ECSAV10$^{Q\&As}$

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/ecsav10.html

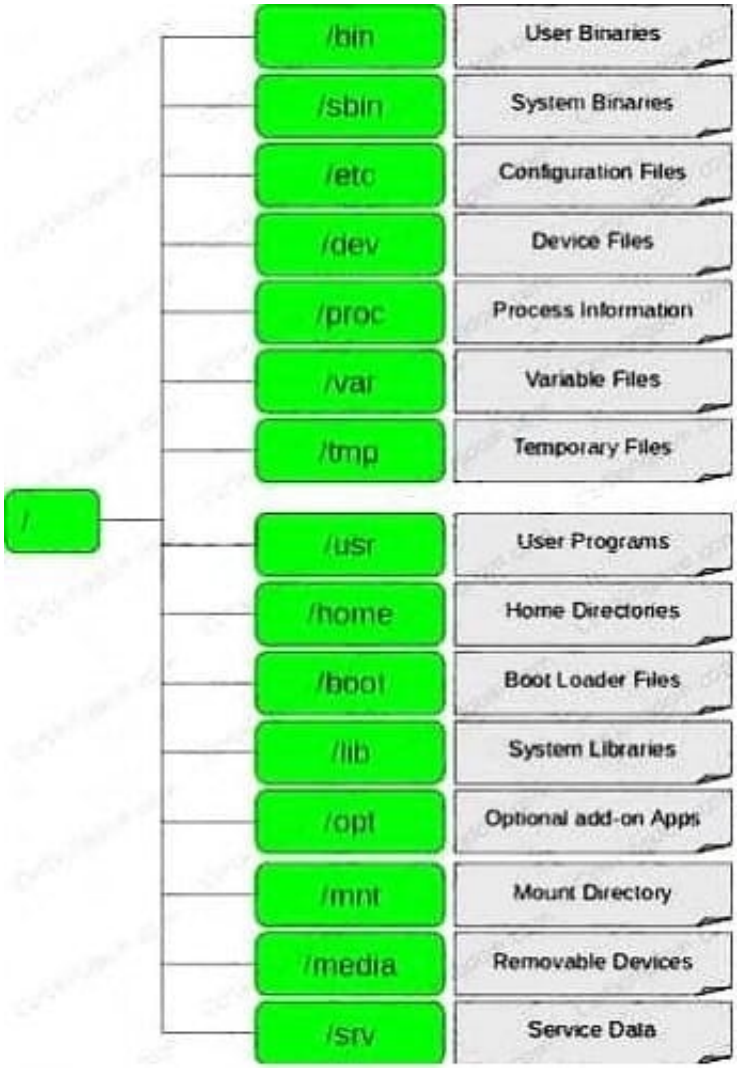
100% Passing Guarantee
100% Money Back Assurance

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

ESTION NO: 92 In Linux, /etc/shadow file stores the real password in encrypted format for user\\'s account with added properties associated with the user\\'s password.



In the example of a /etc/shadow file below, what does the bold letter string indicate? Vivek: 1fnffc$GteyHdicpGOfffXX40w#5:13064:0:99999:7

