EC1-349$^{\text{Q\&As}}$

Computer Hacking Forensic Investigator Exam

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

QUESTION 1

A forensic investigator is a person who handles the complete Investigation process, that is, the preservation, identification, extraction, and documentation of the evidence. The investigator has many roles and responsibilities relating to the cybercrime analysis. The role of the forensic investigator is to:

A. Take permission from all employees of the organization for investigation

B. Harden organization network security

C. Create an image backup of the original evidence without tampering with potential evidence

D. Keep the evidence a highly confidential and hide the evidence from law enforcement agencies

Correct Answer: C

QUESTION 2

Corporate investigations are typically easier than public investigations because:

A. the users have standard corporate equipment and software

B. the investigator does not have to get a warrant

C. the investigator has to get a warrant

D. the users can load whatever they want on their machines

Correct Answer: B

QUESTION 3

WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control which of the following encryption algorithm is used DVWPA2?

A. RC4-CCMP

B. RC4-TKIP

C. AES-CCMP

D. AES-TKIP

Correct Answer: C

QUESTION 4

All the Information about the user activity on the network, like details about login and logoff attempts, is collected in the security log of the computer. When a user\\'s login is successful, successful audits generate an entry whereas unsuccessful audits generate an entry for failed login attempts in the logon event ID table.

In the logon event ID table, which event ID entry (number) represents a successful logging on to a computer?

A. 528

B. 529

C. 530

D. 531

Correct Answer: A

QUESTION 5

When operating systems mark a cluster as used but not allocated, the cluster is considered as _________

A. Corrupt

B. Bad

C. Lost

D. Unallocated

Correct Answer: C

QUESTION 6

When reviewing web logs, you see an entry for resource not found in the HTTP status code filed. What is the actual error code that you would see in the log for resource not found?

A. 202

B. 404

C. 505

D. 909

Correct Answer: B

QUESTION 7

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 8

When a system is compromised, attackers often try to disable auditing, in Windows 7; modifications to the audit policy are recorded as entries of Event ID____________.

A. 4902

B. 3902

C. 4904

D. 3904

Correct Answer: A

QUESTION 9

A system with a simple logging mechanism has not been given much attention during development, this system is now being targeted by attackers, if the attacker wants to perform a new line injection attack, what will he/she inject into the log file?

A. Plaintext

B. Single pipe character

C. Multiple pipe characters

D. HTML tags

Correct Answer: A

QUESTION 10

Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white- collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subjectJulie? paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject of the essay on the most common type of crime found in corporate America. What crime should Julie focus on?

A. Physical theft

B. Copyright infringement

C. Industrial espionage

D. Denial of Service attacks

Correct Answer: C

QUESTION 11

To check for POP3 traffic using Ethereal, what port should an investigator search by?

A. 143

B. 25

C. 110

D. 125

Correct Answer: C

QUESTION 12

The Recycle Bin exists as a metaphor for throwing files away, but it also allows user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin.

Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

A. INFO2 file

B. INFO1 file

C. LOGINFO2 file

D. LOGINFO1 file

Correct Answer: A

QUESTION 13

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city\\'s network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

A. Router Penetration Testing

B. DoS Penetration Testing

C. Internal Penetration Testing

D. Firewall Penetration Testing

Correct Answer: B

QUESTION 14

How do you define Technical Steganography?

A. Steganography that uses physical or chemical means to hide the existence of a message

B. Steganography that utilizes written natural language to hide the message in the carrier in some non-obvious ways

C. Steganography that utilizes written JAVA language to hide the message in the carrier in some non-obvious ways

D. Steganography that utilizes visual symbols or signs to hide secret messages

Correct Answer: A

QUESTION 15

TCP/IP (Transmission Control Protocol/Internet Protocol) is a communication protocol used to connect different hosts in the Internet. It contains four layers, namely the network interface layer. Internet layer, transport layer, and application layer.

Which of the following protocols works under the transport layer of TCP/IP?

A. UDP

B. HTTP

C. FTP

D. SNMP

Correct Answer: A

Latest EC1-349 Dumps EC1-349 Study Guide EC1-349 Exam Questions