

EC0-479^{Q&As}

EC-Council Certified Security Analyst(ECSA)

Pass EC-COUNCIL EC0-479 Exam with 100% Guarantee

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

<https://www.certbus.com/EC0-479.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

Diskcopy is:

- A. a utility by AccessData
- B. a standard MS-DOS command
- C. Digital Intelligence utility
- D. dd copying tool

Correct Answer: B

QUESTION 2

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 3

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 proper destination? 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 proper destination?

- A. Root Internet servers
- B. Border Gateway Protocol
- C. Gateway of last resort
- D. Reverse DNS

Correct Answer: C

QUESTION 4

What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?

- A. rootkit
- B. key escrow
- C. steganography
- D. Offset

Correct Answer: C

QUESTION 5

Area density refers to:

- A. the amount of data per disk
- B. the amount of data per partition
- C. the amount of data per square inch
- D. the amount of data per platter

Correct Answer: A

QUESTION 6

In General, _____ Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

- A. Network Forensics
- B. Data Recovery
- C. Disaster Recovery
- D. Computer Forensics

Correct Answer: D

QUESTION 7

When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

- A. a write-blocker
- B. a protocol analyzer

C. a firewall

D. a disk editor

Correct Answer: A

QUESTION 8

What is a good security method to prevent unauthorized users from "tailgating"?

A. Electronic key systems

B. Man trap

C. Pick-resistant locks

D. Electronic combination locks

Correct Answer: B

QUESTION 9

Which part of the Windows Registry contains the user's password file?

A. HKEY_LOCAL_MACHINE

B. HKEY_CURRENT_CONFIGURATION

C. HKEY_USER

D. HKEY_CURRENT_USER

Correct Answer: A

QUESTION 10

Bob has been trying to penetrate a remote production system for the past two 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 recording 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 11

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

- A. outlook:"search"
- B. allinurl:"exchange/logon.asp"
- C. locate:"logon page"
- D. intitle:"exchange server"

Correct Answer: B

QUESTION 12

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 13

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

- A. Use attack as a launching point to penetrate deeper into the network
- B. Demonstrate that no system can be protected against DoS attacks
- C. List weak points on their network
- D. Show outdated equipment so it can be replaced

Correct Answer: C

QUESTION 14

Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command.

What is he testing at this point?

```
#include
#include
int main(int argc, char *argv[])
{
char buffer[10];
if (argc
{
printf(stderr, "USAGE: %s string\n", argv[0]);
return 1;
}
strcpy(buffer, argv[1]);
return 0;
}
```

- A. Buffer overflow
- B. Format string bug
- C. Kernal injection
- D. SQL injection

Correct Answer: A

QUESTION 15

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

[EC0-479 Study Guide](#)

[EC0-479 Exam Questions](#)

[EC0-479 Braindumps](#)

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

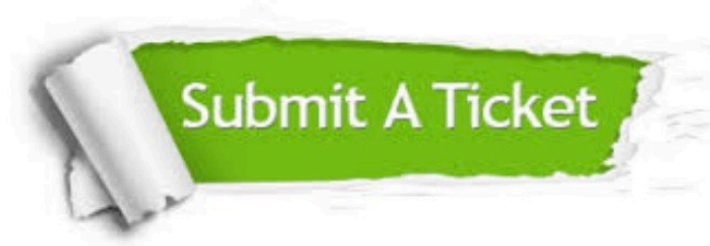
We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.certbus.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © certbus, All Rights Reserved.