312-38 ^{Q&As}

Certified Network Defender (CND)

Pass EC-COUNCIL 312-38 Exam with 100% Guarantee

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

https://www.leads4pass.com/312-38.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

You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

A. Warm site

B. Cold site

C. Hot site

D. Off site

Correct Answer: B

A cold site provides an office space, and in some cases basic equipment. However, you will need to restore your data to that equipment in order to use it. This is a much less expensive solution than the hot site. Answer option C is incorrect. A

hot site has equipment installed, configured and ready to use. This may make disaster recovery much faster, but will also be more expensive. And a school district can afford to be down for several hours before resuming IT operations, so the

less expensive option is more appropriate.

Answer option A is incorrect. A warm site is between a hot and cold site. It has some equipment ready and connectivity ready. However, it is still significantly more expensive than a cold site, and not necessary for this scenario.

Answer option D is incorrect. Off site is not any type of backup site terminology.

QUESTION 2

You are taking over the security of an existing network. You discover a machine that is not being used as such, but has software on it that emulates the activity of a sensitive database server. What is this?

A. A Polymorphic Virus

B. A Virus

C. A reactive IDS.

D. A Honey Pot

Correct Answer: D

A honey pot is a device specifically designed to emulate a high value target such as a database server or entire sub section of your network. It is designed to attract the hacker\\'s attention.

QUESTION 3

Andrew would like to configure IPsec in a manner that provides confidentiality for the content of packets. What component of IPsec provides this capability?

A. IKE

B. ESP

C. AH

D. ISAKMP

Correct Answer: B

QUESTION 4

Fill in the blank with the appropriate term. is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed.

Correct Answer: Network reconnaissance

Network reconnaissance is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed. Network reconnaissance is increasingly used to exploit network standards and automated communication methods. The aim is to determine what types of computers are present, along with additional information about those computers such as the type and version of the operating system. This information can be analyzed for known or recently discovered vulnerabilities that can be exploited to gain access to secure networks and computers. Network reconnaissance is possibly one of the most common applications of passive data analysis. Early generation techniques, such as TCP/IP passive fingerprinting, have accuracy issues that tended to make it ineffective. Today, numerous tools exist to make reconnaissance easier and more effective.

QUESTION 5

Which of the following commands is used for port scanning?

A. nc -t

B. nc -z

C. nc -v

D. nc -d

Correct Answer: B

Latest 312-38 Dumps   312-38 Practice Test   312-38 Study Guide