

ECCouncil Computer Hacking Forensic Investigator (V9)

### Pass EC-COUNCIL 312-49 Exam with 100% Guarantee

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

https://www.leads4pass.com/312-49.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**

What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

- A. Disk deletion
- B. Disk cleaning
- C. Disk degaussing
- D. Disk magnetization

Correct Answer: C

#### **QUESTION 2**

Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri\\'s duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company\\'s switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Trick the switch into thinking it already has a session with Terri\\'s computer

- B. Poison the switch\\'s MAC address table by flooding it with ACK bits
- C. Crash the switch with a DoS attack since switches cannot send ACK bits D. Enable tunneling feature on the switch

Correct Answer: A

#### **QUESTION 3**

What must be obtained before an investigation is carried out at a location?

- A. Search warrant
- B. Subpoena
- C. Habeas corpus
- D. Modus operandi

#### **QUESTION 4**

What is the framework used for application development for iOS-based mobile devices?

A. Cocoa Touch

Correct Answer: A

- B. Dalvik
- C. Zygote
- D. AirPlay

Correct Answer: A

#### **QUESTION 5**

On Linux/Unix based Web servers, what privilege should the daemon service be run under?

- A. Guest
- B. Root
- C. You cannot determine what privilege runs the daemon service
- D. Something other than root
- Correct Answer: D

#### **QUESTION 6**

What file structure database would you expect to find on floppy disks?

- A. NTFS
- **B. FAT32**
- C. FAT16
- D. FAT12

Correct Answer: D

#### **QUESTION 7**

Which of the following statements is incorrect when preserving digital evidence?

- A. Verify if the monitor is in on, off, or in sleep mode
- B. Turn on the computer and extract Windows event viewer log files
- C. Remove the plug from the power router or modem
- D. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals

Correct Answer: B

#### **QUESTION 8**

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

- A. allinurl:"exchange/logon.asp"
- B. intitle:"exchange server"
- C. locate:"logon page"
- D. outlook:"search"

Correct Answer: A

#### **QUESTION 9**

How many bits is Source Port Number in TCP Header packet?

A. 16

- B. 32
- C. 48
- D. 64

Correct Answer: A

#### **QUESTION 10**

What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

- A. digital attack
- B. denial of service
- C. physical attack
- D. ARP redirect
- Correct Answer: B

#### **QUESTION 11**

When examining the log files from a Windows IIS Web Server, how often is a new log file created?

A. the same log is used at all times

B. a new log file is created everyday

- C. a new log file is created each week
- D. a new log is created each time the Web Server is started

Correct Answer: A

#### **QUESTION 12**

Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

- A. Record the system state by taking photographs of physical system and the display
- B. Perform data acquisition without disturbing the state of the systems
- C. Open the systems, remove the hard disk and secure it
- D. Switch off the systems and carry them to the laboratory

#### Correct Answer: A

#### **QUESTION 13**

Analyze the hex representation of mysql-bin.000013 file in the screenshot below. Which of the following will be an inference from this analysis?

3	3886	3	*	9 C	8		20		89 4	a <i>a</i> s,	2	0			~ #P	00	° %	۵ 🖃			
P	66 66 66	1.54		<b>%</b> (6	h	۵		Lega	cy ASC	30		*	101	4 >	101		×				
			0	1	2	3	4	5	6	7	8	9	A	в	С	012	34567	89ABC		Data Inspe 4	
П	0000005	A	21	00	08	0.0	77	6F	72	64	70	72	65	73	73	1	word	press	~	Data at of	fs
	000000F		0.0	49	4E	53	45	52	54	20	49	4E	54	4 F	20		SERT			int8	
	0000010		60	77	6F	72	64	70	72	65	73	73	60	2E	60			55		uint8	•
	0000011		77	70	SF	75	73	65	72	73	60	20	28	60	49		isers			int16	-
I	0000011	E	44	60	2C	20	60	75	73	65	72	SF	6C	6 F	67	D',	use			uint16	i
l	0000012		69	6E	60	2C	20	60	75	73	65	72	5F	70	61	in'		er pa		int32	
	0000013	8	73	73	60	2C	20	60	75	73	65	72	SF	6E	69	ss'		erni		uint32	
	0000014	5	63	65	6E	61	6D	65	60	2C	20	60	75	73	65	cena	ame`,			int64	1
	0000015	2	72	5F	65	6D	61	69	6C	60	2C	20	60	75	73	r er	nail'	, `us		uint64	1
	0000015	F	65	72	5F	73	74	61	74	75	73	60	2C	20	60	er s	statu	s', '		half float	1
	0000016	C	64	69	73	70	6C	61	79	5F	6E	61	6D	65	60	dis	play_	name`		float	
	0000017	9	29	20	56	41	4C	55	45	53	20	28	27	31	32			('12		double	
	0000018	6	33	27	2C	20	27	62	61	64	5F	67	75	79	27	3',	'bad	guy'		DATE	•
	0000019	3	2C	20	4D	44	35	28	27	68	61	63	6B	73	70	, MI	05('h	acksp		DOS date	
	000001A	0	69	72	69	74	27	29	2C	20	27	61	6E	6F	6E	irit	t'),	'anon		DOS time	i
	000001A	D	79	6D	6F	75	73	5F	68	61	63	6B	65	72	27	ymou	is_ha	cker'		<	>
	000001B	A	2C	20	27	62	61	64	67	75	79	40	61	62	63	, '}	badgu	y@abc		Expression #	
	0000010		2E	63	6F	6D	27	2C	20	27	30	27	2C	20	27	.cor	n', '	0', '		Signe v	3
	0000010		54	65	6D	70	20	55	73	65	72	27	29	86	5A	Temp	o Use	r').Z			_
	000001E		EA	56	10	01	00	00	00	1B	00	00	00	FA	01	. V.				4	
	0000011		0.0	0.0	0.0	00	5.9	00	0.0	0.0	0.0	0.0	0.0	0.0	A 17	-		~	<u></u>		-
	wp_users fr	miş	5 e	idata1	E	mysql-	bin.00.	1												Eval	

