Pass2Lead

https://Pass2Lead.com

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

![Pass2Lead Logo](https://Pass2Lead.com)

QUESTION 1

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 2

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

Subscribing to bug and vulnerability, security mailing lists is a good way of staying abreast and keeping up to date with the latest in those fields.

QUESTION 3

A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization\\'s customer database. The database will be accessed by both the company\\'s users and its customers. The procurement department has asked what security activities must be performed for the deal to proceed. Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).

A. Physical penetration test of the datacenter to ensure there are appropriate controls.

B. Penetration testing of the solution to ensure that the customer data is well protected.

C. Security clauses are implemented into the contract such as the right to audit.

D. Review of the organizations security policies, procedures and relevant hosting certifications.

E. Code review of the solution to ensure that there are no back doors located in the software.

Correct Answer: CD

Due diligence refers to an investigation of a business or person prior to signing a contract. Due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance. Due diligence should verify the data supplied in the RFP and concentrate on the following: Company profile, strategy, mission, and reputation Financial status, including reviews of audited financial statements Customer references, preferably from companies that have outsourced similar processes Management qualifications, including criminal background checks Process expertise, methodology, and effectiveness Quality initiatives and certifications Technology, infrastructure stability, and applications Security and audit controls Legal and regulatory compliance, including any outstanding complaints or litigation Use of subcontractors Insurance Disaster recovery and business continuity policies

C and D form part of Security and audit controls.

QUESTION 4

select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson Which of the following types of attacks is the user attempting?

A. XML injection

B. Command injection

C. Cross-site scripting

D. SQL injection

Correct Answer: D

The code in the question is SQL code. The attack is a SQL injection attack.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application\\'s software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL

![Pass2Lead](https://Pass2Lead.com)
database.

QUESTION 5

The risk manager at a small bank wants to use quantitative analysis to determine the ALE of running a business system at a location which is subject to fires during the year. A risk analyst reports to the risk manager that the asset value of the business system is $120,000 and, based on industry data, the exposure factor to fires is only 20% due to the fire suppression system installed at the site. Fires occur in the area on average every four years. Which of the following is the ALE?

A. $6,000

B. $24,000

C. $30,000

D. $96,000

Correct Answer: A

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF) SLE = AV x EF = $120 000 x 20% = $ 24,000 (this is over 4 years) Thus ALE = $ 24,000 / 4 = $ 6,000

References: http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 5th Edition, Project Management Institute, Inc., Newtown Square, 2013, p. 198 McMillan, Troy and Robin Abernathy, CompTIA Advanced Security Practitioner (CASP) CAS-002 Cert Guide, Pearson Education, Indianapolis, 2015, p. 305

RC0-C02 PDF Dumps   RC0-C02 Practice Test   RC0-C02 Exam Questions