412-79Q&As

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/412-79.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

Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\system32\drivers\etc

B. %systemroot%\repair

C. %systemroot%\LSA

D. %systemroot%\system32\LSA

Correct Answer: B

QUESTION 2

What will the following URL produce in an unpatched IIS Web Server?

http://www.thetargetsite.com/ scripts/.. %co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Execute a buffer flow in the C: drive of the web server

B. Insert a Trojan horse into the C: drive of the web server

C. Directory listing of the C:\windows\system32 folder on the web server

D. Directory listing of C: drive on the web server

Correct Answer: D

QUESTION 3

When cataloging digital evidence, the primary goal is to:

A. Make bit-stream images of all hard drives

B. Preserve evidence integrity

C. Not remove the evidence from the scene

D. Not allow the computer to be turned off

Correct Answer: B

QUESTION 4

When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts _____ in the first letter position of the filename in the FAT database.

A. A Capital X

B. A Blank Space

C. The Underscore Symbol

D. The lowercase Greek Letter Sigma (s)

Correct Answer: D

QUESTION 5

Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

A. Application-level proxy firewall

B. Data link layer firewall

C. Packet filtering firewall

D. Circuit-level proxy firewall

Correct Answer: A

QUESTION 6

Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?

A. 18 U.S.C. 1029

B. 18 U.S.C. 1362

C. 18 U.S.C. 2511

D. 18 U.S.C. 2703

Correct Answer: A

QUESTION 7

What type of file is represented by a colon (:) with a name following it in the Master File Table of NTFS disk?

A. A compressed file

B. A Data stream file

C. An encrypted file

D. A reserved file

Correct Answer: B

QUESTION 8

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 9

Software firewalls work at which layer of the OSI model?

A. Transport

B. Application

C. Network

D. Data Link

Correct Answer: D

QUESTION 10

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 11

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 SAM file from Hillary computer

B. Hillary network username and password hash

C. The SID of Hillary network account

D. The network shares that Hillary has permissions

Correct Answer: B

QUESTION 12

Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\LSA

B. %systemroot%\repair

C. %systemroot%\system32\drivers\etc

D. %systemroot%\system32\LSA

Correct Answer: B

QUESTION 13

When monitoring for both intrusion and security events between multiple computers, it is essential that the computers clocks are synchronize D. 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. Universal Time Set

B. Network Time Protocol

C. SyncTime Service

D. Time-Sync Protocol

Correct Answer: B

QUESTION 14

When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

A. on the individual computer s ARP cache

B. in the Web Server log files

C. in the DHCP Server log files

D. there is no way to determine the specific IP address

Correct Answer: C

QUESTION 15

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

412-79 Practice Test 412-79 Study Guide 412-79 Exam Questions