312-49^{Q&As}

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.certbus.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

⚙ **800,000+** Satisfied Customers

QUESTION 1

Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

A. A text file deleted from C drive in sixth sequential order

B. A text file deleted from C drive in fifth sequential order

C. A text file copied from D drive to C drive in fifth sequential order

D. A text file copied from C drive to D drive in fifth sequential order

Correct Answer: B

QUESTION 2

While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface. Which of the following operating systems is present on the hard disk?

A. Windows 10

B. Windows 8

C. Windows 7

D. Windows 8.1

Correct Answer: C

QUESTION 3

What will the following command accomplish? dd if=/dev/xxx of=mbr.backup bs=512 count=1

A. Back up the master boot record

B. Restore the master boot record

C. Mount the master boot record on the first partition of the hard drive

D. Restore the first 512 bytes of the first partition of the hard drive

Correct Answer: A

QUESTION 4

Software firewalls work at which layer of the OSI model?

A. Application

B. Network

C. Transport

D. Data Link

Correct Answer: D

QUESTION 5

Which of the following should a computer forensics lab used for investigations have?

A. isolation

B. restricted access

C. open access

D. an entry log

Correct Answer: B

QUESTION 6

You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a "simple backup copy" of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a "simple backup copy" will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

A. Robust copy

B. Incremental backup copy

C. Bit-stream copy

D. Full backup copy

Correct Answer: C

QUESTION 7

Rusty, a computer forensics apprentice, uses the command nbtstat ? while analyzing the network information in a suspect system. What information is he looking for?

A. Contents of the network routing table

B. Status of the network carrier

C. Contents of the NetBIOS name cache

D. Network connections

Correct Answer: C

QUESTION 8

You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position: 7+ years experience in Windows Server environment 5+ years experience in Exchange 2000/2003 environment Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired, MCSE, CEH preferred No Unix/Linux Experience needed What is this information posted on the job website considered?

A. Social engineering exploit

B. Competitive exploit

C. Information vulnerability

D. Trade secret

Correct Answer: C

QUESTION 9

Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?

A. File fingerprinting

B. Identifying file obfuscation

C. Static analysis

D. Dynamic analysis

Correct Answer: A

QUESTION 10

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city\\'s network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

A. Router Penetration Testing

B. DoS Penetration Testing

C. Firewall Penetration Testing

D. Internal Penetration Testing

Correct Answer: B

QUESTION 11

Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

A. Three

B. One

C. Two

D. Four

Correct Answer: B

QUESTION 12

You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

A. Net sessions

B. Net config

C. Net share

D. Net use

Correct Answer: D

QUESTION 13

Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?

A. 18 U.S.C. 1029

B. 18 U.S.C. 1362

C. 18 U.S.C. 2511

D. 18 U.S.C. 2703

Correct Answer: A

QUESTION 14

Item 2If you come across a sheepdip machine at your client site, what would you infer?

A. A sheepdip coordinates several honeypots

B. A sheepdip computer is another name for a honeypot

C. A sheepdip computer is used only for virus-checking.

D. A sheepdip computer defers a denial of service attack

Correct Answer: C

QUESTION 15

Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

A. Swap space

B. Application data

C. Files and documents

D. Slack space

Correct Answer: A

Latest 312-49 Dumps   312-49 Practice Test   312-49 Braindumps