ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Eccouncil

Code: ECSAV10

Exam: Certified Security Analyst (ECSA) v10 (ECSA v10)

https://www.examsnest.com/exam/ecsav10/

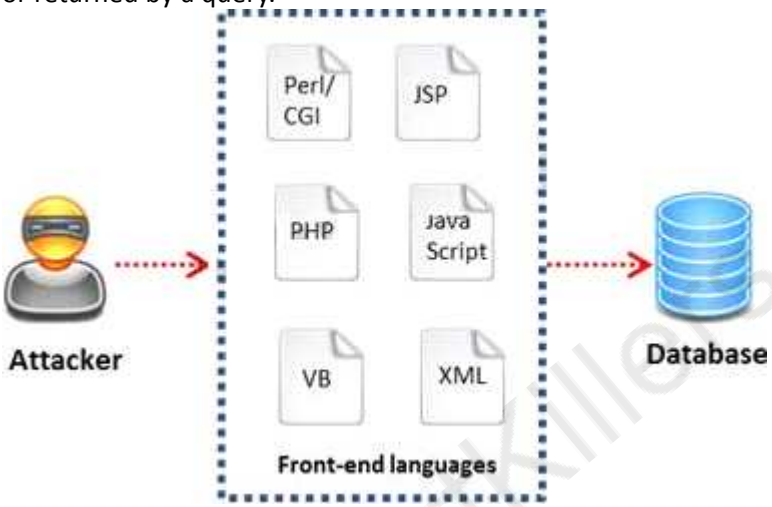
QUESTIONS & ANSWERS

DEMO VERSION

Version: 8.0

Question: 1

A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteri
a. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).
What query does he need to write to retrieve the information?
A. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000
B. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1—
C. SELECT * FROM StudentTable WHERE roll_number = '' or '1' = '1‘
D. RETRIVE * FROM StudentTable WHERE roll_number = 1'#

Answer: C

Question: 2

Which of the following has an offset field that specifies the length of the header and data?

A. IP Header
B. UDP Header
C. ICMP Header
D. TCP Header

Answer: D

Question: 3

War Driving is the act of moving around a specific area, mapping the population of wireless access points for statistical purposes. These statistics are then used to raise awareness of the security problems associated with these types of networks.
Which one of the following is a Linux based program that exploits the weak IV (Initialization Vector) problem documented with static WEP?

A. Airsnort
B. Aircrack
C. WEPCrack
D. Airpwn

Answer: A

Question: 4

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: 5

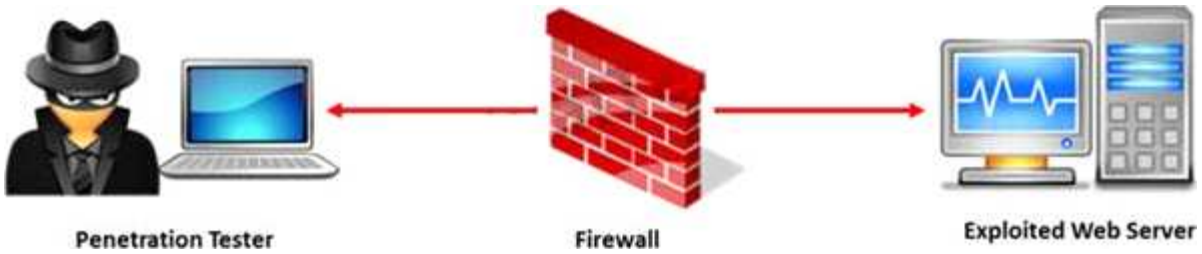
Which of the following methods is used to perform server discovery?

A. Banner Grabbing
B. Who is Lookup
C. SQL Injection
D. Session Hijacking

Answer: B

Question: 6

A penetration test will show you the vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/Medium/Low risk issues.



What are the two types of 'white-box' penetration testing?

A. Announced testing and blind testing
B. Blind testing and double blind testing
C. Blind testing and unannounced testing
D. Announced testing and unannounced testing

Answer: D

Question: 7

The objective of social engineering pen testing is to test the strength of human factors in a security chain within the organization. It is often used to raise the level of security awareness among employees.