A. A user with username bad\_guy has logged into the WordPress web application

B. A WordPress user has been created with the username anonymous\_hacker

C. An attacker with name anonymous\_hacker has replaced a user bad\_guy in the WordPress database

D. A WordPress user has been created with the username bad\_guy

Correct Answer: D

#### **QUESTION 14**

To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

- A. Computer Forensics Tools and Validation Committee (CFTVC)
- B. Association of Computer Forensics Software Manufactures (ACFSM)
- C. National Institute of Standards and Technology (NIST)
- D. Society for Valid Forensics Tools and Testing (SVFTT)



Correct Answer: C

### **QUESTION 15**

Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.

### ex C:\WINDOW5\system32\cmd.exe

C:\>netstat -an

### Active Connections

Proto	Local Address	Foreign Address
TCP	0.0.0.0:135	0.0.0.0:0
TCP	0.0.0.0:242	0.0.0.0:0
TCP	0.0.0.0:445	0.0.0.0:0
TCP	0.0.0.0:990	0.0.0.0:0
TCP	0.0.0.0:2584	0.0.0.0:0
TCP	0.0.0.0:2585	0.0.0.0:0
TCP	0.0.0.0:2967	0.0.0.0:0
TCP	0.0.0.0:3389	0.0.0.0:0
TCP	0.0.0.0:12174	0.0.0.0:0
TCP	0.0.0.0:38292	0.0.0.0:0
TCP	127.0.0.1:242	127.0.0.1:1042
TCP	127.0.0.1:1042	127.0.0.1:242
TCP	127.0.0.1:1044	0.0.0.0:0
TCP	127.0.0.1:1046	0.0.0.0:0
TCP	127.0.0.1:1078	0.0.0.0:0
TCP	127.0.0.1:2584	127.0.0.1:2909
TCP	127.0.0.1:2909	127.0.0.1:2584
TCP	127.0.0.1:5679	0.0.0.0
TCP	127.0.0.1:7438	0.0.0.0:0
TCP	172.16.28.75:139	0.0.0.0:0
TCP	172.16.28.75:1067	172.16.28.102:445
TCP	172.16.28.75:1071	172.16.28.103:139
TCP	172.16.28.75:1116	172.16.28.102:1026
TCP	172.16.28.75:1135	172.16.28.101:389
TCP	172.16.28.75:1138	172.16.28.104:445
TCP	172.16.28.75:1148	172.16.28.101:389
TCP	172.16.28.75:1610	172.16.28.101:139
TCP	172.16.28.75:2589	172.16.28.101:389
TCP	172.16.28.75:2793	172.16.28.106:445
TCP	172.16.28.75:3801	172.16.28.104:1148
TCP	172.16.28.75:3890	172.16.28.104:135
TCP	172.16.28.75:3891	172.16.28.104:1056
TCP	172.16.28.75:3892	172.16.28.104:1155
TCP	172.16.28.75:3893	172.16.28.102:135
TCP	172.16.28.75:3896	172.16.28.101:135
TCP	172.16.28.75:3899	172.16.28.104:135
ICP	172.16.28.75:3900	172.16.28.104:1056
TCP	172.16.28.75:3901	172.16.28.104-1155

He runs the netstat command on the machine to see its current connections. In the following screenshot, what do the 0.0.0.0 IP addresses signify?

- A. Those connections are established
- B. Those connections are in listening mode



- C. Those connections are in closed/waiting mode
- D. Those connections are in timed out/waiting mode

Correct Answer: B

Latest 312-49 Dumps

312-49 VCE Dumps

312-49 Practice Test