
**Vendor:**EC-COUNCIL

**Exam Code:**EC1-349

**Exam Name:**Computer Hacking Forensic Investigator Exam

**Version:**Demo

**QUESTION 1**

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. ICMP ping sweep

B. Ping trace

C. Tracert

D. Smurf scan

Correct Answer: A

---

**QUESTION 2**

What is one method of bypassing a system BIOS password?

A. Removing the processor

B. Removing the CMOS battery

C. Remove all the system memoryRemove all the system? memory

D. Login to Windows and disable the BIOS password

Correct Answer: B

---

**QUESTION 3**

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 4**

Quality of a raster Image is determined by the _____and the amount of information in each pixel.

A. Total number of pixels

B. Image file format

C. Compression method

D. Image file size

Correct Answer: A

---

**QUESTION 5**

How many sectors will a 125 KB file use in a FAT32 file system?

A. 32

B. 16

C. 250

D. 25

Correct Answer: C

---

**QUESTION 6**

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Fraggle

B. Smurf

C. SYN flood

D. Trinoo

Correct Answer: B

---

**QUESTION 7**

You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

A. Stringsearch

B. grep

C. dir

D. vim

Correct Answer: B

---

**QUESTION 8**

The evolution of web services and their increasing use in business offers new attack vectors in an application framework. Web services are based on XML protocols such as web Services Definition Language (WSDL) for describing the connection points, Universal Description, Discovery, and Integration (UDDI) for the description and discovery of Web services and Simple Object Access Protocol (SOAP) for communication between Web services that are vulnerable to various web application threats. Which of the following layer in web services stack is vulnerable to fault code leaks?

A. Presentation Layer

B. Security Layer

C. Discovery Layer

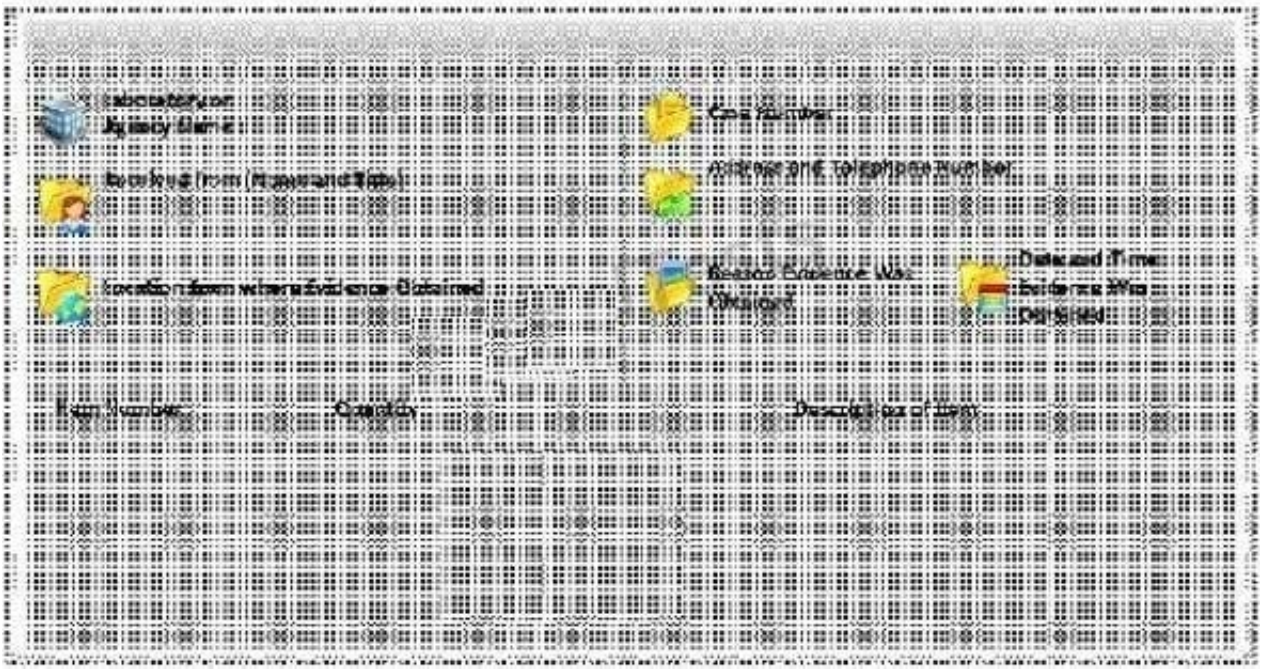
D. Access Layer

Correct Answer: C

---

**QUESTION 9**

What document does the screenshot represent?



A. Chain of custody form

B. Search warrant form

C. Evidence collection form

D. Expert witness form

Correct Answer: A

---

**QUESTION 10**

You are using DriveSpy, a forensic tool and want to copy 150 sectors where the starting sector is 1709 on the primary hard drive. Which of the following formats correctly specifies these sectors?

A. 0:1000, 150

B. 0:1709, 150

C. 1:1709, 150

D. 0:1709-1858

Correct Answer: B

---

**QUESTION 11**

Which of the following password cracking techniques works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

A. Brute forcing attack

B. Hybrid attack

C. Syllable attack

D. Rule-based attack

Correct Answer: B

---

**QUESTION 12**

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