The tester should demonstrate extreme care and professionalism during a social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization.
Which of the following methods of attempting social engineering is associated with bribing, handing out gifts, and becoming involved in a personal relationship to befriend someone inside the company?

A. Accomplice social engineering technique
B. Identity theft
C. Dumpster diving
D. Phishing social engineering technique

Answer: A

Question: 8

What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?

A. Server Side Includes
B. Sort Server Includes
C. Server Sort Includes
D. Slide Server Includes

Answer: A

Question: 9

During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

A. Examine Source of the Available Pages
B. Perform Web Spidering
C. Perform Banner Grabbing
D. Check the HTTP and HTML Processing by the Browser

Answer: D

Question: 10

After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. A switched network will not respond to packets sent to the broadcast address
B. Only IBM AS/400 will reply to this scan
C. Only Unix and Unix-like systems will reply to this scan
D. Only Windows systems will reply to this scan

Answer: C

Question: 11

Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

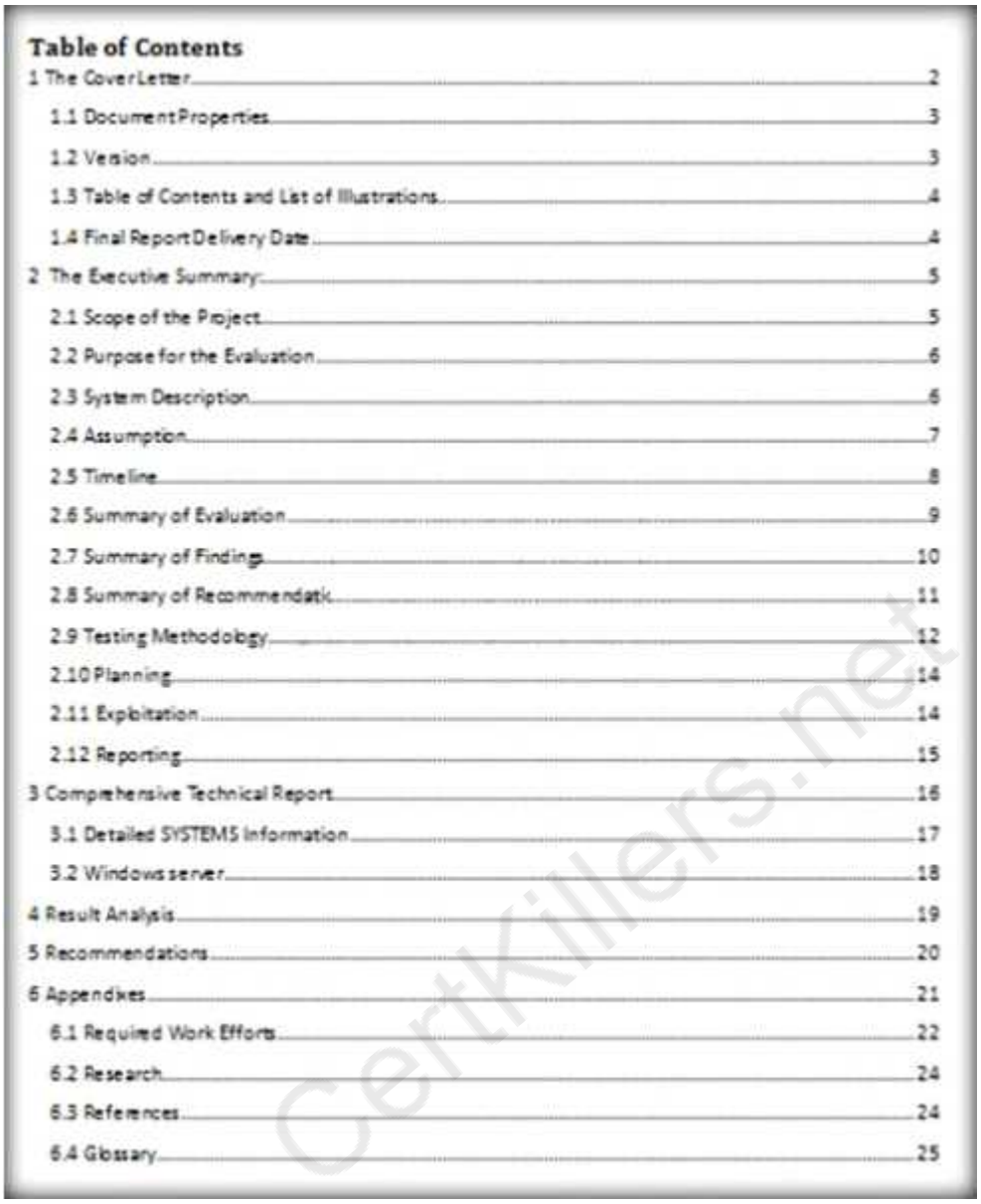


Table of Contents

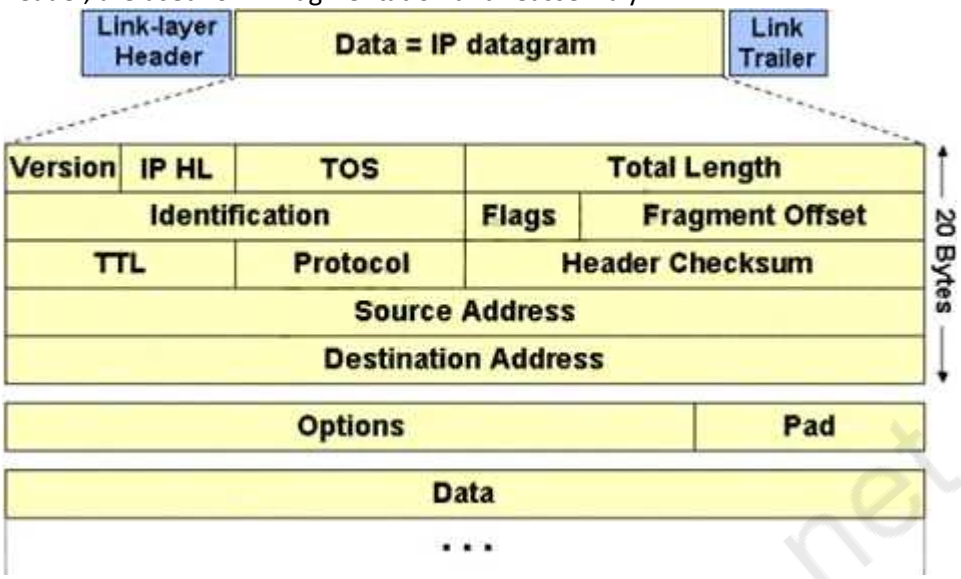
A. Client-Side Test Report
B. Activity Report
C. Host Report
D. Vulnerability Report

Answer: A

Question: 12

The IP protocol was designed for use on a wide variety of transmission links. Although the maximum length of an IP datagram is 64K, most transmission links enforce a smaller maximum packet length limit, called a MTU.
The value of the MTU depends on the type of the transmission link. The design of IP accommodates

MTU differences by allowing routers to fragment IP datagrams as necessary. The receiving station is responsible for reassembling the fragments back into the original full size IP datagram.
IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields in the IP header, are used for IP fragmentation and reassembly.



The fragment offset is 13 bits and indicates where a fragment belongs in the original IP datagram. This value is a:

A. Multiple of four bytes
B. Multiple of two bytes
C. Multiple of eight bytes
D. Multiple of six bytes

Answer: C

Question: 13

The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc.
Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control. This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations.
Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.

What is the best way to protect web applications from parameter tampering attacks?

A. Validating some parameters of the web application
B. Minimizing the allowable length of parameters
C. Using an easily guessable hashing algorithm
D. Applying effective input field filtering parameters

Answer: D

Question: 14

Which one of the following scans starts, but does not complete the TCP handshake sequence for each port selected, and it works well for direct scanning and often works well through firewalls?

A. SYN Scan
B. Connect() scan
C. XMAS Scan
D. Null Scan

Answer: A

Question: 15

The first and foremost step for a penetration test is information gathering. The main objective of this test is to gather information about the target system which can be used in a malicious manner to gain access to the target systems.

