

PassTest

Bessere Qualität , bessere Dienstleistungen!



Q&A

<http://www.passtest.de>

Einjährige kostenlose Aktualisierung

Exam : **412-79v8**

Title : EC-Council Certified
Security Analyst (ECSA)

Version : DEMO

1.Which of the following password cracking techniques is used when the attacker has some information about the password?

- A. Hybrid Attack
- B. Dictionary Attack
- C. SyllableAttack
- D. Rule-based Attack

Answer: D

Explanation:<http://202.154.59.182/mfile/files/Information%20System/Computer%20Forensics%3B%20Hard%20Disk%20and%20Operating%20Systems/CHAPTER%207%20Application%20Password%20Crackers.pdf>(page 4, rule-based attack)

2.Which of the following is an application alert returned by a web application that helps an attacker guess a valid username?

- A. Invalid username or password
- B. Account username was not found
- C. Incorrect password
- D. Username or password incorrect

Answer: C

3.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

Answer: C

4.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

Answer: B

5.HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where 'xx' is the

- A. ASCII value of the character
- B. Binary value of the character
- C. Decimal value of the character
- D. Hex value of the character

Answer: D

Explanation:[https://books.google.nl/books?id=0RfANAwOUdIC&pg=PA720&lpg=PA720&dq=%22xx+notation %22+binary&source=bl&ots=pGMqass7ti&sig=rnlG1xZ78ScUvullTmDY3r7REuc&hl=nl&sa=X&ei=8C4dVYe1NorgaszgoAL&ved=0CEQQ6AEwBQ#v=onepage&q=%22xx%20notation%22%20binary&f=false](https://books.google.nl/books?id=0RfANAwOUdIC&pg=PA720&lpg=PA720&dq=%22xx+notation%22+binary&source=bl&ots=pGMqass7ti&sig=rnlG1xZ78ScUvullTmDY3r7REuc&hl=nl&sa=X&ei=8C4dVYe1NorgaszgoAL&ved=0CEQQ6AEwBQ#v=onepage&q=%22xx%20notation%22%20binary&f=false)