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.leads4pass.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 use of warning banners helps a company avoid litigation by overcoming an employees assumed _____ When connecting to the company s intranet, network or Virtual Private Network(VPN) and will allow the company s investigators to monitor, search and retrieve information stored within the network.

A. Right to work

B. Right of free speech

C. Right to Internet Access

D. Right of Privacy

Correct Answer: D

QUESTION 2

You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position:

7+ years experience in Windows Server environment 5+ years experience in Exchange 2000/2003 environment Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired, MCSE, CEH preferred No Unix/Linux Experience needed

What is this information posted on the job website considered?

A. Information vulnerability

B. Social engineering exploit

C. Trade secret

D. Competitive exploit

Correct Answer: A

QUESTION 3

You are working as an independent computer forensics investigator and receive a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer laB. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a simple backup copy of the hard drive in the PC and put it on this drive and requests that you examine that drive for evidence of the suspected images. You inform him that a simple backup copy will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceedings?

A. Bit-stream Copy

B. Robust Copy

C. Full backup Copy

D. Incremental Backup Copy

Correct Answer: A

QUESTION 4

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 5

What happens when a file is deleted by a Microsoft operating system using the FAT file system?

A. only the reference to the file is removed from the FAT

B. the file is erased and cannot be recovered

C. a copy of the file is stored and the original file is erased

D. the file is erased but can be recovered

Correct Answer: A

QUESTION 6

A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloadeD. What can the investigator do to prove the violation? Choose the most feasible option.

A. Image the disk and try to recover deleted files

B. Seek the help of co-workers who are eye-witnesses

C. Check the Windows registry for connection data (You may or may not recover)

D. Approach the websites for evidence

Correct Answer: A

QUESTION 7

When obtaining a warrant it is important to:

A. particularlydescribe the place to be searched and particularly describe the items to be seized

B. generallydescribe the place to be searched and particularly describe the items to be seized

C. generallydescribe the place to be searched and generally describe the items to be seized

D. particularlydescribe the place to be searched and generally describe the items to be seized

Correct Answer: A

QUESTION 8

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. OSPF

B. BPG

C. ATM

D. UDP

Correct Answer: A

QUESTION 9

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. Ping trace

B. Tracert

C. Smurf scan

D. ICMP ping sweep

Correct Answer: D

QUESTION 10

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 11

In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?

A. evidence must be handled in the same way regardless of the type of case

B. evidence procedures are not important unless you work for a law enforcement agency

C. evidence in a criminal case must be secured more tightly than in a civil case

D. evidence in a civil case must be secured more tightly than in a criminal case

Correct Answer: C

QUESTION 12

You are working for a local police department that services a population of 1,000,000 people and you have been given the task of building a computer forensics laB. How many law-enforcement computer investigators should you request to staff the lab?

A. 8

B. 1

C. 4

D. 2

Correct Answer: C

QUESTION 13

Study the log given below and answer the following question: Apr 24 14:46:46 [4663]: spp_portscan:

portscan detected from 194.222.156.169 Apr 24 14:46:46 [4663]: IDS27/FIN Scan:

194.222.156.169:56693 -> 172.16.1.107:482 Apr 24 18:01:05 [4663]: IDS/DNS-version-query:

212.244.97.121:3485 -> 172.16.1.107:53 Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval:

194.222.156.169:1425 -> 172.16.1.107:21 Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53 Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53 Apr 25 02:08:07

[5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53 Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111 Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard:

198.173.35.164:4221 -> 172.16.1.107:80 Apr 26

05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53 Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53 Apr 26 06:44:25 victim7 PAM_pwdb [12509]: (login) session opened for

user simple by (uid=0) Apr 26 06:44:36 victim7 PAM_pwdb[12521]:

(su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe:

24.112.167.35:20 -> 172.16.1.107:1080 Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect:

172.16.1.107:23

-> 213.28.22.189:4558 Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

A.

Disallow UDP53 in from outside to DNS server

B.

Allow UDP53 in from DNS server to outside

C.

Disallow TCP53 in from secondaries or ISP server to DNS server

D.

Block all UDP traffic

Correct Answer: A

QUESTION 14

A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its properA packet is sent to a router that does not have the packet? destination address in its route table, how will the packet get to its proper destination?

A. Root Internet servers

B. Border Gateway Protocol

C. Gateway of last resort

D. Reverse DNS

Correct Answer: C

QUESTION 15

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. False negatives

B. True positives

C. True negatives

D. False positives

Correct Answer: A