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.leads4pass.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Before performing a logical or physical search of a drive in Encase, what must be added to the program?

A. File signatures

B. Keywords

C. Hash sets

D. Bookmarks

Correct Answer: B

QUESTION 2

Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?

A. network-based IDS systems (NIDS)

B. host-based IDS systems (HIDS)

C. anomaly detection

D. signature recognition

Correct Answer: BC

QUESTION 3

You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so Quickly?

A. Passwords of 14 characters or less are broken up into two 7-character hashes

B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network

C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty

D. The passwords that were cracked are local accounts on the Domain Controller

Correct Answer: A

QUESTION 4

Computer security logs contain information about the events occurring within an organization\\'s systems and networks. Which of the following security logs contains Logs of network and host- based security software?

A. Operating System (OS) logs

B. Application logs

C. Security software logs

D. Audit logs

Correct Answer: C

QUESTION 5

You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printed out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the _____ in order to track the emails back to the suspect.

A. Routing Table

B. Firewall log

C. Configuration files

D. Email Header

Correct Answer: D

QUESTION 6

When monitoring for both intrusion and security events between multiple computers, it is essential that the computers\\' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

A. Time-Sync Protocol

B. SyncTime Service

C. Network Time Protocol

D. Universal Time Set

Correct Answer: C

QUESTION 7

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company\\'s network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr

commands using DIG. What is Simon trying to accomplish here?

A. Send DOS commands to crash the DNS servers

B. Perform DNS poisoning

C. Enumerate all the users in the domain

D. Perform a zone transfer

Correct Answer: D

QUESTION 8

In the context of file deletion process, which of the following statement holds true?

A. When files are deleted, the data is overwritten and the cluster marked as available

B. The longer a disk is in use, the less likely it is that deleted files will be overwritten

C. While booting, the machine may create temporary files that can delete evidence

D. Secure delete programs work by completely overwriting the file in one go

Correct Answer: C

QUESTION 9

Network forensics can be defined as the sniffing, recording, acquisition and analysis of the network traffic and event logs in order to investigate a network security incident.

A. True

B. False

Correct Answer: A

QUESTION 10

Area density refers to:

A. the amount of data per disk

B. the amount of data per partition

C. the amount of data per square inch

D. the amount of data per platter

Correct Answer: AC

QUESTION 11

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

(Select up to 4)

A. user account that was used to send the account

B. attachments sent with the e-mail message

C. unique message identifier

D. contents of the e-mail message

E. date and time the message was sent

Correct Answer: ACDE

QUESTION 12

Ever-changing advancement or mobile devices increases the complexity of mobile device examinations. Which or the following is an appropriate action for the mobile forensic investigation?

A. To avoid unwanted interaction with devices found on the scene, turn on any wireless interfaces such as Bluetooth and Wi-Fi radios

B. Do not wear gloves while handling cell phone evidence to maintain integrity of physical evidence

C. If the device\\'s display is ON. the screen\\'s contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed icons

D. If the phone is in a cradle or connected to a PC with a cable, then unplug the device from the computer

Correct Answer: C

QUESTION 13

Router log files provide detailed Information about the network traffic on the Internet. It gives information about the attacks to and from the networks. The router stores log files in the_____.

A. Router cache

B. Application logs

C. IDS logs

D. Audit logs

Correct Answer: A

QUESTION 14

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. 137.189.96.52

B. 8.12.1.0

C. 203.218.39.20

D. 203.218.39.50

Correct Answer: C

QUESTION 15

If a suspect computer is located in an area that may have toxic chemicals, you must:

A. coordinate with the HAZMAT team

B. determine a way to obtain the suspect computer

C. assume the suspect machine is contaminated

D. do not enter alone

Correct Answer: A