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.passapply.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

Which of the following file in Novel GroupWise stores information about user accounts?

A. ngwguard.db

B. gwcheck.db

C. PRIV.EDB

D. PRIV.STM

Correct Answer: A

QUESTION 2

Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion \ProfileList

B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \NetworkList

C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentsVersion \setup

D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule

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

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 5

Data compression involves encoding the data to take up less storage space and less bandwidth for transmission. It helps in saving cost and high data manipulation in many business applications.

Which data compression technique maintains data integrity?

A. Lossless compression

B. Lossy compression

C. Speech encoding compression

D. Lossy video compression

Correct Answer: A

QUESTION 6

JPEG is a commonly used method of compressing photographic Images. It uses a compression algorithm to minimize the size of the natural image, without affecting the quality of the image. The JPEG lossy algorithm divides the image in separate blocks of_____.

A. 4x4 pixels

B. 8x8 pixels

C. 16x16 pixels

D. 32x32 pixels

Correct Answer: B

QUESTION 7

Networks are vulnerable to an attack which occurs due to overextension of bandwidth, bottlenecks,

network data interception, etc.

Which of the following network attacks refers to a process in which an attacker changes his or her IP

address so that he or she appears to be someone else?

A. IP address spoofing

B. Man-in-the-middle attack

C. Denial of Service attack

D. Session sniffing

Correct Answer: A

QUESTION 8

Attackers can manipulate variables that reference files with "dot-dot-slash (./)" sequences and their

variations such as http://www.juggyDoy.corn/GET/process.php././././././././etc/passwd.

Identify the attack referred.

A. Directory traversal

B. SQL Injection

C. XSS attack

D. File injection

Correct Answer: A

QUESTION 9

Which one of the following is not a consideration in a forensic readiness planning checklist?

A. Define the business states that need digital evidence

B. Identify the potential evidence available

C. Decide the procedure for securely collecting the evidence that meets the requirement fn a forensically sound manner

D. Take permission from all employees of the organization

Correct Answer: D

QUESTION 10

SIM is a removable component that contains essential information about the subscriber. It has both volatile and non-volatile memory. The file system of a SIM resides in _____ memory.

A. Volatile

B. Non-volatile

Correct Answer: B

QUESTION 11

The evolution of web services and their increasing use in business offers new attack vectors in an application framework. Web services are based on XML protocols such as web Services Definition Language (WSDL) for describing the connection points, Universal Description, Discovery, and Integration (UDDI) for the description and discovery of Web services and Simple Object Access Protocol (SOAP) for communication between Web services that are vulnerable to various web application threats. Which of the following layer in web services stack is vulnerable to fault code leaks?

A. Presentation Layer

B. Security Layer

C. Discovery Layer

D. Access Layer

Correct Answer: C

QUESTION 12

Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where, "X" represents the _____.

A. Drive name

B. Sequential number

C. Original file name\\'s extension

D. Original file name

Correct Answer: A

QUESTION 13

First response to an incident may involve three different groups of people, and each will have differing skills and need to carry out differing tasks based on the incident. Who is responsible for collecting, preserving, and packaging electronic evidence?

A. System administrators

B. Local managers or other non-forensic staff

C. Forensic laboratory staff

D. Lawyers

Correct Answer: C

QUESTION 14

Computer security logs contain information about the events occurring within an organization\\'s systems and networks. Application and Web server log files are useful in detecting web attacks. The source, nature, and time of the attack can be determined by _____of the compromised system.

A. Analyzing log files

B. Analyzing SAM file

C. Analyzing rainbow tables

D. Analyzing hard disk boot records

Correct Answer: A

QUESTION 15

Who is responsible for the following tasks?

A. Non-Laboratory Staff

B. System administrators

C. Local managers or other non-forensic staff

D. Lawyers

Correct Answer: A