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.pass2lead.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 is not a part of data acquisition forensics Investigation?

A. Permit only authorized personnel to access

B. Protect the evidence from extremes in temperature

C. Work on the original storage medium not on the duplicated copy

D. Disable all remote access to the system

Correct Answer: C

QUESTION 2

Wireless network discovery tools use two different methodologies to detect, monitor and log a WLAN device (i.e. active scanning and passive scanning). Active scanning methodology involves _____and waiting for responses from available wireless networks.

A. Broadcasting a probe request frame

B. Sniffing the packets from the airwave

C. Scanning the network

D. Inspecting WLAN and surrounding networks

Correct Answer: A

QUESTION 3

In which step of the computer forensics investigation methodology would you run MD5 checksum on the evidence?

A. Obtain search warrant

B. Evaluate and secure the scene

C. Collect the evidence

D. Acquire the data

Correct Answer: D

QUESTION 4

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 5

An Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Which of the following statement is true for NTP Stratum Levels?

A. Stratum-0 servers are used on the network; they are not directly connected to computers which then operate as stratum-1 servers

B. Stratum-1 time server is linked over a network path to a reliable source of UTC time such as GPS, WWV, or CDMA transmissions

C. A stratum-2 server is directly linked (not over a network path) to a reliable source of UTC time such as GPS, WWV, or CDMA transmissions

D. A stratum-3 server gets its time over a network link, via NTP, from a stratum-2 server, and so on

Correct Answer: D

QUESTION 6

Digital evidence validation involves using a hashing algorithm utility to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a disk drive or file. Which of the following hash algorithms produces a message digest that is 128 bits long?

A. CRC-32

B. MD5

C. SHA-1

D. SHA-512

Correct Answer: B

QUESTION 7

Smith, an employee of a reputed forensic Investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in hacking of organization DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry key Smith will check to find the above information?

A. UserAssist Key

B. MountedDevices key

C. RunMRU key

D. TypedURLs key

Correct Answer: C

QUESTION 8

Which of the following commands shows you the username and IP address used to access the system via a remote login session and the Type of client from which they are accessing the system?

A. Net sessions

B. Net file

C. Net config

D. Net share

Correct Answer: A

QUESTION 9

Tracks numbering on a hard disk begins at 0 from the outer edge and moves towards the center, typically reaching a value of _____.

A. 1023

B. 1020

C. 1024

D. 2023

Correct Answer: A

QUESTION 10

Which of the following commands shows you all of the network services running on Windows-based servers?

A. Net start

B. Net use

C. Net Session

D. Net share

Correct Answer: A

QUESTION 11

Which of the following is not a part of the technical specification of the laboratory-based imaging system?

A. High performance workstation PC

B. Remote preview and imaging pod

C. Anti-repudiation techniques

D. very low image capture rate

Correct Answer: D

QUESTION 12

Digital evidence is not fragile in nature.

A. True

B. False

Correct Answer: B

QUESTION 13

Identify the attack from following sequence of actions? Step 1: A user logs in to a trusted site and creates a new session Step 2: The trusted site stores a session identifier for the session in a cookie in the web browser Step 3: The user is tricked to visit a malicious site Step 4: the malicious site sends a request from the user\\'s browser using his session cookie

A. Web Application Denial-of-Service (DoS) Attack

B. Cross-Site Scripting (XSS) Attacks

C. Cross-Site Request Forgery (CSRF) Attack

D. Hidden Field Manipulation Attack

Correct Answer: C

QUESTION 14

Quality of a raster Image is determined by the _____and the amount of information in each pixel.

A. Total number of pixels

B. Image file format

C. Compression method

D. Image file size

Correct Answer: A

QUESTION 15

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