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.leads4pass.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

QUESTION 1

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 which sessions the machine has opened with other systems?

A. Net sessions

B. Net use

C. Net config

D. Net share

Correct Answer: B

QUESTION 2

What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

A. Copyright

B. Design patent

C. Trademark

D. Utility patent

Correct Answer: D

QUESTION 3

When investigating a wireless attack, what information can be obtained from the DHCP logs?

A. The operating system of the attacker and victim computersThe operating system of the attacker and victim? computers

B. IP traffic between the attacker and the victim

C. MAC address of the attacker If any computers on the network are running in promiscuous mode

Correct Answer: C

QUESTION 4

Why is it a good idea to perform a penetration test from the inside?

A. It is never a good idea to perform a penetration test from the inside

B. It is easier to hack from the inside

C. Because 70% of attacks are from inside the organization

D. To attack a network from a hacker\\'s perspective

Correct Answer: C

QUESTION 5

Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest. Which of the following acts does the email breach?

A. CAN-SPAM Act

B. HIPAA

C. GLBA

D. SOX

Correct Answer: A

QUESTION 6

When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

A. UTC

B. PTP

C. Time Protocol

D. NTP

Correct Answer: D

QUESTION 7

An investigator has extracted the device descriptor for a 1GB thumb drive that looks like: DiskandVen_Best_BuyandProd_Geek_Squad_U3andRev_6.15. What does the “Geek_Squad” part represent?

A. Product description

B. Manufacturer Details

C. Developer description

D. Software or OS used

Correct Answer: A

QUESTION 8

Windows Security Event Log contains records of login/logout activity or other security- related events specified by the system\\'s audit policy. What does event ID 531 in Windows Security Event Log indicates?

A. A user successfully logged on to a computer

B. The logon attempt was made with an unknown user name or a known user name with a bad password

C. An attempt was made to log on with the user account outside of the allowed time

D. A logon attempt was made using a disabled account

Correct Answer: D

QUESTION 9

The offset in a hexadecimal code is:

A. The 0x at the beginning of the code

B. The 0x at the end of the code

C. The first byte after the colon

D. The last byte after the colon

Correct Answer: A

QUESTION 10

Where should the investigator look for the Edge browser\\'s browsing records, including history, cache, and cookies?

A. ESE Database

B. Virtual Memory

C. Sparse files

D. Slack Space

Correct Answer: A

QUESTION 11

Depending upon the Jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

A. 18 USC 7029

B. 18 USC 7030

C. 18 USC 7361

D. 18 USC 7371

Correct Answer: B

QUESTION 12

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 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. Header

B. The RGBQUAD array

C. Information header

D. Image data

Correct Answer: B

QUESTION 13

Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?

A. gif

B. bmp

C. jpeg

D. png

Correct Answer: C

QUESTION 14

A. Snort

B. Airsnort

C. Ettercap

D. RaidSniff

Correct Answer: C

QUESTION 15

Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

A. netstat – r

B. netstat – ano

C. netstat – b

D. netstat – s

Correct Answer: B