Which of the following information gathering terminologies refers to gathering information through social engineering on-site visits, face-to-face interviews, and direct questionnaires?

A. Active Information Gathering

B. Pseudonymous Information Gathering
C. Anonymous Information Gathering
D. Open Source or Passive Information Gathering

Answer: A

Question: 16

You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses.
You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Metamorphic
B. Oligomorhic
C. Polymorphic
D. Transmorphic

Answer: A

Question: 17

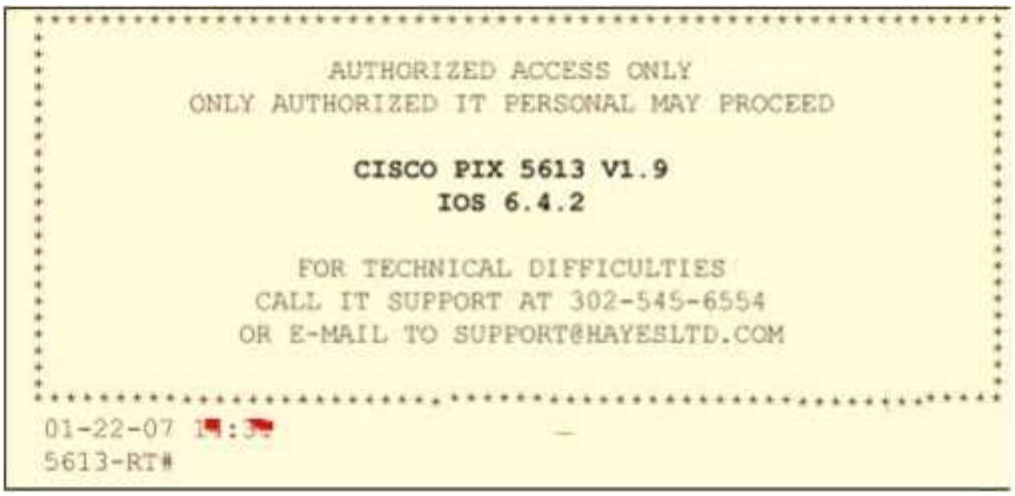
Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

A. Decreases consumed employee time and increases system uptime
B. Increases detection and reaction time
C. Increases response time
D. Both Decreases consumed employee time and increases system uptime and Increases response time

Answer: A

Question: 18

Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible.
Paulette presents the following screenshot to her boss so he can inform the clients about necessary changes need to be made. From the screenshot, what changes should the client company make?
Exhibit:



A. The banner should not state "only authorized IT personnel may proceed"
B. Remove any identifying numbers, names, or version information
C. The banner should include the Cisco tech support contact information as well
D. The banner should have more detail on the version numbers for the network equipment

Answer: B

Question: 19

Which of the following statements is true about the LM hash?

A. Disabled in Windows Vista and 7 OSs
B. Separated into two 8-character strings
C. Letters are converted to the lowercase
D. Padded with NULL to 16 characters

Answer: A

Question: 20

Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

A. Testing to provide a more complete view of site security
B. Testing focused on the servers, infrastructure, and the underlying software, including the target
C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections
D. Testing performed from a number of network access points representing each logical and physical segment

Answer: B

Question: 21

A framework for security analysis is composed of a set of instructions, assumptions, and limitations to analyze and solve security concerns and develop threat free applications.
Which of the following frameworks helps an organization in the evaluation of the company's information security with that of the industrial standards?

A. Microsoft Internet Security Framework
B. Information System Security Assessment Framework
C. The IBM Security Framework
D. Nortell's Unified Security Framework

Answer: B

Question: 22

A framework is a fundamental structure used to support and resolve complex issues. The framework that delivers an efficient set of technologies in order to develop applications which are more secure in using Internet and Intranet is:

A. Microsoft Internet Security Framework
B. Information System Security Assessment Framework (ISSAF)
C. Bell Labs Network Security Framework
D. The IBM Security Framework

Answer: A

Thank You for trying the PDF Demo

Vendor: Eccouncil

Code: ECSAV10

Exam: Certified Security Analyst (ECSA) v10 (ECSA v10)

https://www.examsnest.com/exam/ecsav10/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation