

412-79V10^{Q&As}

EC-Council Certified Security Analyst (ECSA) V10

Pass EC-COUNCIL 412-79V10 Exam with 100% Guarantee

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

<https://www.pass2lead.com/412-79v10.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

Wireshark is a network analyzer. It reads packets from the network, decodes them, and presents them in an easy-to-understand format. Which one of the following is the command-line version of Wireshark, which can be used to capture the live packets from the wire or to read the saved capture files?

- A. Tcpdump
- B. Capinfos
- C. Tshark
- D. Idl2wrs

Correct Answer: B

QUESTION 2

DNS information records provide important data about:

- A. Phone and Fax Numbers
- B. Location and Type of Servers
- C. Agents Providing Service to Company Staff
- D. New Customer

Correct Answer: B

QUESTION 3

Amazon Consulting Corporation provides penetration testing and managed security services to companies. Legality and regulatory compliance is one of the important components in conducting a successful security audit.

Before starting a test, one of the agreements both the parties need to sign relates to limitations, constraints, liabilities, code of conduct, and indemnification considerations between the parties.



Which agreement requires a signature from both the parties (the penetration tester and the company)?

- A. Non-disclosure agreement
- B. Client fees agreement
- C. Rules of engagement agreement
- D. Confidentiality agreement

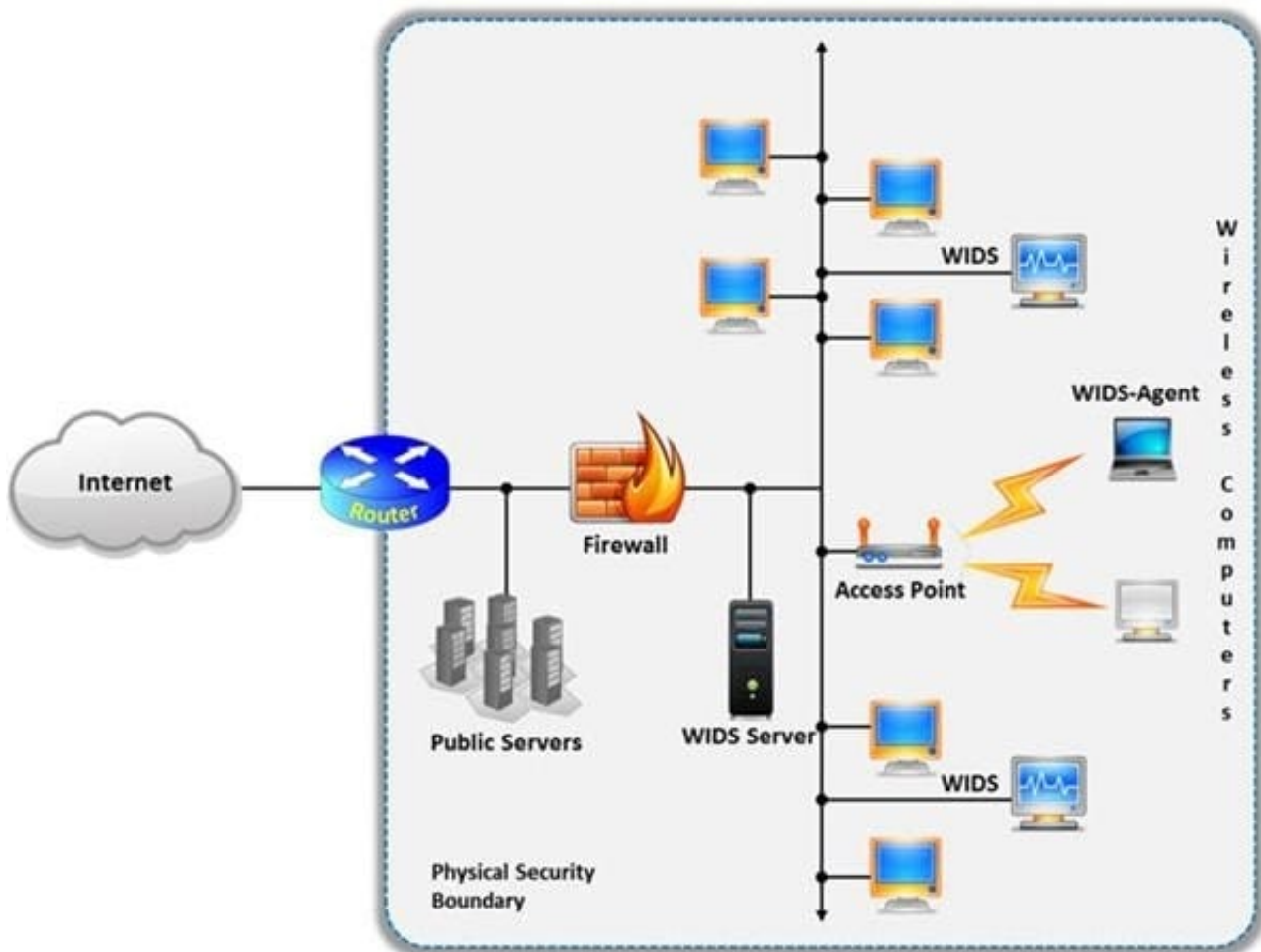
Correct Answer: C

QUESTION 4

A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected.

Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?



- A. Social engineering
- B. SQL injection
- C. Parameter tampering
- D. Man-in-the-middle attack

Correct Answer: D

Reference: http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf (page 5)

QUESTION 5

The first phase of the penetration testing plan is to develop the scope of the project in consultation with the client. Pen testing test components depend on the client's operating environment, threat perception, security and compliance requirements, ROE, and budget. Various components need to be considered for testing while developing the scope of the project.



Which of the following is NOT a pen testing component to be tested?

- A. System Software Security
- B. Intrusion Detection
- C. Outside Accomplices
- D. Inside Accomplices

Correct Answer: C

[Latest 412-79V10 Dumps](#)

[412-79V10 PDF Dumps](#)

[412-79V10 VCE Dumps](#)