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.passapply.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

QUESTION 1

Which of the following indicators refers to potential risk exposures that attackers can use to breach the security of an organization?

A. Indicators of attack

B. Key risk indicators

C. Indicators of exposure

D. Indicators of compromise

Correct Answer: C

QUESTION 2

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 3

Which of the following standards defines Logical Link Control (LLC)?

A. 802.2

B. 802.3

C. 802.5

D. 802.4

Correct Answer: A

QUESTION 4

Which of the following is a network analysis tool that sends packets with nontraditional IP stack parameters?

A. Nessus

B. COPS

C. SAINT

D. HPing

Correct Answer: D

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.