Vendor:EC-COUNCIL

Exam Code:412-79

Exam Name:EC-Council Certified Security Analyst (ECSA)

Version: Demo

QUESTION 1

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web

security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

alert("This is a test.")

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to CSS

B. Your website is not vulnerable

C. Your website is vulnerable to SQL injection

D. Your website is vulnerable to web bugs

Correct Answer: A

QUESTION 2

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

A. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps

B. It can recover deleted file space and search it for datA. However, it does not allow the investigator t preview them

C. The tools scans for i-node information, which is used by other tools in the tool kit

D. It is tool specific to the MAC OS and forms a core component of the toolkit

Correct Answer: A

QUESTION 3

You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?

A. the attorney-work-product rule

B. Good manners

C. Trade secrets

D. ISO 17799

Correct Answer: A

QUESTION 4

In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

A. one who has NTFS 4 or 5 partitions

B. one who uses dynamic swap file capability

C. one who uses hard disk writes on IRQ 13 and 21

D. one who has lots of allocation units per block or cluster

Correct Answer: D

QUESTION 5

John and Hillary works at the same department in the company. John wants to find out Hillary\\'s network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

A. The SID of Hillary\\'s network account

B. The network shares that Hillary has permissions

C. The SAM file from Hillary\\'s computer

D. Hillary\\'s network username and password hash

Correct Answer: D

QUESTION 6

When investigating a Windows System, it is important to view the contents of the page or swap file because:

A. Windows stores all of the systems configuration information in this file

B. This is file that windows use to communicate directly with Registry

C. A Large volume of data can exist within the swap file of which the computer user has no knowledge

D. This is the file that windows use to store the history of the last 100 commands that were run from the command line

Correct Answer: C

QUESTION 7

How many possible sequence number combinations are there in TCP/IP protocol?

A. 320 billion

B. 32 million

C. 4 billion

D. 1 billion

Correct Answer: C

QUESTION 8

In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

A. The ISP can investigate anyone using their service and can provide you with assistance

B. The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant

C. The ISP can t conduct any type of investigations on anyone and therefore can t assist you

D. ISP s never maintain log files so they would be of no use to your investigation

Correct Answer: B

QUESTION 9

Bob has been trying to penetrate a remote production system for the past tow weeks. This time however, he is able to get into the system. He was able to use the System for a period of three weeks. However law enforcement agencies were recoding his every activity and this was later presented as evidence. The organization had used a Virtual Environment to trap BoB. What is a Virtual Environment?

A. A Honeypot that traps hackers

B. A system Using Trojaned commands

C. An environment set up after the user logs in

D. An environment set up before an user logs in

Correct Answer: A

QUESTION 10

What is the target host IP in the following command?

C:\> firewalk -F 50 10.10.150.1 172.16.28.95 -p UDP

A. Firewalk does not scan target hosts

B. 172.16.28.95

C. This command is using FIN packets, which cannot scan target hosts

D. 10.10.150.1

Correct Answer: B

QUESTION 11

Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

A. 2.4 Ghz Cordless phones

B. Satellite television

C. CB radio

D. Computers on his wired network

Correct Answer: A

QUESTION 12

Windows identifies which application to open a file with by examining which of the following?

A. The File extension

B. The file attributes

C. The file Signature at the end of the file

D. The file signature at the beginning of the file

Correct Answer: A