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.pass4itsure.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

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

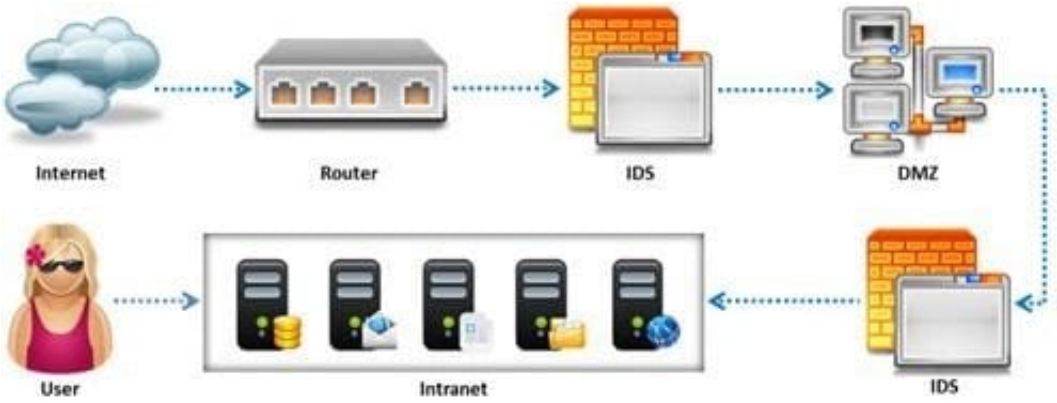
D. C:\Windows\System32\restore

Correct Answer: B

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

QUESTION 2

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 3

You are conducting a penetration test against a company and you would like to know a personal email address of John, a crucial employee. What is the fastest, cheapest way to find out John\\'s email address.

A. Call his wife and ask for his personal email account

B. Call a receptionist and ask for John Stevens\\' personal email account

C. Search in Google for his personal email ID

D. Send an email to John stating that you cannot send him an important spreadsheet attachment file to his business email account and ask him if he has any other email accounts

Correct Answer: D

QUESTION 4

SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the

data input or transmitted from the client (browser) to the web application.

A successful SQL injection attack can:

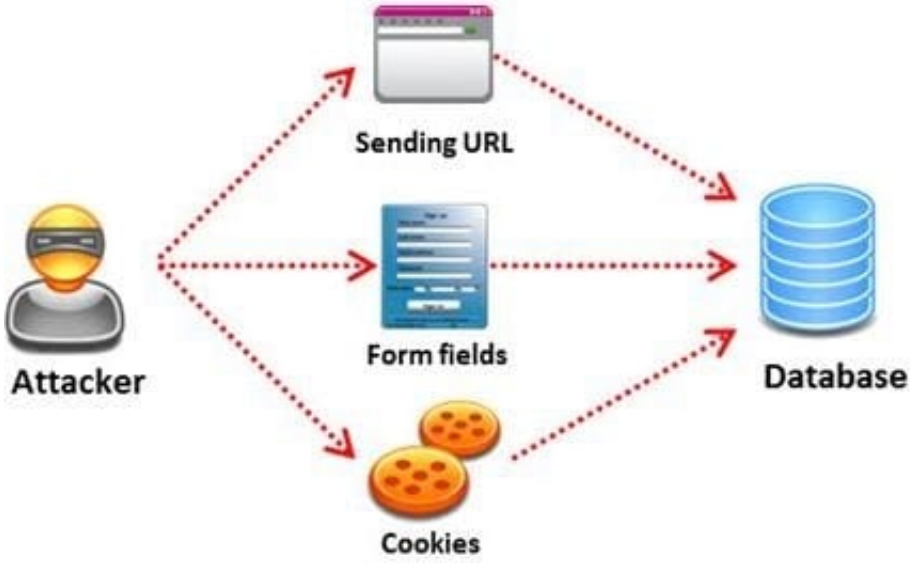
i)Read sensitive data from the database

iii)Modify database data (insert/update/delete)

iii)Execute administration operations on the database (such as shutdown the DBMS)

iV)Recover the content of a given file existing on the DBMS file system or write files into the file system

v)Issue commands to the operating system



Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error.

In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

A. Automated Testing

B. Function Testing

C. Dynamic Testing

D. Static Testing

Correct Answer: D

Reference:

http://ijritcc.org/IJRITCC%20Vol_2%20Issue_5/Removal%20of%20Data%20Vulnerabilities %20Using%

20SQL.pdf

QUESTION 5

How many possible sequence number combinations are there in TCP/IP protocol?

A. 320 billion

B. 32 million

C. 4 billion

D. 1 billion

Correct Answer: C