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.geekcert.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

John, a penetration tester from a pen test firm, was asked to collect information about the host file in a Windows system directory. Which of the following is the location of the host file in Window system directory?

A. C:\Windows\System32\Boot

B. C:\WINNT\system32\drivers\etc

C. C:\WINDOWS\system32\cmd.exe

D. C:\Windows\System32\restore

Correct Answer: B

Reference: http://en.wikipedia.org/wiki/Hosts_(file) (location in the file system, see the table)

QUESTION 2

A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. 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.
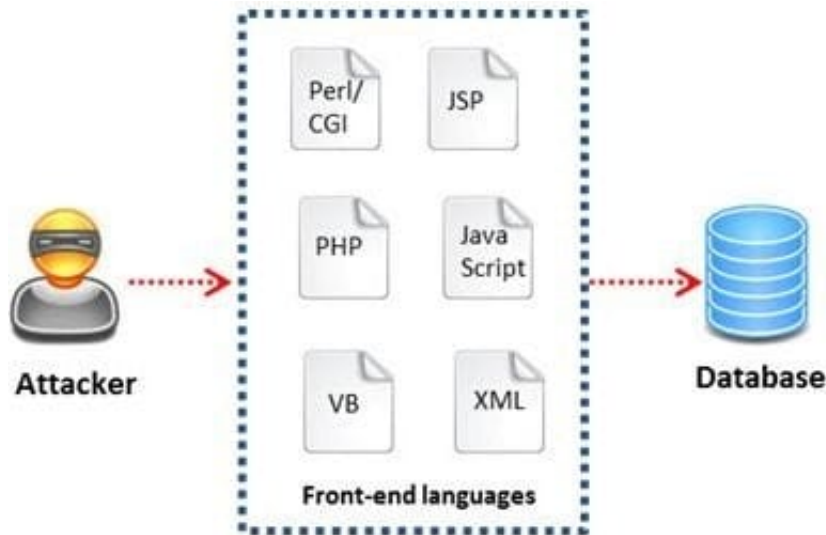
A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).

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\\'#

Correct Answer: C

QUESTION 3

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS

B. Active IDS

C. Progressive IDS

D. NIPS

Correct Answer: B

QUESTION 4

In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?

A. IPS evasion technique

B. IDS evasion technique

C. UDP evasion technique

D. TTL evasion technique

Correct Answer: D

Reference: http://is.muni.cz/th/172999/fi_m/MT_Bukac.pdf (page 24)

QUESTION 5

You work as an IT security auditor hired by a law firm in Boston. You have been assigned the responsibility to audit the client for security risks. When assessing the risk to the clients network, what step should you take first?

A. Analyzing, categorizing and prioritizing resources

B. Evaluating the existing perimeter and internal security

C. Checking for a written security policy

D. Analyzing the use of existing management and control architecture

Correct Answer: C

Latest 412-79V10 Dumps   412-79V10 PDF Dumps   412-79V10 VCE Dumps