Vendor: EC-Council

Exam Code: 312-49

Exam Name: Computer Hacking Forensic Investigator (CHFI) VUE

Version: DEMO

QUESTION 1
Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

A. Point-to-point
B. End-to-end
C. Thorough
D. Complete event analysis

Answer: B

QUESTION 2
What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

A. hda
B. hdd
C. hdb
D. hdc

Answer: B

QUESTION 3
From the following spam mail header, identify the host IP that sent this spam?

From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id
fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1)
with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)
Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk
From: "china hotel web"
To: "Shlam"
Subject: SHANGHAI (HILTON HOTEL) PACKAGE
Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0
X-Priority: 3 X-MSMail-
Priority: Normal
Reply-To: "china hotel web"

A. 203.218.39.50
B. 203.218.39.20
C. 137.189.96.52
D. 8.12.1.0

Answer: B

QUESTION 4
You have used a newly released forensic investigation tool, which doesnt meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to

weaken your case?

A. Only the local law enforcement should use the tool
B. You are not certified for using the tool
C. The toolhasnt been tested by the International Standards Organization (ISO)
D. The tool has not been reviewed and accepted by your peers

Answer: D

QUESTION 5
What type of attack sends SYN requests to a target system with spoofed IP addresses?

A. SYN flood
B. Ping of death
C. Cross site scripting
D. Land

Answer: A

QUESTION 6
If you plan to startup a suspect's computer, you must modify the _____ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

A. Scandisk utility
B. deltree command
C. CMOS
D. Boot.sys

Answer: C

QUESTION 7
Why would an investigator use Visual TimeAnalyzer when investigating a computer used by numerous users?

A. To see if the Kerberos ticket time is in sync with the rest of the domain
B. To see if any of the users changed the system time on the computer
C. To see how long each user utilized different programs
D. To see if any of the users were able to change their local permission

Answer: C

QUESTION 8
You are working as an independent computer forensics investigator and receive 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 proceedings?

A. incremental backup copy
B. bit-stream copy
C. robust copy
D. full backup copy

Answer: B

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

Answer: A

QUESTION 10
What does mactime, an essential part of the coroner's toolkit do?

A. It is a tool specific to the MAC OS and forms a core component of the toolkit
B. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps
C. The toolsscans for i-node information, which is used by other tools in the tool kit
D. It can recover deleted file space and search it for data. However, it does not allow the investigator to preview them

Answer: B

QUESTION 11
What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

A. Fraggle
B. Smurf scan
C. SYN flood
D. Teardrop

Answer: A

QUESTION 12
What file on an iPod stores the computer names and usernames used to connect to an iPod?

A. StoredInfo
B. UserInfo

C. iPodInfo
D. DeviceInfo

Answer: D

QUESTION 13
E-mail logs contain which of the following information to help you in your investigation?

A. attachments sent with the e-mail message
B. contents of the e-mail message
C. user account that was used to send the message
D. unique message identifier
E. date and time the message was sent

Answer: ABCE

QUESTION 14
Microsoft Outlook maintains email messages in a proprietary format in what type of file?

A. .email
B. .mail
C. .pst
D. .doc

Answer: C

QUESTION 15
Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus. He runs the netstat command on the machine to see its current connections. In the following screenshot, what do the 0.0.0.0 IP addresses signify?

A. Those connections are established
B. Those connections are in listening mode
C. Those connections are in closed/waiting mode
D. Those connections are in timed out/waiting mode

Answer: B

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**