



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

A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table:

```
http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype=\\'U\\')=3) WAITFOR DELAY \\00:00:10\\'-
```

```
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY \\00:00:10\\'-
```

```
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY \\00:00:10\\'-
```

```
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY \\00:00:10\\'-
```

What is the table name?

- A. CTS
- B. QRT
- C. EMP
- D. ABC

Correct Answer: C

QUESTION 2

Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

- A. 3001-3100
- B. 5000-5099
- C. 6666-6674
- D. 0-1023

Correct Answer: D

Reference: <https://www.ietf.org/rfc/rfc1700.txt> (well known port numbers, 4th para)

QUESTION 3

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of three Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.



The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.

```
C:\Windows\system32\cmd.exe - tracert www.eccouncil.org
C:\>tracert www.eccouncil.org

Tracing route to www.eccouncil.org [66.111.3.186]
over a maximum of 30 hops:

  0  *          *          *          Request timed out.
  1  *          *          *          Request timed out.
  2  111 ms    27 ms     1 ms    ras.beamtele.net [183.82.14.17]
  3  124 ms    156 ms    128 ms  121.240.252.5.STATIC-Hyderabad.usn1.net.in [121.
240.252.5]
  4  155 ms    193 ms    186 ms  172.29.253.33
  5  300 ms    *         142 ms  172.25.81.134
  6  242 ms    *         *       ix-0-100.tcore1.MLU-Mumbai.as6453.net [180.87.38
.5]
  7  243 ms    *         *       if-9-5.tcore1.WYN-Marseille.as6453.net [80.231.2
17.17]
  8  *         *         *       Request timed out.
  9  369 ms    *         *       if-9-2.tcore2.L78-London.as6453.net [80.231.200.
14]
 10  319 ms    380 ms    *       if-1-2.tcore1.L78-London.as6453.net [80.231.130.
121]
 11  *         337 ms    *       if-17-2.tcore1.LDN-London.as6453.net [80.231.130
.130]
 12  *         *         290 ms  195.219.83.102
 13  284 ms    332 ms    497 ms  v1-3604-ue-228.csw2.London1.Level3.net [4.69.166
```

During routing, each router reduces packets\' TTL value by

- B. 1
- C. 4
- D. 2

Correct Answer: B

Reference: <http://www.packetu.com/2009/10/09/traceroute-through-the-asa/>

QUESTION 4

Which among the following information is not furnished by the Rules of Engagement (ROE) document?

- A. Techniques for data collection from systems upon termination of the test
- B. Techniques for data exclusion from systems upon termination of the test
- C. Details on how data should be transmitted during and after the test
- D. Details on how organizational data is treated throughout and after the test



Correct Answer: A

QUESTION 5

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

- A. Smurf
- B. Trinoo
- C. Fraggle
- D. SYN flood

Correct Answer: A

[Latest 412-79V10 Dumps](#)

[412-79V10 PDF Dumps](#)

[412-79V10 Braindumps](#)