ECSAV8Q&As

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL ECSAV8 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/ecsav8.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

A. Frame Injection Attack

B. LDAP Injection Attack

C. XPath Injection Attack

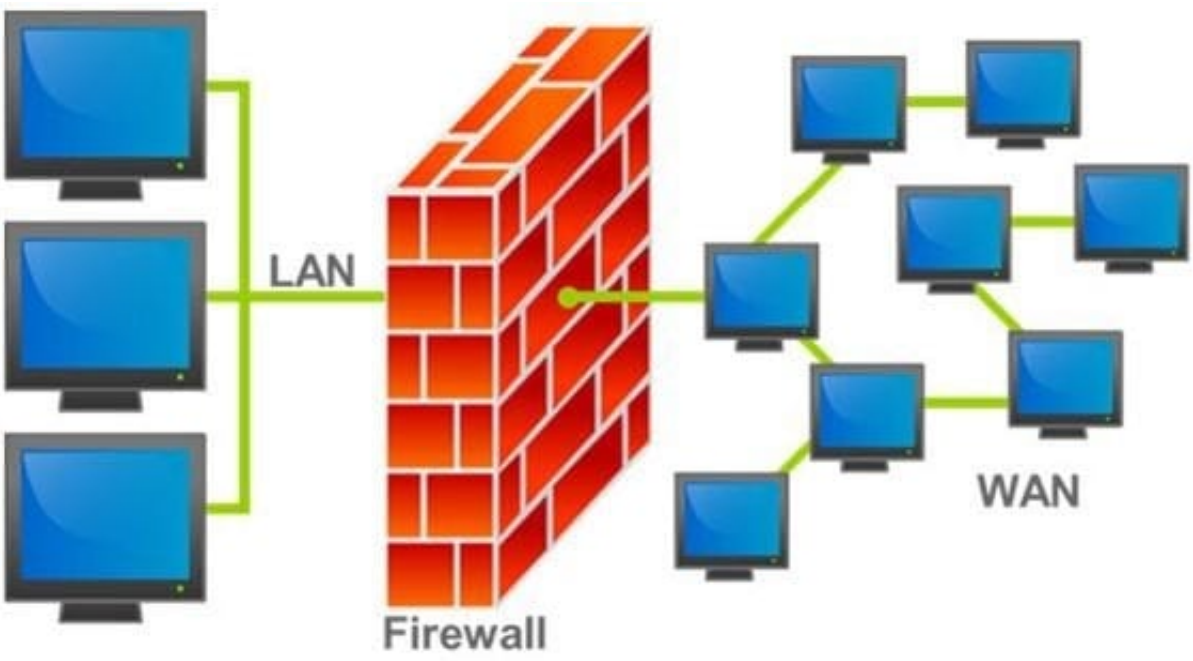
D. SOAP Injection Attack

Correct Answer: D

Explanation: http://luizfirmino.blogspot.com/2011_09_01_archive.html

QUESTION 2

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped.



Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

A. Appliance based firewalls cannot be upgraded

B. Firewalls implemented on a hardware firewall are highly scalable

C. Hardware appliances does not suffer from security vulnerabilities associated with the underlying operating system

D. Operating system firewalls are highly configured

Correct Answer: C

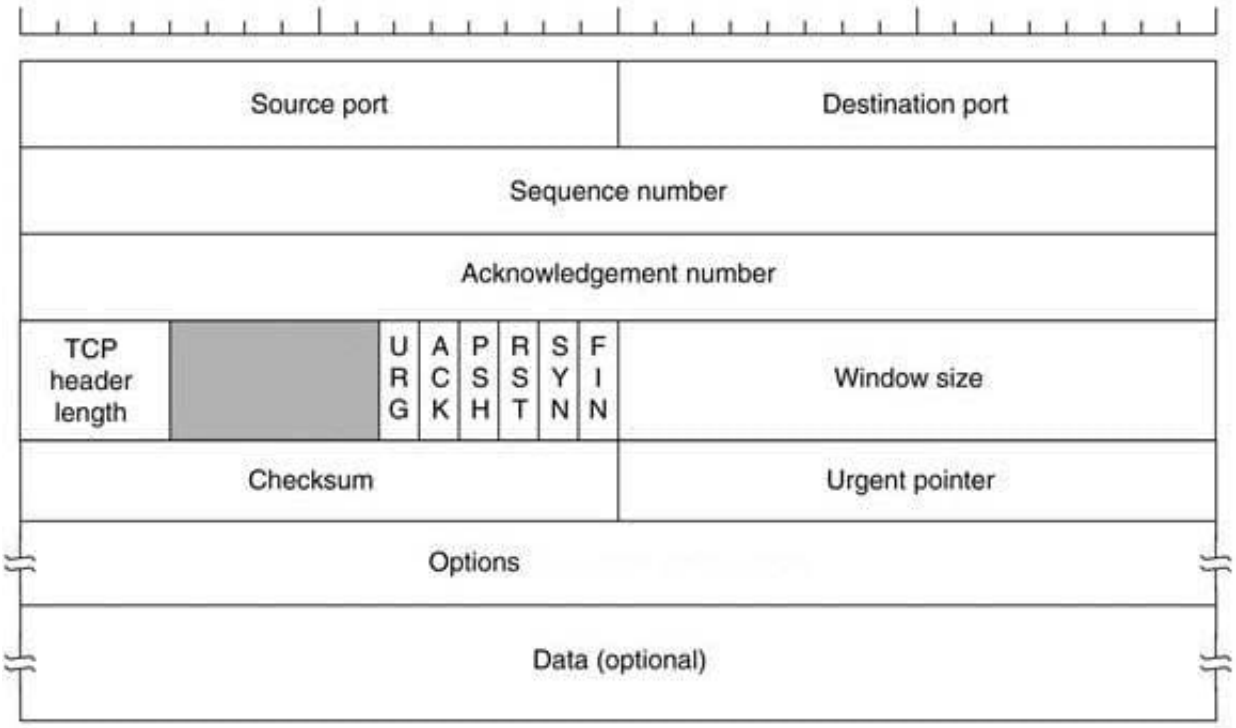
QUESTION 3

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 endto-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

Correct Answer: B

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

QUESTION 4

Identify the attack represented in the diagram below: A. Input Validation

B. Session Hijacking

C. SQL Injection

D. Denial-of-Service

Correct Answer: B

Reference: http://en.wikipedia.org/wiki/Session_hijacking

QUESTION 5

Identify the person who will lead the penetration-testing project and be the client point of contact.

A. Database Penetration Tester

B. Policy Penetration Tester

C. Chief Penetration Tester

D. Application Penetration Tester

Correct Answer: C

Reference: http://www.scribd.com/doc/133635286/LPTv4-Module-15-Pre-Penetration- Testing-Checklist-NoRestriction (page 15)

QUESTION 6

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

Correct Answer: A

Reference: http://www.onlinehashcrack.com/how_to_crack_windows_passwords.php (first paragraph of the page)

QUESTION 7

Which of the following defines the details of services to 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

Correct Answer: D

QUESTION 8

Which of the following is an application alert returned by a web application that helps an attacker guess a valid username?

A. Invalid username or password

B. Account username was not found

C. Incorrect password

D. Username or password incorrect

Correct Answer: C

QUESTION 9

Which of the following policies helps secure data and protects the privacy of organizational information?

A. Special-Access Policy

B. Document retention Policy

C. Cryptography Policy

D. Personal Security Policy

Correct Answer: C

QUESTION 10

Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.

Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes.

Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.

What can a pen tester do to detect input sanitization issues?

