312-49V10 Q&As

ECCouncil Computer Hacking Forensic Investigator (V10)

Pass EC-COUNCIL 312-49V10 Exam with 100% Guarantee

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

https://www.pass2lead.com/312-49v10.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
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following is an iOS Jailbreaking tool?

A. Kingo Android ROOT

B. Towelroot

C. One Click Root

D. Redsn0w

Correct Answer: D

QUESTION 2

An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

A. Name of the Database

B. Name of SQL Server

C. Operating system of the system

D. Network credentials of the database

Correct Answer: B

QUESTION 3

The objective of this act was to protect consumers personal financial information held by financial institutions and their service providers.

A. HIPAA

B. Sarbanes-Oxley 2002

C. California SB 1386

D. Gramm-Leach-Bliley Act

Correct Answer: D

QUESTION 4

Where is the default location for Apache access logs on a Linux computer?

A. usr/local/apache/logs/access_log

B. bin/local/home/apache/logs/access_log

C. usr/logs/access_log

D. logs/usr/apache/access_log

Correct Answer: A

QUESTION 5

BMP (Bitmap) is a standard file format for computers running the Windows operating system. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains a header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?

A. Information header

B. Image data

C. The RGBQUAD array

D. Header

Correct Answer: A

QUESTION 6

Which type of attack is possible when attackers know some credible information about the victim\\'s password, such as the password length, algorithms involved, or the strings and characters used in its creation?

A. Rule-Based Attack

B. Brute-Forcing Attack

C. Dictionary Attack

D. Hybrid Password Guessing Attack

Correct Answer: A

Reference: https://info-savvy.com/password-cracking-techniques/#:~:text=Attackers%20use%20the%20rule%2Dbased,characters%20used%20in%20its%20creation

QUESTION 7

John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they shouldJohn is working on his company? policies and guidelines. The section he is currently

working on covers company documents; how they should be handled, stored, and eventually destroyed. John is concerned about the process whereby outdated documents are destroyed. What type of shredder should John write in the guidelines to be used when destroying documents?

A. Strip-cut shredder

B. Cross-cut shredder

C. Cross-hatch shredder

D. Cris-cross shredder

Correct Answer: B

QUESTION 8

George is a senior security analyst working for a state agency in Florida. His state\\'s congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used. What IDS feature must George implement to meet this requirement?

A. Pattern matching

B. Statistical-based anomaly detection

C. Real-time anomaly detection

D. Signature-based anomaly detection

Correct Answer: C

QUESTION 9

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 10

Why should you never power on a computer that you need to acquire digital evidence from?

A. When the computer boots up, files are written to the computer rendering the data nclean?When the computer boots up, files are written to the computer rendering the data ?nclean

B. When the computer boots up, the system cache is cleared which could destroy evidence

C. When the computer boots up, data in the memory buffer is cleared which could destroy evidenceWhen the computer boots up, data in the memory? buffer is cleared which could destroy evidence

D. Powering on a computer has no affect when needing to acquire digital evidence from it

Correct Answer: A

QUESTION 11

The process of restarting a computer that is already turned on through the operating system is called?

A. Warm boot

B. Ice boot

C. Hot Boot

D. Cold boot

Correct Answer: A

QUESTION 12

If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?

A. Lossful compression

B. Lossy compression

C. Lossless compression

D. Time-loss compression

Correct Answer: B

QUESTION 13

Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?

A. pstree

B. pgrep

C. ps

D. grep

Correct Answer: B

Reference: https://askubuntu.com/questions/180336/how-to-find-the-process-id-pid-of-a-running-terminalprogram

QUESTION 14

The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux. Identify the Apache error log from the following logs.

A. http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..% c0% af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1

B. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/ home/live/ap/htdocs/test

C. 127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]"GET /apache_pb.gif HTTP/1.0" 200 2326 D. 127.0.0.1 - - [10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0" 200 2326

Correct Answer: B

QUESTION 15

What does the part of the log, “% SEC-6-IPACCESSLOGP”, extracted from a Cisco router represent?

A. The system was not able to process the packet because there was not enough room for all of the desired IP header options

B. Immediate action required messages

C. Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available

D. A packet matching the log criteria for the given access list has been detected (TCP or UDP)

Correct Answer: D