Chapter 1- Quiz

1. Thwarting cyber criminals includes which of the following? (Choose two.)

- establishing early warning systems
- changing operating systems
- hiring hackers
- shutting down the network
- sharing cyber Intelligence information

Explanation: Organization can join efforts to thwart cyber crime by establishing early warning systems and sharing cyber intelligence.

2. What does the acronym IoE represent?

- Internet of Everyday
- Insight into Everything
- Intelligence on Everything
- Internet of Everything

Explanation: Internet of Everything is the term used for Internet-connected devices

3. What name is given to a amateur hacker?

- blue team
- red hat
- script kiddie
- black hat

Explanation: Script kiddies is a term used to describe inexperienced hackers.

4. Pick three types of records that cyber criminals would be interested in stealing from organizations. (Choose three.)

- game
- rock
- employment
- food
- education
- flight
- medical

Explanation: Employment, medical, and education records are important to protect because they contain personal information.

5. What is the workforce framework category that includes highly specialized review and evaluation of incoming cybersecurity information to determine if it is useful for intelligence?

- Oversight and Development
- Protect and Defend
- Analyze
- Securely Provision

Explanation: The "Analyze" category of the workforce framework includes specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness.

6. What name is given to hackers who hack for a cause?

- white hat
- blue hat
- hacker
- hactivist

Explanation: The term is used to describe gray hackers who rally and protect for a cause.

7. What does the term BYOD represent?

- bring your own decision
- buy your own disaster
- bring your own disaster
- bring your own device

Explanation: The term bring-your-own-device is used to describe mobile devices such as iPhones, smartphones, tablets, and other devices,

8. What does the term vulnerability mean?

- a computer that contains sensitive information
- a method of attack to exploit a target
- a weakness that makes a target susceptible to an attack
- a known target or victim machine
- a potential threat that a hacker creates

Explanation: A vulnerability is not a threat, but it is a weakness that makes the PC or the software a target for attacks.

9. What type of attack uses many systems to flood the resources of a target, thus making the target unavailable?

- ping sweep
- DDoS
- spoof
- DoS

Explanation: DDoS is is an attack that involves multiple systems. DoS involves only a single attack system.

10. What is an example of an Internet data domain?

- Palo Alto
- Juniper
- Cisco
- Linkedin

Explanation: A data domain is a repository for data.

11. What type of an attack can disable a computer by forcing it to use memory or by overworking its CPU?

- exhaustion
- algorithm
- DDoS
- APT

Explanation: Algorithm attacks can force computers to use memory or overwork the CPU.