412-79 Q&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.passapply.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

QUESTION 1

The objective of this act was to protect consumers personal financial information held by financial institutions and their service providers.

A. HIPAA

B. Sarbanes-Oxley 2002

C. Gramm-Leach-Bliley Act

D. California SB 1386

Correct Answer: C

QUESTION 2

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well- tested hardware write-blocking device to:

A. Automate Collection from image files

B. Avoiding copying data from the boot partition

C. Acquire data from host-protected area on a disk

D. Prevent Contamination to the evidence drive

Correct Answer: D

QUESTION 3

How many bits is Source Port Number in TCP Header packet?

A. 48

B. 32

C. 64

D. 16

Correct Answer: D

QUESTION 4

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. SYN flood

C. Trinoo

D. Smurf

Correct Answer: D

QUESTION 5

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. Perform a zone transfer

B. Perform DNS poisoning

C. Send DOS commands to crash the DNS servers

D. Enumerate all the users in the domain

Correct Answer: A

QUESTION 6

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 7

What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

A. Service account passwords in plain text

B. Cached password hashes for the past 20 users

C. IAS account names and passwords

D. Local store PKI Kerberos certificates

Correct Answer: A

QUESTION 8

What is the target host IP in the following command?

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 9

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 10

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. NIPS

B. Passive IDS

C. Progressive IDS

D. Active IDS

Correct Answer: D

QUESTION 11

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 12

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. RaidSniff

B. Snort

C. Ettercap

D. Airsnort

Correct Answer: C

QUESTION 13

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162

B. 160

C. 161

D. 163

Correct Answer: AC

QUESTION 14

After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

A. Enable BGP

B. Disable BGP

C. Enable direct broadcasts

D. Disable direct broadcasts

Correct Answer: D

QUESTION 15

What information do you need to recover when searching a victims computer for a crime committed with specific e-mail message?

A. Internet service provider information

B. E-mail header

C. Username and password

D. Firewall log

Correct Answer: B