Charpter 1 – Quiz

1. What three items are components of the CIA triad? (Choose three.)

- intervention
- availability
- scalability
- confidentiality
- integrity
- access

Explanation:
The CIA triad contains three components: confidentiality, integrity, and availability. It is a guideline for information security for an organization.

2. What is another name for confidentiality of information?

- trustworthiness
- privacy
- accuracy
- consistency

Explanation:
Privacy is another name for confidentiality. Accuracy, consistency, and trustworthiness describe integrity of data.

3. Which statement describes cyberwarfare?

- Cyberwarfare is an attack carried out by a group of script kiddies.
- It is simulation software for Air Force pilots that allows them to practice under a simulated war scenario.
- It is a series of personal protective equipment developed for soldiers involved in nuclear war.
- It is Internet-based conflict that involves the penetration of information systems of other nations.

Explanation:
Cyberwarfare is Internet-based conflict that involves the penetration of the networks and computer systems of other nations. Organized hackers are typically involved in such an attack.

4. What is an example of “hacktivism”?

- A group of environmentalists launch a denial of service attack against an oil company that is responsible for a large oil spill.
- A teenager breaks into the web server of a local newspaper and posts a picture of a favorite cartoon character.
- A country tries to steal defense secrets from another country by infiltrating government networks.
- Criminals use the Internet to attempt to steal money from a banking company.

Explanation:
Hacktivism is a term used to describe cyberattacks carried out by people who are considered political or ideological extremists. Hacktivists attack people or organizations that they believe are enemies to the hacktivist agenda.

5. What is the motivation of a white hat attacker?

- discovering weaknesses of networks and systems to improve the security level of these systems
- studying operating systems of various platforms to develop a new system
- taking advantage of any vulnerability for illegal personal gain
- fine tuning network devices to improve their performance and efficiency

Explanation:
White hat attackers break into networks or computer systems in order to discover weaknesses for the purpose of improving the security of these systems. These break-ins are done with permission from the owner or the organization. Any results are reported back to the owner or the organization.

6. Which method is used to check the integrity of data?

- checksum
- backup
- authentication
- encryption

Explanation:
A checksum value of a block of data is calculated and transmitted with the data. After the data is received, the checksum hashing is performed again. The calculated value is compared with the transmitted value to verify the integrity of the data.

7. Fill in the blank.

The individual user profile on a social network site is an example of a/an online identity.

8. Match the type of cyber attackers to the description. (Not all options are used.)

- gather intelligence or commit sabotage on specific goals on behalf of their government ————-> state-sponsored attackers
- make political statements, or create fear, by causing physical or psychological damage to victims ————-> terrorists
- make political statements in order to create an awareness of issues that are important to them ————> hacktivists
- Other Incorrect Match Options:
  - script kiddies

9. What are three methods that can be used to ensure confidentiality of information? (Choose three.)

- data encryption
- backup
- file permission settings
- username ID and password
- two factor authentication
- version control

Explanation:
Methods including data encryption, username ID and password, and two factor authentication can be used to help ensure confidentiality of information. File permission control, version control, and backup are methods that can be used to help ensure integrity of information.

10. What is a reason that internal security threats might cause greater damage to an organization than external security threats?

- Internal users can access the infrastructure devices through the Internet.
- Internal users can access the corporate data without authentication.
- Internal users have direct access to the infrastructure devices.
- Internal users have better hacking skills.

Explanation:
Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Internal users may not have better hacking skills than external attackers. Both internal users and external users can access the network devices through the Internet. A well designed security implementation should require authentication before corporate data is accessed, regardless of whether the access request is from within the corporate campus or from the outside network.