312-49V8^Q&As

Computer Hacking Forensic Investigator Exam

Pass EC-COUNCIL 312-49V8 Exam with 100% Guarantee

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

https://www.leads4pass.com/312-49v8.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Graphics Interchange Format (GIF) is a _____RGB bitmap Image format for Images with up to 256 distinct colors per frame.

A. 8-bit

B. 16-bit

C. 24-bit

D. 32-bit

Correct Answer: A

QUESTION 2

Which device in a wireless local area network (WLAN) determines the next network point to which a packet should be forwarded toward its destination?

A. Wireless router

B. Wireless modem

C. Antenna

D. Mobile station

Correct Answer: A

QUESTION 3

In what circumstances would you conduct searches without a warrant?

A. When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity

B. Agents may search a place or object without a warrant if he suspect the crime was committed C. A search warrant is not required if the crime involves Denial-Of-Service attack over the Internet

D. Law enforcement agencies located in California under section SB 567 are authorized to seize computers without warrant under all circumstances

Correct Answer: A

QUESTION 4

A steganographic file system is a method to store the files in a way that encrypts and hides the data without the knowledge of others

A. True

B. False

Correct Answer: A

QUESTION 5

Why is it Important to consider health and safety factors in the work carried out at all stages of the forensic process conducted by the forensic analysts?

A. This is to protect the staff and preserve any fingerprints that may need to be recovered at a later date

B. All forensic teams should wear protective latex gloves which makes them look professional and cool

C. Local law enforcement agencies compel them to wear latest gloves

D. It is a part of ANSI 346 forensics standard

Correct Answer: A

QUESTION 6

Cyber-crime is defined as any Illegal act involving a gun, ammunition, or its applications.

A. True

B. False

Correct Answer: B

QUESTION 7

All the Information about the user activity on the network, like details about login and logoff attempts, is collected in the security log of the computer. When a user\\'s login is successful, successful audits generate an entry whereas unsuccessful audits generate an entry for failed login attempts in the logon event ID table.

In the logon event ID table, which event ID entry (number) represents a successful logging on to a computer?

A. 528

B. 529

C. 530

D. 531

Correct Answer: A

QUESTION 8

What is cold boot (hard boot)?

A. It is the process of starting a computer from a powered-down or off state

B. It is the process of restarting a computer that is already turned on through the operating system

C. It is the process of shutting down a computer from a powered-on or on state

D. It is the process of restarting a computer that is already in sleep mode

Correct Answer: A

QUESTION 9

What is static executable file analysis?

A. It is a process that consists of collecting information about and from an executable file without actually launching the file under any circumstances

B. It is a process that consists of collecting information about and from an executable file by launching the file under any circumstances

C. It is a process that consists of collecting information about and from an executable file without actually launching an executable file in a controlled and monitored environment

D. It is a process that consists of collecting information about and from an executable file by launching an executable file in a controlled and monitored environment

Correct Answer: A

QUESTION 10

Wi-Fi Protected Access (WPA) is a data encryption method for WLANs based on 802.11 standards. Temporal Key Integrity Protocol (TKIP) enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. Temporal keys are changed for every_____.

A. 5,000 packets

B. 10.000 packets

C. 15,000 packets

D. 20.000 packets

Correct Answer: B

QUESTION 11

Which of the following commands shows you the NetBIOS name table each?

A. nbtstat -n

B. nbtstat -c

C. nbtstat -r

D. nbtstat -s

Correct Answer: A

QUESTION 12

When a system is compromised, attackers often try to disable auditing, in Windows 7; modifications to the audit policy are recorded as entries of Event ID_____.

A. 4902

B. 3902

C. 4904

D. 3904

Correct Answer: A

QUESTION 13

Which table is used to convert huge word lists (i .e. dictionary files and brute-force lists) into password hashes?

A. Rainbow tables

B. Hash tables

C. Master file tables

D. Database tables

Correct Answer: A

QUESTION 14

What is the goal of forensic science?

A. To determine the evidential value of the crime scene and related evidence

B. Mitigate the effects of the information security breach

C. Save the good will of the investigating organization

D. It is a disciple to deal with the legal processes

Correct Answer: A

QUESTION 15

Which of the following Steganography techniques allows you to encode information that ensures creation of cover for secret communication?

A. Substitution techniques

B. Transform domain techniques

C. Cover generation techniques

D. Spread spectrum techniques

Correct Answer: C