ECSAV10Q&As

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

https://www.passapply.com/ecsav10.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The penetration testers are required to follow predefined standard frameworks in making penetration

testing reporting formats.

Which of the following standards does NOT follow the commonly used methodologies in penetration

testing?

A. National Institute of Standards and Technology (NIST)

B. Information Systems Security Assessment Framework (ISSAF)

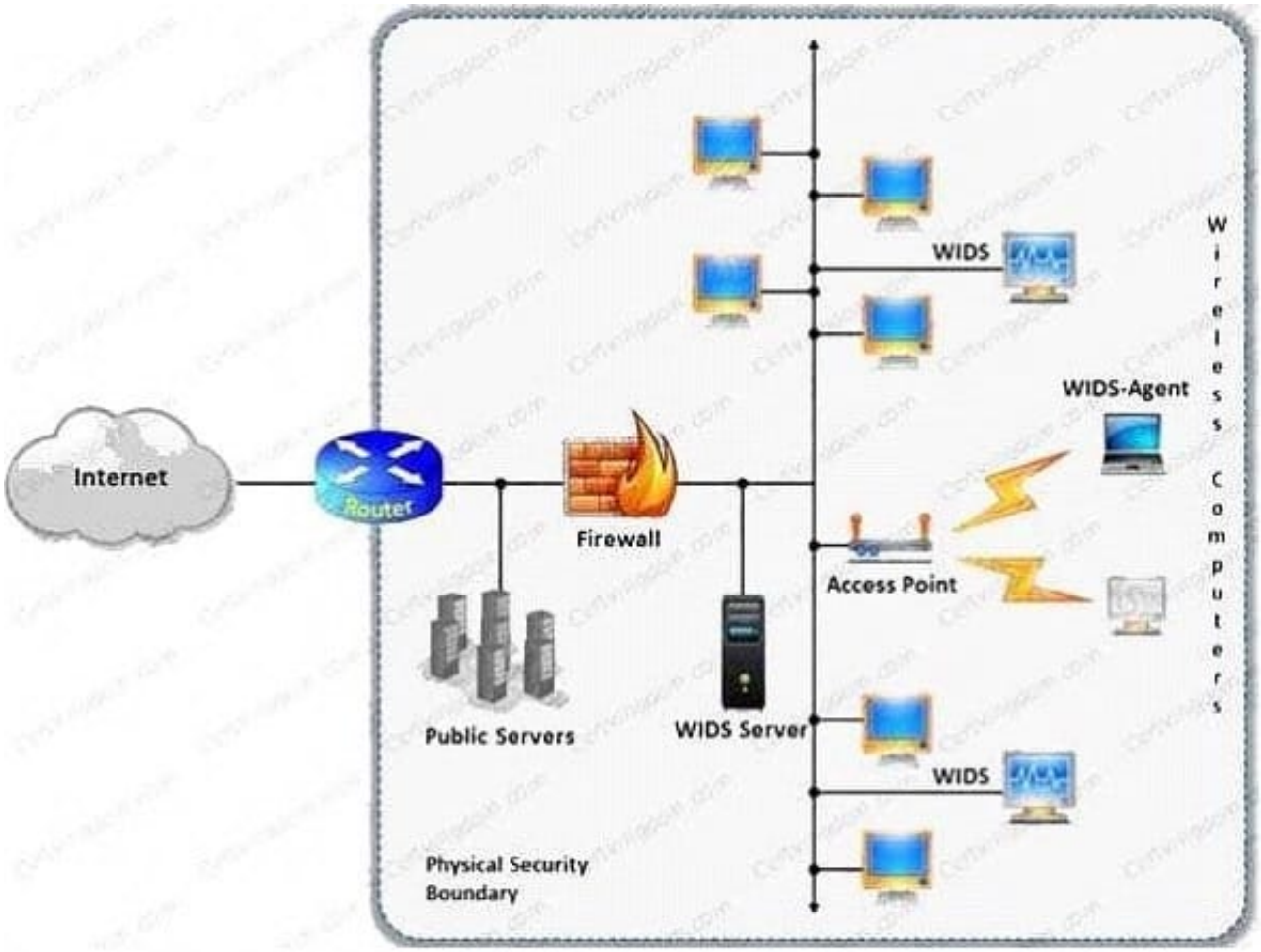
C. Open Web Application Security Project (OWASP)

D. American Society for Testing Materials (ASTM)

Correct Answer: D

QUESTION 2

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

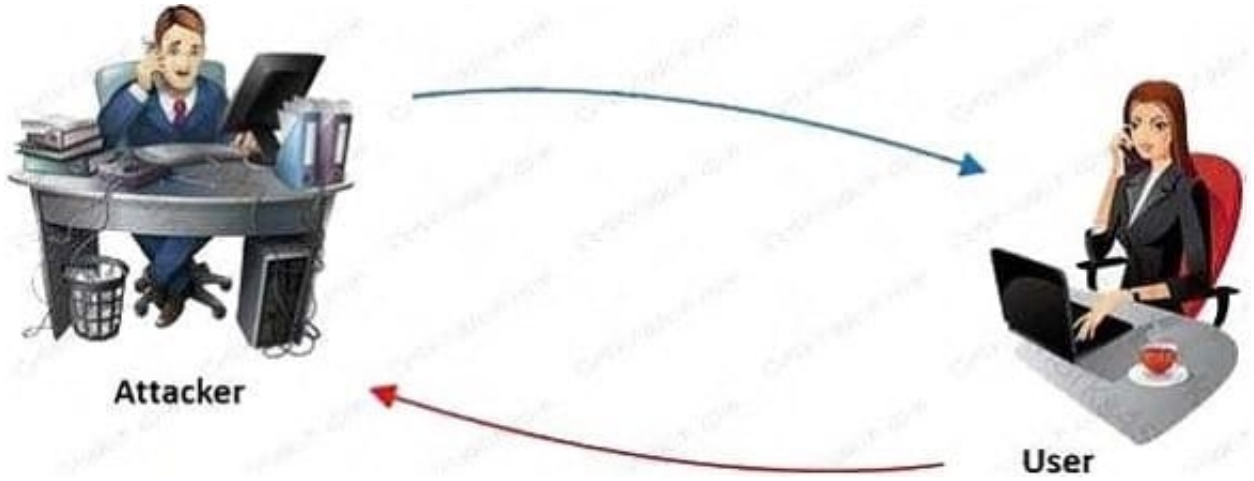
C. Parameter tampering

D. Man-in-the-middle attack

Correct Answer: D

QUESTION 3

The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?

A. Phishing

B. Spoofing

C. Tapping

D. Vishing

Correct Answer: D

QUESTION 4

You have just completed a database security audit and writing the draft pen testing report.

Which of the following will you include in the recommendation section to enhance the security of the

database server?

A. Allow direct catalog updates

B. Install SQL Server on a domain controller

C. Install a certificate to enable SSL connections

D. Grant permissions to the public database role

Correct Answer: C

QUESTION 5

Sam is auditing a web application for SQL injection vulnerabilities. During the testing, Sam discovered that

the web application is vulnerable to SQL injection. He starts fuzzing the search field in the web application

with UNION based SQL queries, however, he realized that the underlying WAF is blocking the requests.

To avoid this, Sam is trying the following query:

UNION/**/SELECT/**/\\'/**/OR/**/1/**/=/**/1

Which of the following evasion techniques is Sam using?

A. Sam is using char encoding to bypass WAF

B. Sam is using obfuscated code to bypass WAF

C. Sam is using inline comments to bypass WAF

D. Sam is manipulating white spaces to bypass WAF

Correct Answer: C