Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

412-79 MCQs
412-79 TestPrep
412-79 Study Guide
412-79 Practice Test
412-79 Exam Questions

killexams.com

EC-Council

412-79

EC-Council Certified Security Analyst (ECSA V9)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/412-79

QUESTION: 187
Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

A. Vulnerability Report
B. Executive Report
C. Client-side test Report
D. Host Report

Answer: B

QUESTION: 188
An automated electronic mail message from a mail system which indicates that the user does not exist on that server is called as?

A. SMTP Queue Bouncing
B. SMTP Message Bouncing
C. SMTP Server Bouncing
D. SMTP Mail Bouncing

Answer: D
Reference:http://en.wikipedia.org/wiki/Bounce_message

QUESTION: 189
Which one of the following tools of trade is an automated, comprehensive penetration testing product for assessing the specific information security threats to an organization?

A. Sunbelt Network Security Inspector (SNSI)
B. CORE Impact
C. Canvas
D. Microsoft Baseline Security Analyzer (MBSA)

Answer: C

QUESTION: 190
Output modules allow Snort to be much more flexible in the formatting and presentation of output to its users. Snort has 9 output plug-ins that push out data in different formats. Which one of the following output plug-ins allows alert data to be written in a format easily importable to a database?

A. unified
B. csv
C. alert_unixsock
D. alert_fast

Answer: B

QUESTION: 191
Application security assessment is one of the activity that a pen tester performs in the attack phase. It is

designed to identify and assess threats to the organization through bespoke, proprietary applications or systems. It checks the application so that a malicious user cannot access, modify, or destroy data or services within the system.

Identify the type of application security assessment which analyzes the application-based code to confirm that it does not contain any sensitive information that an attacker might use to exploit an application.

A. Web Penetration Testing
B. Functionality Testing
C. Authorization Testing
D. Source Code Review

Answer: D

QUESTION: 192
Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

A. Threat-Assessment Phase
B. Pre-Assessment Phase
C. Assessment Phase
D. Post-Assessment Phase

Answer: B

QUESTION: 193
Which of the following defines the details of servicesto be provided for the client's organization and the list of services required for performing the test in the organization?

A. Draft

B. Report
C. Requirement list
D. Quotation

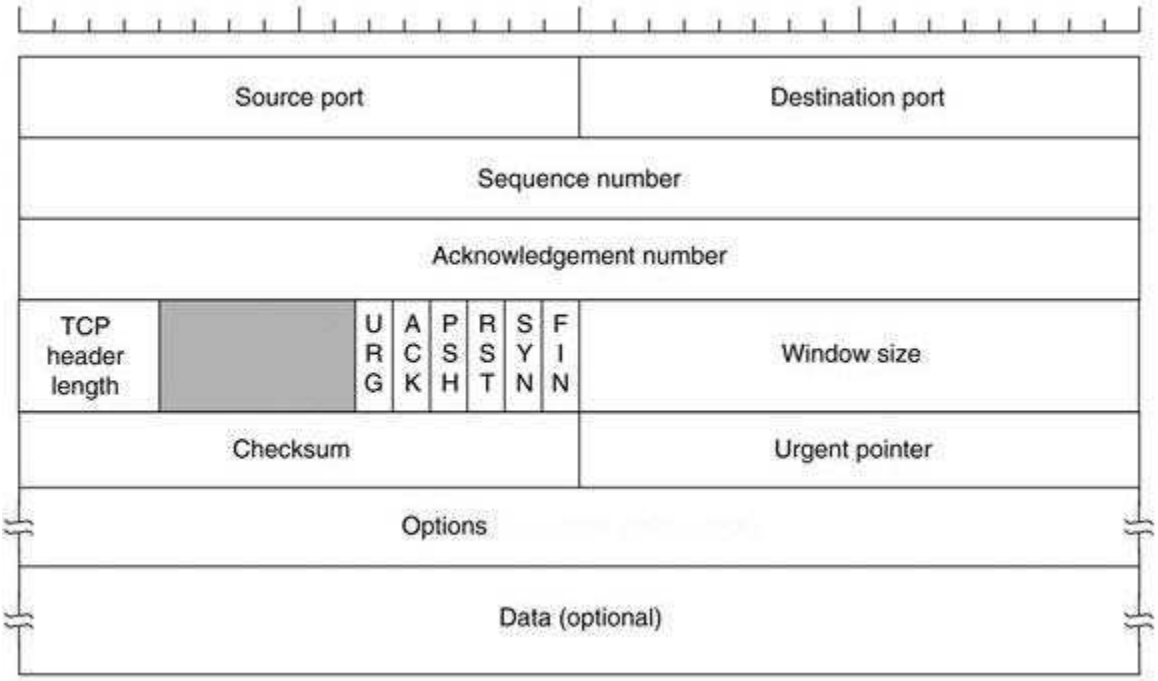
Answer: D

QUESTION: 194
Which of the following is not a condition specified by Hamel and Prahalad (1990)?

A. Core competency should be aimed at protecting company interests
B. Core competency is hard for competitors to imitate
C. Core competency provides customer benefits
D. Core competency can be leveraged widely to many products and markets

Answer: A
Reference:http://www.studymode.com/essays/Hamel-Prahalad-Core-Competency-1228370.html

QUESTION: 195
Transmission control protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment.
The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. It is used to track the state of communication between two TCP endpoints.
For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side
The below diagram shows the TCP Header format:



How many bits is a acknowledgement number?

A. 16 bits
B. 32 bits
C. 8 bits
D. 24 bits

Answer: B
Reference:http://en.wikipedia.org/wiki/Transmission_Control_Protocol(acknowledgement number)

QUESTION: 196
A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the tableinside the database using the below query and finds the table:
http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'—
What is the table name?

A. CTS
B. QRT
C. EMP
D. ABC

Answer: C

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.