412-79V8 Q&As

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79V8 Exam with 100% Guarantee

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

https://www.passapply.com/412-79v8.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Network scanning is used to identify the available network resources. Which one of the following is also known as a half-open scan, because a full TCP connection is never completed and it is used to determine which ports are open and listening on a target device?

A. SYN Scan

B. TCP Connect Scan

C. XMAS Scan

D. Null Scan

Correct Answer: A

QUESTION 2

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

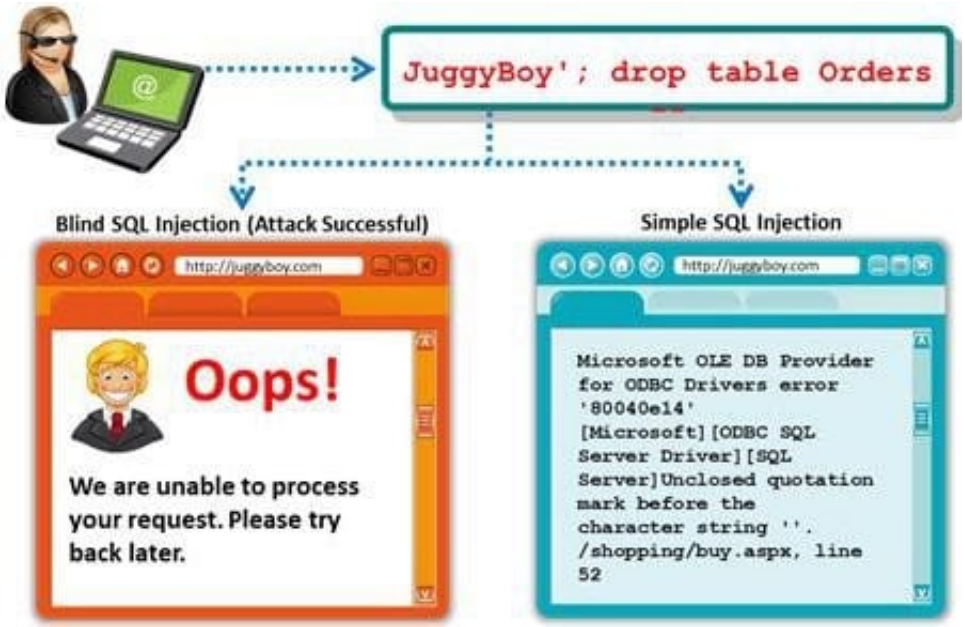
C. The IBM Security Framework

D. Nortell\\'s Unified Security Framework

Correct Answer: B

QUESTION 3

A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer\\'s specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases. A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name. http://juggyboy.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY \\'00:00:10\\'-http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY \\'00:00:10\\'-http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY \\'00:00:10\\'-http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY \\'00:00:10\\'-http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY \\'00:00:10\\'-

What is the database name?

A. WXYZ

B. PQRS

C. EFGH

D. ABCD

Correct Answer: D

QUESTION 4

Which one of the following is a supporting tool for 802.11 (wireless) packet injections, it spoofs 802.11 packets to verify whether the access point is valid or not?

A. Airsnort

B. Aircrack

C. Airpwn

D. WEPCrack

Correct Answer: C

QUESTION 5

NTP protocol is used to synchronize the system clocks of computers with a remote time server or time source over a network. Which one of the following ports is used by NTP as its transport layer?

A. TCP port 152

B. UDP port 177

C. UDP port 123

D. TCP port 113

Correct Answer: C