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

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

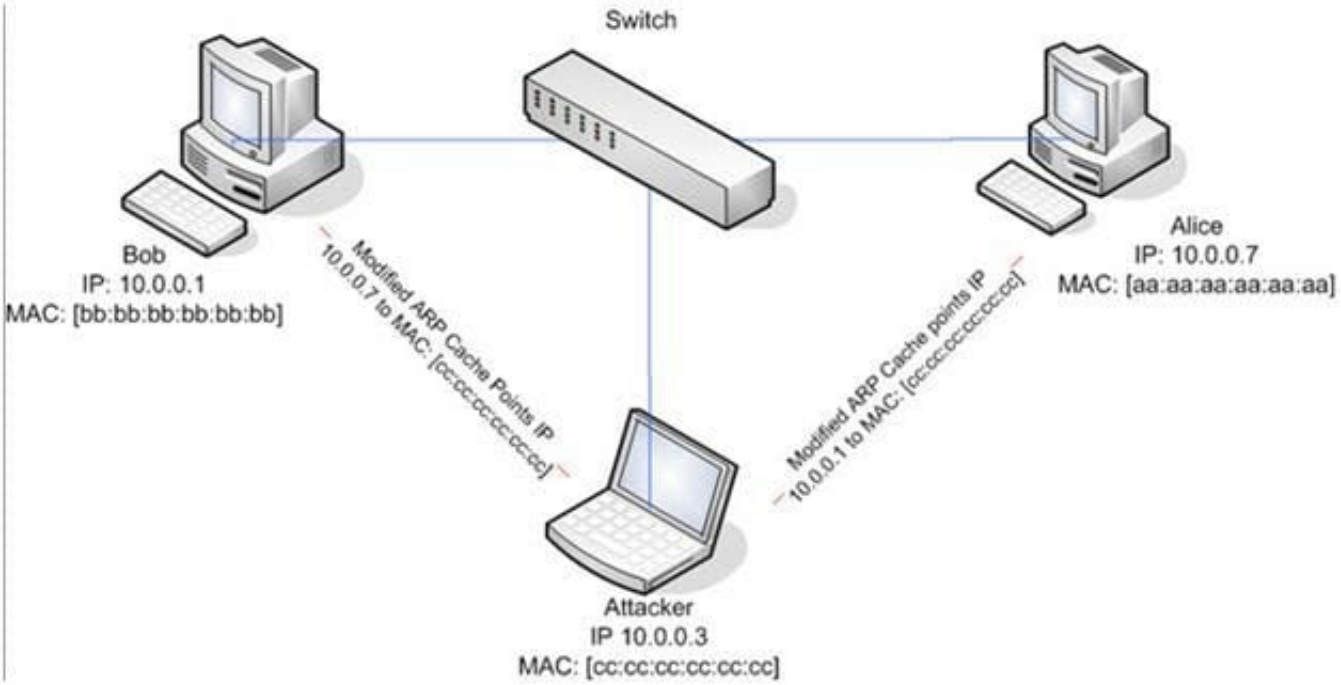
C. EMP

D. ABC

Correct Answer: C

QUESTION 2

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker\\'s MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead. ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?

A. Parameter Filtering

B. Social Engineering

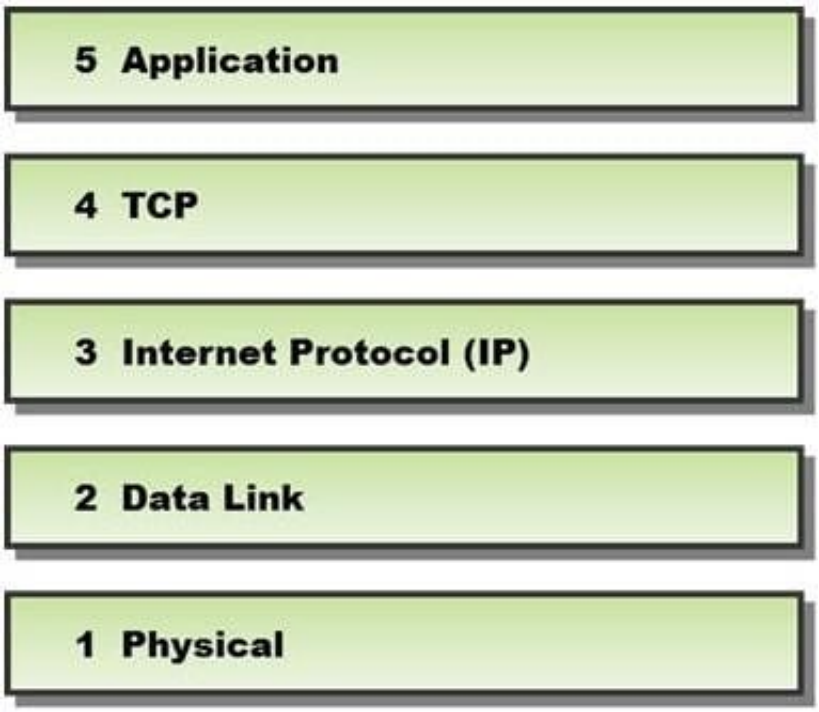
C. Input Validation

D. Session Hijacking

Correct Answer: D

QUESTION 3

In a TCP packet filtering firewall, traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer.



Identify the level up to which the unknown traffic is allowed into the network stack.

A. Level 5 Application

B. Level 2 Data Link

C. Level 4 TCP

D. Level 3 Internet Protocol (IP)

Correct Answer: D

QUESTION 4

Which of the following is not a condition specified by Hamel and Prahalad (1990)?

A. Core competency should be aimed at protecting company interests

B. Core competency is hard for competitors to imitate

C. Core competency provides customer benefits

D. Core competency can be leveraged widely to many products and markets

Correct Answer: A

QUESTION 5

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