QUESTION 2

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

A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. As an attack that aims at circumventing mutual authentication, or lack thereof, a man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to their satisfaction as expected from the legitimate other end. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, TLS can authenticate one or both parties using a mutually trusted certification authority. Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party

may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

QUESTION 3

The DLP solution has been showing some unidentified encrypted data being sent using FTP to a remote server. A vulnerability scan found a collection of Linux servers that are missing OS level patches. Upon further investigation, a technician notices that there are a few unidentified processes running on a number of the servers. What would be a key FIRST step for the data security team to undertake at this point?

- A. Capture process ID data and submit to anti-virus vendor for review.
- B. Reboot the Linux servers, check running processes, and install needed patches.
- C. Remove a single Linux server from production and place in quarantine.
- D. Notify upper management of a security breach.
- E. Conduct a bit level image, including RAM, of one or more of the Linux servers.

Correct Answer: E

Incident management (IM) is a necessary part of a security program. When effective, it mitigates business impact, identifies weaknesses in controls, and helps fine-tune response processes.

In this question, an attack has been identified and confirmed. When a server is compromised or used to commit a crime, it is often necessary to seize it for forensics analysis. Security teams often face two challenges when trying to remove a

physical server from service: retention of potential evidence in volatile storage or removal of a device from a critical business process.

Evidence retention is a problem when the investigator wants to retain RAM content. For example, removing power from a server starts the process of mitigating business impact, but it also denies forensic analysis of data, processes, keys,

and possible footprints left by an attacker.

A full a bit level image, including RAM should be taken of one or more of the Linux servers. In many cases, if your environment has been deliberately attacked, you may want to take legal action against the perpetrators. In order to preserve

this option, you should gather evidence that can be used against them, even if a decision is ultimately made not to pursue such action. It is extremely important to back up the compromised systems as soon as possible. Back up the systems prior to performing any actions that could affect data integrity on the original media.

QUESTION 4

Joe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).

- A. Jailbroken mobile device
- B. Reconnaissance tools

- C. Network enumerator
- D. HTTP interceptor
- E. Vulnerability scanner
- F. Password cracker

Correct Answer: DE

Communications between a mobile web application and a RESTful application server will use the HTTP protocol. To capture the HTTP communications for analysis, you should use an HTTP Interceptor.

To assess the security of the application server itself, you should use a vulnerability scanner.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are

important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a

database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. Vulnerability scanning typically refers to the

scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

QUESTION 5

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 listening 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.

[RC0-C02 VCE Dumps](#)

[RC0-C02 Practice Test](#)

[RC0-C02 Exam Questions](#)