A. Number of days the user is warned before the expiration date

B. Minimum number of days required between password changes

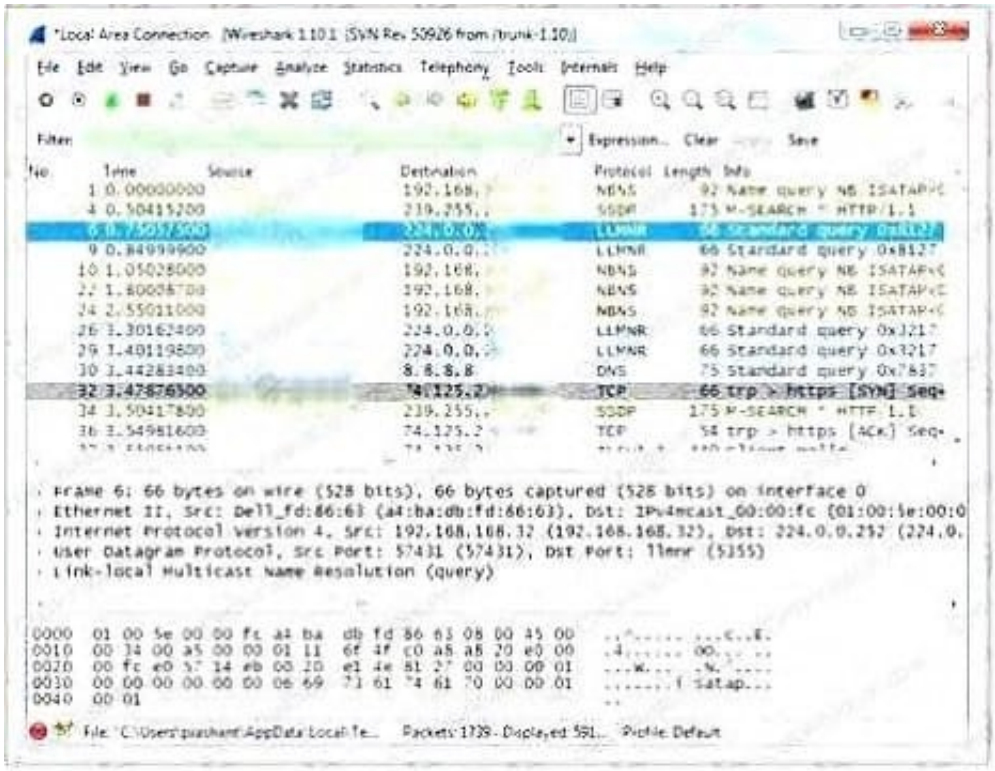
C. Maximum number of days the password is valid

D. Last password changed

Correct Answer: B

QUESTION 2

Which Wireshark filter displays all the packets where the IP address of the source host is 10.0.0.7?



A. ip.dst==10.0.0.7

B. ip.port==10.0.0.7

C. ip.src==10.0.0.7

D. ip.dstport==10.0.0.7

Correct Answer: C

QUESTION 3

George, an ex-employee of Netabb Ltd. with bruised feelings due to his layoff, tries to take revenge against the company. He randomly tried several attacks against the organization. As some of the employees used weak passwords to their user accounts, George was successful in cracking the user accounts of several employees with the help of a common passwords file. What type of password cracking attack did George perform?

A. Hybrid attack

B. Dictionary attack

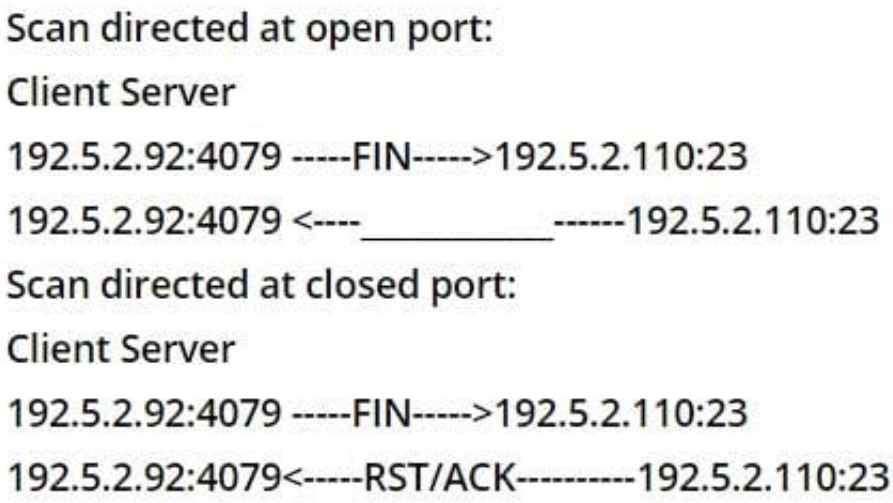
C. Brute forcing attack

D. Birthday attack

Correct Answer: B

QUESTION 4

As a part of the pen testing process, James performs a FIN scan as given below:



What will be the response if the port is open?

A. No response

B. FIN/RST

C. FIN/ACK

D. RST

Correct Answer: A

QUESTION 5

Today, most organizations would agree that their most valuable IT assets reside within applications and databases. Most would probably also agree that these are areas that have the weakest levels of security, thus making them the prime target for malicious activity from system administrators, DBAs, contractors, consultants, partners, and customers.

Which of the following flaws refers to an application using poorly written encryption code to securely encrypt and store sensitive data in the database and allows an attacker to steal or modify weakly protected data such as credit card numbers, SSNs, and other authentication credentials?

A. SSI injection attack

B. Insecure cryptographic storage attack

C. Hidden field manipulation attack

D. Man-in-the-Middle attack

Correct Answer: B

Latest ECSAV10 Dumps ECSAV10 VCE Dumps ECSAV10 Braindumps