Cisco Certified Support Technician (CCST) Cybersecurity

1. Why is it important to maintain the chain of custody when handling digital evidence?

A. To accelerate the analysis of the evidence.

B. To prevent unauthorized access or tampering.

C. To ensure the evidence is stored securely.

D. To recover lost or deleted data from the evidence.

Answer(s): B

---

2. What is the purpose of conducting a hardware inventory assessment on an endpoint system?

A. To determine software compatibility requirements

B. To ensure compliance with hardware standards

C. To identify potential gaps in security policies

D. To track changes made to hardware configurations

Answer(s): B

---

3. Which of the following is an essential component of information security assessments?

A. Penetration testing

B. All of the above

C. Incident response planning

D. User training

Answer(s): B

---

4. What is configuration management in the context of cybersecurity?

A. Managing and securing access to network devices

B. Protecting the physical infrastructure of an organization

C. Establishing role-based access controls

D. Ensuring consistency and control over the configuration of IT systems

Answer(s): D

---

5. Which of the following is an integral part of the CIA triad in cybersecurity?

A. Data loss prevention (DLP)

B. Two-factor authentication (2FA)

C. Intrusion Detection System (IDS)

D. Firewall

Answer(s): B

---

6. Which malicious activity is NOT typically associated with cyber attacks?

A. Phishing

B. Malware

C. Data encryption

D. Denial of Service (DoS)

Answer(s): C

---

7. Which of the following must be documented throughout the chain of custody process?

A. Encryption protocols applied to protect the evidence.

B. Names of all individuals who handled the evidence.

C. Timeline of events that led to the acquisition of the evidence.

D. Analysis methods used on the evidence.

Answer(s): B

---

8. Which component of network security architecture is designed to separate the internal network from the external network?

A. Cloud

B. DMZ

C. Proxy

D. Virtualization

Answer(s): B

---

9. Which of the following features help to secure a wireless SoHo network from unauthorized access?

A. MAC filtering

B. Weak encryption

C. Default admin credentials

D. SSID broadcast

Answer(s): A

---

10. What is an Advanced Persistent Threat (APT)?

A. A vulnerability in network communication protocols.

B. A cyberattack that compromises multiple devices simultaneously.

C. A sophisticated and targeted attack that aims to gain unauthorized access and maintain persistence over a long period.

D. A type of malware that spreads rapidly through a network.

Answer(s): C

---

11. What is the purpose of a disaster recovery plan (DRP)?

A. To prevent the occurrence of disasters or disruptive events

B. To provide a secondary data storage location for backup purposes

C. To regularly test the effectiveness of backup systems and processes

D. To outline procedures and strategies for recovering critical systems and data after a disaster

Answer(s): D

---

12. Which of the following is true regarding the incident response process?

A. It is a reactive process that is only initiated after an incident has occurred.

B. It is a proactive process that focuses on preventing incidents from occurring.

C. It is an iterative process that involves continuous improvement based on lessons learned.

D. It is a one-time process that is only performed when an organization first establishes its security program.

Answer(s): C

---

13. Which of the following is an example of a network layer (Layer 3) security control?

A. Encryption

B. Intrusion Detection System (IDS)

C. Antivirus software

D. Firewall

Answer(s): D

---

14. What are botnets?

A. An attack that manipulates individuals into revealing sensitive information or performing certain actions.

B. A network of compromised computers controlled by a central entity to carry out malicious activities.

C. A form of cyber attack that attempts to gain unauthorized access to a network.

D. A software program that is designed to damage, disrupt, or gain unauthorized access to a computer system.

Answer(s): B

---

15. Which of the following is a characteristic of a network-based firewall?

A. Inspects and filters traffic at the application layer

B. Operates at the data link layer

C. Provides protection against external threats only

D. Requires software installed on client devices

Answer(s): C

---

16. What is ransomware?

A. A technique used by attackers to obtain sensitive information through deception.

B. A software program that is designed to damage, disrupt, or gain unauthorized access to a computer system.

C. Malicious software that encrypts files on a victim's computer and demands ransom for their release.

D. A form of cyber attack that attempts to gain unauthorized access to a network.

Answer(s): C

---

17. Which regulation sets standards for the security and privacy of protected health information (PHI) in the United States?

A. GDPR

B. BYOD

C. HIPAA

D. PCI DSS

Answer(s): C

18. Which of the following techniques is commonly used for monitoring security events "as they occur"?

A. Access control lists (ACL)

B. Vulnerability scanning

C. Firewall configuration

D. Intrusion detection systems (IDS)

Answer(s): D

19. Which of the following is an example of a detective control in information assurance?

A. Security Information and Event Management (SIEM) system

B. Encryption of sensitive data

C. Security awareness training

D. Intrusion Prevention System (IPS)

Answer(s): A

20. What is the purpose of Common Vulnerabilities and Exposures (CVEs)?

A. To protect sensitive information from unauthorized access.

B. To evaluate the effectiveness of cybersecurity measures.

C. To identify hackers and cybercriminals.

D. To categorize and provide unique identifiers for known vulnerabilities.

Answer(s): D