

# 312-38<sup>Q&As</sup>

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

Ryan works as a network security engineer at an organization the recently suffered an attack. As a countermeasure, Ryan would like to obtain more information about the attacker and chooses to deploy a honeypot into the organizations production environment called Kojoney. Using this honeypot, he would like to emulate the network vulnerability that was attacked previously. Which type of honeypot is he trying to implement?

- A. High interaction honeypots
- B. Research honeypot
- C. Low interaction honeypots
- D. Pure honeypots

Correct Answer: C

---

### QUESTION 2

Which of the following is a device that provides local communication between the datalogger and a computer?

- A. Controllerless modem
- B. Optical modem
- C. Acoustic modem
- D. Short haul modem

Correct Answer: D

A short haul modem is a device that provides local communication between the datalogger and a computer with an RS-232 serial port. It transmits data up to 6.5 miles over a four-wire unconditioned line (two twisted pairs). Answer option B is incorrect. An optical modem is a device that is used for converting a computer's electronic signals into optical signals for transmission over optical fiber. It also converts optical signals from an optical fiber cable back into electronic signals. It provides higher data transmission rates because it uses extremely high capacity of the optical fiber cable for transmitting data. Answer option C is incorrect. An acoustic modem provides wireless communication under water. The optimum performance of a wireless acoustic modem system depends upon the speed of sound, water depth, existence of thermocline zones, ambient noise, and seasonal change. Answer option A is incorrect. A controllerless modem is a hardware-based modem that does not have the physical communications port controller circuitry. It is also known as WinModem or software modem. A controllerless modem is very inexpensive and can easily be upgraded with new software.

---

### QUESTION 3

Lyle is the IT director for a medium-sized food service supply company in Nebraska. Lyle's company employs over 300 workers, half of which use computers. He recently came back from a security training seminar on logical security. He now wants to ensure his company is as secure as possible. Lyle has many network nodes and workstation nodes across the network. He does not have much time for implementing a network-wide solution. He is primarily concerned about preventing any external attacks on the network by using a solution that can drop packets if they are found to be malicious. Lyle also wants this solution to be easy to implement and be network-wide. What type of solution would be

best for Lyle?

- A. A NEPT implementation would be the best choice.
- B. To better serve the security needs of his company, Lyle should use a HIDS system.
- C. Lyle would be best suited if he chose a NIPS implementation
- D. He should choose a HIPS solution, as this is best suited to his needs.

Correct Answer: C

---

#### QUESTION 4

Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

- A. Disaster Recovery Plan
- B. Business Continuity Plan
- C. Contingency Plan
- D. Continuity of Operations Plan

Correct Answer: B

BCP is a strategy to minimize the consequence of the instability and to allow for the continuation of business processes. The goal of BCP is to minimize the effects of a disruptive event on a company, and is formed to avoid interruptions to normal business activity. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Answer option C is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer option A is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity. Answer option D is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.

---

#### QUESTION 5

Fill in the blank with the appropriate term. A network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or tokenpassing scheme is used for preventing the collision of data between two computers that want to send messages at the same time.

Correct Answer: Token Ring

A Token Ring network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time. The Token Ring protocol is the second most widely-used protocol on local area networks after Ethernet. The IBM Token Ring protocol led to a standard version, specified as IEEE 802.5. Both protocols are used and are very similar. The IEEE 802.5 Token Ring technology provides for data transfer rates of either 4 or 16 megabits per second. Working: Empty information frames are constantly circulated on the ring. When a computer has a message to send, it adds a token to an empty frame and adds a message and a destination identifier to the frame. The frame is then observed by each successive workstation. If the workstation sees that it is the destination for the message, it copies the message from the frame and modifies the token back to 0. When the frame gets back to the originator, it sees that the token has been modified to 0 and that the message has been copied and received. It removes the message from the particular frame. The frame continues to circulate as an empty frame, ready to be taken by a workstation when it has a message to send.

[312-38 VCE Dumps](#)

[312-38 Exam Questions](#)

[312-38 Braindumps](#)