A. Send single quotes as the input data to catch instances where the user input is not sanitized

B. Send double quotes as the input data to catch instances where the user input is not sanitized

C. Send long strings of junk data, just as you would send strings to detect buffer overruns

D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

Correct Answer: D

QUESTION 11

Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

A. Service-based Assessment Solutions

B. Product-based Assessment Solutions

C. Tree-based Assessment

D. Inference-based Assessment

Correct Answer: C

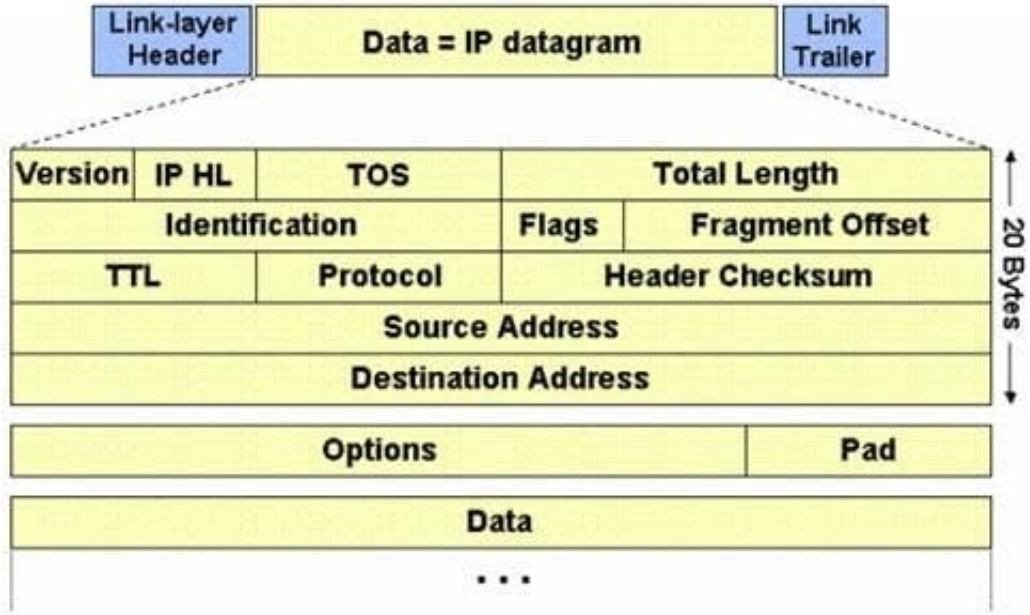
Reference: http://www.netsense.info/downloads/security_wp_mva.pdf (page 12, tree-based assessment technology, second para)

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

Correct Answer: C

Reference: http://www.freesoft.org/CIE/Course/Section3/7.htm (fragment offset: 13 bits)

QUESTION 13

What threat categories should you use to prioritize vulnerabilities detected in the pen testing report?

A. 1, 2, 3, 4, 5

B. Low, medium, high, serious, critical

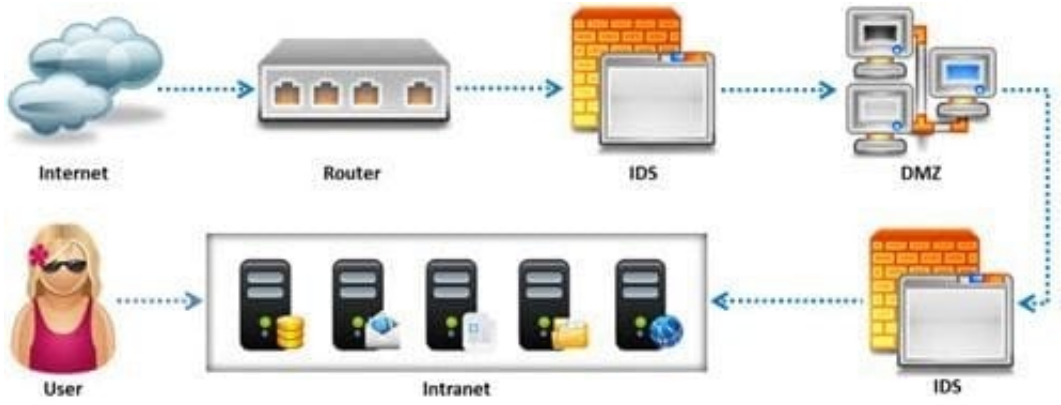
C. Urgent, dispute, action, zero, low

D. A, b, c, d, e

Correct Answer: B

QUESTION 14

Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol\\'s urgency feature, which could allow testers to evade the IDS.



Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/ FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS.

Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

A. SYN/RST/ACK

B. SYN/FIN/ACK

C. SYN/FIN

D. All Flags

Correct Answer: D

Reference:

http://books.google.com.pk/books?id=tUCumJot0ocCandpg=PA63andlpg=PA63anddq=TCP+flag +combinations

+combines+the+problem+of+initiation,+midstream,+and+termination+flags+ with+the+PSH+and

+URGandsource=blandots=mIGSXBIi15andsig=WMnXlEChVSU4RhK65W_V

3tzNjnsandhl=enandsa=Xandei=H7AfVJCtLaufygO1v4DQDgandved=0CBsQ6AEwAA#v=onepageand q=TCP%

20flag%20combinations%20combines%20the%20problem%20of%20initiation%2 C%20midstream%2C%

20and%20termination%20flags%20with%20the%20PSH%20and% 20URGandf=false (see the highlighted

sentence in Table 3-1 at the end of the page)

QUESTION 15

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels.

A vulnerability assessment is used to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

Which of the following vulnerability assessment technique is used to test the web server infrastructure for any misconfiguration and outdated content?

A. Passive Assessment

B. Host-based Assessment

C. External Assessment

D. Application Assessment

Correct Answer: B