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

Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

A. Model.log

B. Model.txt

C. Model.ldf

D. Model.lgf

Correct Answer: C

QUESTION 2

Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

A. Record the system state by taking photographs of physical system and the display

B. Perform data acquisition without disturbing the state of the systems

C. Open the systems, remove the hard disk and secure it

D. Switch off the systems and carry them to the laboratory

Correct Answer: A

QUESTION 3

Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?

A. C: $Recycled.Bin

B. C: \$Recycle.Bin

C. C:\RECYCLER

D. C:\$RECYCLER

Correct Answer: B

QUESTION 4

Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?

A. International Mobile Equipment Identifier (IMEI)

B. Integrated circuit card identifier (ICCID)

C. International mobile subscriber identity (IMSI)

D. Equipment Identity Register (EIR)

Correct Answer: A

QUESTION 5

What file structure database would you expect to find on floppy disks?

A. NTFS

B. FAT32

C. FAT16

D. FAT12

Correct Answer: D

QUESTION 6

International Mobile Equipment Identifier (IMEI) is a 15-dlgit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

A. Type Allocation Code (TAC)

B. Device Origin Code (DOC)

C. Manufacturer identification Code (MIC)

D. Integrated Circuit Code (ICC)

Correct Answer: A

QUESTION 7

Which of the following files gives information about the client sync sessions in Google Drive on Windows?

A. sync_log.log

B. Sync_log.log

C. sync.log

D. Sync.log

Correct Answer: B

QUESTION 8

Checkpoint Firewall logs can be viewed through a Check Point Log viewer that uses icons and colors in the log table to represent different security events and their severity. What does the icon in the checkpoint logs represent?

A. The firewall rejected a connection

B. A virus was detected in an email

C. The firewall dropped a connection

D. An email was marked as potential spam

Correct Answer: C

QUESTION 9

Digital evidence is not fragile in nature.

A. True

B. False

Correct Answer: B

QUESTION 10

In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
         Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
        by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTP id 151EfCEh032241
        for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
         Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewherelese.com>
MIME-Version: 1.0
```

A. Somedomain.com

B. Smtp1.somedomain.com

C. Simon1.state.ok.gov.us

D. David1.state.ok.gov.us

Correct Answer: C

QUESTION 11

Damaged portions of a disk on which no read/Write operation can be performed is known as ______________.

A. Lost sector

B. Bad sector

C. Empty sector

D. Unused sector

Correct Answer: B

QUESTION 12

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 02 00 01 86 A0 .....

00 00 00 02 00 00 00 03 00 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 .....

=+= +=

03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773

UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104

Len: 1084

47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8 G..c.....

00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 20 .....

3A B1 5E E5 00 00 00 09 6C 6F 63 61 6C 68 6F 73 :.^.....localhost

=+= +=+=+

03/15-20:21:36.539731 211.185.125.124:4450 -> 172.16.1.108:39168

TCP TTL:43 TOS:0x0 ID:31660 IpLen:20 DgmLen:71 DF

AP Seq: 0x9C6D2BFF Ack: 0x59606333 Win: 0x7D78 TcpLen: 32

TCP Options (3) => NOP NOP TS: 23679878 2880015

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

69 64 3B id;

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

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 13

Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_CONFIG

C. HKEY_LOCAL_MACHINE

D. HKEY_USERS

Correct Answer: A

QUESTION 14

Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

A. Accunetix

B. Nikto

C. Snort

D. Kismet

Correct Answer: C

QUESTION 15

Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

A. FAT File System

B. ReFS

C. exFAT

D. NTFS File System

Correct Answer: D