EC1-349 Q&As

Computer Hacking Forensic Investigator Exam

Pass EC-COUNCIL EC1-349 Exam with 100% Guarantee

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

https://www.pass4itsure.com/ec1-349.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Email archiving is a systematic approach to save and protect the data contained in emails so that it can tie easily accessed at a later date.

A. True

B. False

Correct Answer: A

QUESTION 2

A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its properA packet is sent to a router that does not have the packet? destination address in its route table, how will the packet get to its proper destination?

A. Border Gateway Protocol

B. Root Internet servers

C. Gateway of last resort

D. Reverse DNS

Correct Answer: C

QUESTION 3

Which of the following statements is incorrect related to acquiring electronic evidence at crime scene?

A. Sample banners are used to record the system activities when used by the unauthorized user

B. In warning banners, organizations give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring

C. The equipment is seized which is connected to the case, knowing the role of the computer which will indicate what should be taken

D. At the time of seizing process, you need to shut down the computer immediately

Correct Answer: D

QUESTION 4

One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

A. the File Allocation Table

B. the file header

C. the file footer

D. the sector map

Correct Answer: B

QUESTION 5

When collecting electronic evidence at the crime scene, the collection should proceed from the most volatile to the least volatile

A. True

B. False

Correct Answer: A

QUESTION 6

What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 server the course of its lifetime?

A. forensic duplication of hard drive

B. analysis of volatile data

C. comparison of MD5 checksums

D. review of SIDs in the Registry

Correct Answer: D

QUESTION 7

When conducting computer forensic analysis, you must guard against _____ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

A. Hard Drive Failure

B. Scope Creep

C. Unauthorized expenses

D. Overzealous marketing

Correct Answer: B

QUESTION 8

A law enforcement officer may only search for and seize criminal evidence with _____, which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists and the evidence of the specific crime exists at the place to be searched.

A. Mere Suspicion

B. A preponderance of the evidence

C. Probable cause

D. Beyond a reasonable doubt

Correct Answer: C

QUESTION 9

You can interact with the Registry through intermediate programs. Graphical user interface (GUI) Registry editors such as Regedit.exe or Regedt32 exe are commonly used as intermediate programs in Windows 7. Which of the following is a root folder of the registry editor?

A. HKEY_USERS

B. HKEY_LOCAL_ADMIN

C. HKEY_CLASSES_ADMIN

D. HKEY_CLASSES_SYSTEM

Correct Answer: A

QUESTION 10

Email spoofing refers to:

A. The forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source

B. The criminal act of sending an illegitimate email, falsely claiming to be from a legitimate site in an attempt to acquire the user\\'s personal or account information

C. Sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address Is hosted to cause a denial-of-service attack

D. A sudden spike of "Reply All" messages on an email distribution list, caused by one misdirected message

Correct Answer: A

QUESTION 11

Why would a company issue a dongle with the software they sell?

A. To provide source code protection

B. To provide wireless functionality with the software

C. To provide copyright protection

D. To ensure that keyloggers cannot be used

Correct Answer: C

QUESTION 12

Which one of the following is not a consideration in a forensic readiness planning checklist?

A. Define the business states that need digital evidence

B. Identify the potential evidence available

C. Decide the procedure for securely collecting the evidence that meets the requirement fn a forensically sound manner

D. Take permission from all employees of the organization

Correct Answer: D

QUESTION 13

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 14

Dumpster Diving refers to:

A. Searching for sensitive information in the user\\'s trash bins and printer trash bins, and searching the user\\'s desk for sticky notes

B. Looking at either the user\\'s keyboard or screen while he/she is logging in

C. Convincing people to reveal the confidential information

D. Creating a set of dictionary words and names, and trying all the possible combinations to crack the password

Correct Answer: A

QUESTION 15

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 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 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