

# 312-49V10<sup>Q&As</sup>

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.passapply.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



# https://www.passapply.com/312-49v10.html 2024 Latest passapply 312-49V10 PDF and VCE dumps Download

QUESTION 1
Which response organization tracks hoaxes as well as viruses?
A. NIPC
B. FEDCIRC
C. CERT
D. CIAC
Correct Answer: D
QUESTION 2
What is one method of bypassing a system BIOS password?
A. Removing the processor
B. Removing the CMOS battery
C. Remove all the system memoryRemove all the system? memory
D. Login to Windows and disable the BIOS password
Correct Answer: B
QUESTION 3
A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker. Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt.
(Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.) 03/15-20:21:24.107053 211.185.125.124:3500 -: 172.16.1.108:111 TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF ***A**** Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32 TCP Options (3) => NOP NOP TS: 23678634 2878772 =+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111 UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84 Len: 64
01 0A 8A 0A 00 00 00 00 00 00 00 01 86 A0
00 00 00 02 00 00 03 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01
00 00 00 11 00 00 00 00



2024 Latest passapply 312-49V10 PDF and VCE dumps Download

69 64 3B id;

A. The attacker has conducted a network sweep on port 111

63 64 20 2F 3B 20 75 6E 61 6D 65 20 2D 61 3B 20 cd /; uname -a;

- B. The attacker has scanned and exploited the system using Buffer Overflow
- C. The attacker has used a Trojan on port 32773
- D. The attacker has installed a backdoor

Correct Answer: A

#### **QUESTION 4**

Which principle states that "anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave"?

- A. Locard\\'s Exchange Principle
- B. Enterprise Theory of Investigation
- C. Locard\\'s Evidence Principle
- D. Evidence Theory of Investigation

Correct Answer: A

2024 Latest passapply 312-49V10 PDF and VCE dumps Download

QUESTION 5			

Hard disk data addressing is a method of allotting addresses to each of data on a hard disk.
A. Physical block
B. Operating system block
C. Hard disk block
D. Logical block
Correct Answer: A
QUESTION 6
Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in the mobile device. Smith found that the SIM was protected by a Personal Identification Number (PIN) code, but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?
A. He should contact the network operator for a Temporary Unlock Code (TUK)
B. Use system and hardware tools to gain access
C. He can attempt PIN guesses after 24 hours
D. He should contact the network operator for Personal Unlock Number (PUK)
Correct Answer: D
QUESTION 7

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

2024 Latest passapply 312-49V10 PDF and VCE dumps Download

Correct Answer: B

#### **QUESTION 8**

Which of the following statements is incorrect when preserving digital evidence?

- A. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals
- B. Verily if the monitor is in on, off, or in sleep mode
- C. Remove the power cable depending on the power state of the computer i.e., in on. off, or in sleep mode
- D. Turn on the computer and extract Windows event viewer log files

Correct Answer: D

#### **QUESTION 9**

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe.

What are you trying to accomplish here?

- A. Enumerate domain user accounts and built-in groups
- B. Enumerate MX and A records from DNS
- C. Establish a remote connection to the Domain Controller
- D. Poison the DNS records with false records

Correct Answer: A

#### **QUESTION 10**

Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

- A. Simple Network Management Protocol
- B. Cisco Discovery Protocol
- C. Border Gateway Protocol
- D. Broadcast System Protocol



2024 Latest passapply 312-49V10 PDF and VCE dumps Download

Correct Answer: B

#### **QUESTION 11**

Which of the following tools is not a data acquisition hardware tool?

- A. UltraKit
- B. Atola Insight Forensic
- C. F-Response Imager
- D. Triage-Responder

Correct Answer: C

#### **QUESTION 12**

What is the size value of a nibble?

- A. 0.5 kilo byte
- B. 0.5 bit
- C. 0.5 byte
- D. 2 bits

Correct Answer: C

#### **QUESTION 13**

Self-Monitoring, Analysis, and Reporting Technology (SMART) is built into the hard drives to monitor and report system activity. Which of the following is included in the report generated by SMART?

- A. Power Off time
- B. Logs of high temperatures the drive has reached
- C. All the states (running and discontinued) associated with the OS
- D. List of running processes

Correct Answer: B

Reference: https://www.hdsentinel.com/smart/index.php

#### https://www.passapply.com/312-49v10.html 2024 Latest passapply 312-49V10 PDF and VCE dumps Download

# **QUESTION 14**

What does the acronym POST mean as it relates to a PC?

- A. Power On Self Test
- B. Pre Operational Situation Test
- C. Primary Operating System Test
- D. Primary Operations Short Test

Correct Answer: A

#### **QUESTION 15**

You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?

- A. The X509 Address
- B. The SMTP reply Address
- C. The E-mail Header
- D. The Host Domain Name

Correct Answer: C

312-49V10 VCE Dumps

312-49V10 Practice Test

<u>312-49V10 Braindumps</u>