# ECSAV10<sup>Q&As</sup>

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

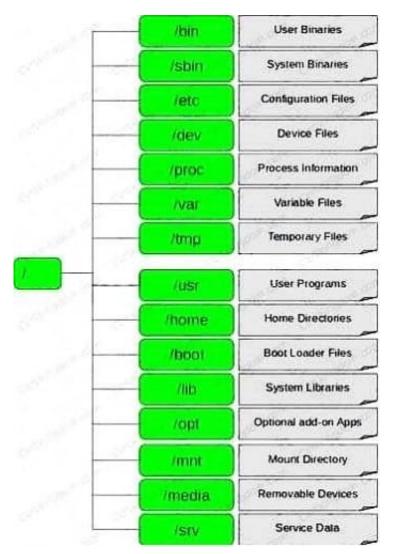
Leads4Pass

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: \$1\$fnffc\$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?

1000	Edit View Go Capture Analyze			and the second
0	· · · · Sex B	1. 0 10 GI 17 1	E) 3 Q,	0.5 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Filter			· Expression	Clear Save
40.	Trine Source	Dethalism	Protecul Le	and the second se
	1 0.00000000	192.168, >	NESS	92 NADE QUELY NO ISATAPHO
-	4 0.50415200	219.255	5504	173 M-SEARCH - HTTP/1.1
	9 0, 84939900	224.0.0	LUNNE	be scandard query Datu27
	10 1.05028000	192.168.	NBNS	66 Standard query 0x8127 92 Name query NE ISATAFYC
	22 1.80008700	192.168.	NENS	32 NAME QUELY NE ISATAPIC
	34 2.55011000	192.165.	NENS	92 Name Guery AD ISATAR-C
	26 1.30162400	224.0.0.2	LIMNE	
	29 1.40119800	224.0.0.	LLMAR	66 Standard query 0x3217
	10 1.44283400	8. 8. 8. 8	DNS	75 Standard query 0x7837
100	32 3.47876300	14(125,2)	TCP	66 trp > https [SyN] Seq.
	34 3,50417800	239.255	SODP	175 M-SEARCH " HTTF 1.1
	16 1.54981600	74.125.2	TEP	34 trp > https [ACK] Seq-
	57 3 ELOCHANS	TA + 14 1	+7 *1.8 *	the time matte
+ Ett	ternet Protocol version 4. er Datagram Protocol, Src P	63 (a4:ba:db:fd:66:63) Src: 192.168.168.32 (1 Ort: 57431 (57431), Ds	. DSt: 1Pu4 92.168.168.	<pre>mcast_60:00:fc (01:00:5e:00: 32), bst: 324.0.0.257 (224.0</pre>
1 4/54	nk-local Hulticast Name Res	anacian (dam'y)		
1 4/54	nk-local Hulticast Name Res	and the the garage		100

- 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:

Scan directed at open port:			
Client Server			
192.5.2.92:4079FIN>1	92.5.2.110:23		
192.5.2.92:4079 <	192.5.2.110:23		
Scan directed at closed port	:		
Client Server			
192.5.2.92:4079FIN>192.5.2.110:23			
192.5.2.92:4079 <rst ack<="" td=""><td>(192.5.2.110:23</td></rst>	(192.5.2.110:23		

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