# 312-38Q&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.pass2lead.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**

Which of the following procedures is designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial-of-service, or unauthorized changes to system hardware, software, or data?

A. Cyber Incident Response Plan

B. Crisis Communication Plan

C. Disaster Recovery Plan

D. Occupant Emergency Plan

Correct Answer: A

The Cyber Incident Response Plan is used to address cyber attacks against an organization\\'s IT system through various procedures. These procedures enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as denial-of-service attacks, unauthorized accessing of a system or data, or unauthorized changes to system hardware, software, or data. Answer option C is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data. Answer option D is incorrect. The Occupant Emergency Plan (OEP) is used to reduce the risk to personnel, property, and other assets while minimizing work disorders in the event of an emergency. It is the response procedure for occupants of a facility on the occurrence of a situation, which is posing a potential threat to the health and safety of personnel, the environment, or property. OEPs are developed at the facility level, specific to the geographic site and structural design of the building. Answer option B is incorrect. The crisis communication plan can be broadly defined as the plan for the exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public relations profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation. The aim of crisis communication plan is to assist organizations to achieve continuity of critical business processes and information flows under crisis, disaster or event driven circumstances.

**QUESTION 2**

Which of the following UTP cables uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps?

A. Category 5e

B. Category 5

C. Category 3

D. Category 6

Correct Answer: C

Category 3 type of UTP cable uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps. They are commonly used in Ethernet networks that operate at the speed of 10 Mbps. A higher speed is also possible by these cables implementing the Fast Ethernet (100Base-T4) specifications. This cable is used mainly for telephone systems. Answer option B is incorrect. This category of UTP cable is the most commonly used cable in present day networks. It consists of four twisted pairs and is used in those Ethernet networks that run at the speed of 100 Mbps. Category 5 cable can also provide a higher speed of up to 1000 Mbps. Answer option A is incorrect. It is also known as Category 5 Enhanced cable. Its specification is the same as category 5, but it has some enhanced features and is used in Ethernets

that run at the speed of 1000 Mbps. Answer option D is incorrect. This category of UTP cable is designed to support high-speed networks that run at the speed of 1000 Mbps. It consists of four pairs of wire and uses all of them for data transmission. Category 6 provides more than twice the speed of Category 5e, but is also more expensive.

**QUESTION 3**

Fill in the blank with the appropriate term. encryption is a type of encryption that uses two keys, i.e., a public key and a private key pair for data encryption. It is also known as public key encryption.

Correct Answer: Asymmetric

Asymmetric encryption is a type of encryption that uses two keys, i.e., a public key and a private key pair for data encryption. The public key is available to everyone, while the private or secret key is available only to the recipient of the message. For example, when a user sends a message or data to another user, the sender uses the public key to encrypt the data. The receiver uses his private key to decrypt the data.

**QUESTION 4**

Which of the following policies is used to add additional information about the overall security posture and serves to protect employees and organizations from inefficiency or ambiguity?

A. User policy

B. Group policy

C. Issue-Specific Security Policy

D. IT policy

Correct Answer: C

The Issue-Specific Security Policy (ISSP) is used to add additional information about the overall security posture. It helps in providing detailed, targeted guidance for instructing organizations in the secure use of tech systems. This policy serves to protect employees and organizations from inefficiency or ambiguity. Answer option A is incorrect. A user policy helps in defining what users can and should do to use network and organization\\'s computer equipment. It also defines what limitations are put on users for maintaining the network secure such as whether users can install programs on their workstations, types of programs users are using, and how users can access data. Answer option D is incorrect. IT policy includes general policies for the IT department. These policies are intended to keep the network secure and stable. It includes the following: Virus incident and security incident Backup policy Client update policies Server configuration, patch update, and modification policies (security) Firewall policies, Dmz policy, email retention, and auto forwarded email policy Answer option B is incorrect. A group policy specifies how programs, network resources, and the operating system work for users and computers in an organization.

**QUESTION 5**

Fill in the blank with the appropriate term. A is a set of tools that take Administrative control of a computer system without authorization by the computer owners and/or legitimate managers.

Correct Answer: rootkit

A rootkit is a set of tools that take Administrative control of a computer system without authorization by the computer owners and/or legitimate managers. A rootkit requires root access to be installed in the Linux operating system, but once

installed, the attacker can get root access at any time. Rootkits have the following features:

They allow an attacker to run packet sniffers secretly to capture passwords.

They allow an attacker to set a Trojan into the operating system and thus open a backdoor for anytime access.

They allow an attacker to replace utility programs that can be used to detect the attacker\\'s activity.

They provide utilities for installing Trojans with the same attributes as legitimate programs.