[Updated Constantly]

HERE

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 1 Exam Answers

1. What is a potential risk when using a free and open wireless hotspot in a public location?

- Too many users trying to connect to the Internet may cause a network traffic jam.
- The Internet connection can become too slow when many users access the wireless hotspot.
- **Network traffic might be hijacked and information stolen.**
- Purchase of products from vendors might be required in exchange for the Internet access.

2. How does a security information and event management system (SIEM) in a SOC help the personnel fight against security threats?

- by integrating all security devices and appliances in an organization
- by analyzing logging data in real time
- **by combining data from multiple technologies**
- by dynamically implementing firewall rules

3. Which statement best describes a motivation of hacktivists?

- **They are part of a protest group behind a political cause.**
- They are curious and learning hacking skills.
- They are trying to show off their hacking skills.
- They are interested in discovering new exploits.

4. If a SOC has a goal of 99.999% uptime, how many minutes of downtime a year would be considered within its goal?

- **Approximately 5 minutes per year.**
- Approximately 10 minutes per year.
- Approximately 20 minutes per year.
- Approximately 30 minutes per year.

5. Why do IoT devices pose a greater risk than other computing devices on a network?

- Most IoT devices do not require an Internet connection and are unable to receive new updates.
- IoT devices cannot function on an isolated network with only an Internet connection.
- **Most IoT devices do not receive frequent firmware updates.**
- IoT devices require unencrypted wireless connections.

6. Which two services are provided by security operations centers? (Choose two.)

- **managing comprehensive threat solutions**
- ensuring secure routing packet exchanges
- responding to data center physical break-ins
- **monitoring network security threats**
- providing secure Internet connections

7. Users report that a database file on the main server cannot be accessed. A database administrator verifies the issue and notices that the database file is now encrypted. The

organization receives a threatening email demanding payment for the decryption of the database file. What type of attack has the organization experienced?

- man-in-the-middle attack
- DoS attack
- **ransomware**
- Trojan horse

8. Which organization offers the vendor-neutral CySA+ certification?

- IEEE
- **CompTIA**
- (ISC)²
- GIAC

9. What was used as a cyberwarfare weapon to attack a uranium enrichment facility in Iran?

- DDoS
- SQL injection
- PSYOPS
- **Stuxnet**

10. Which three technologies should be included in a SOC security information and event management system? (Choose three.)

- firewall appliance
- **security monitoring**
- **log management**
- intrusion prevention
- proxy service
- **threat intelligence**

11. Which personnel in a SOC is assigned the task of verifying whether an alert triggered by monitoring software represents a true security incident?

- SOC Manager
- Tier 2 personnel
- Tier 3 personnel
- **Tier 1 personnel**

12. Which statement describes cyberwarfare?

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

13. in the operation of a SOC, which system is frequently used to let an analyst select alerts from a pool to investigate?

- syslog server
- registration system
- **ticketing system**
- security alert knowledge-based system

14. What name is given to an amateur hacker?

- red hat

- **script kiddie**
- black hat
- blue team

15. Which personnel in a SOC are assigned the task of hunting for potential threats and implementing threat detection tools?

- Tier 1 Analyst
- SOC Manager
- Tier 2 Incident Reporter
- **Tier 3 SME**