CompTIA Security+ Guide to Network Security Fundamentals 8th edition Ciampa Test Bank

SKU: 9798214000633-TEST-BANK

Name:_____ Class:_____ Date:_____

Mod 01 Introduction to Information Security

1. You have excellent technical acumen. Part of your responsibilities where you work include overlooking daily operations as well as analyzing and designing security solutions in a specific area. You encounter a situation that needs to be escalated. Which of the following are you most likely to approach with the situation?

a. CIO
b. CISO
c. Security manager
d. Security administrator

ANSWER: c

2. When analyzing a security breach, Acer determines the attacker was able to change the price of an item from $200 to $20. What security protection was compromised?

a. Confidentiality
b. Integrity
c. Authorization
d. Authentication

ANSWER: b

3. A visitor is trying to access a military base. The visitor needs to supply their license and enter other personal information via a kiosk. The visitor is eventually allowed to enter the base but is limited to certain areas only. What security principles are being employed? Select two.

a. Authentication
b. Authorization
c. Confidentiality
d. Accounting
e. Availability

ANSWER: a, b

4. Which of the following best describes what Della could do to prevent unauthorized parties from viewing sensitive customer information at her retail store?

a. Use software to encrypt data in a secure database.
b. Verify the ID of the party requesting access to the data.
c. Limit access to certain areas once access is granted.
d. Ensure the data cannot be manipulated or changed.

ANSWER: a

5. Evin thinks one of the computer systems where he works may have been compromised. He does not currently have a good way of determining if an unauthorized user logged in successfully. Which of the following can Evin implement that will, going forward, help him identify who logs in?

a. Authentication

b. Authorization
c. Availability
d. Accounting

ANSWER: d

6. A friend gets a virus and asks if you can help them fix the problem. You boot the computer with a bootable flash drive containing security-related tools and remove the virus. What type of control did you employ?

a. Deterrent
b. Corrective
c. Directive
d. Compensating

ANSWER: b

7. As a consultant, you are asked by a company to help them work on a security-related project that falls under the operational control scope. Which of the following will you help implement?

a. Define an acceptable use policy
b. Install a card reader to access the data center
c. Install hardware to block malicious content
d. Implement security awareness training

ANSWER: d

8. Which of the following best describes the differences or similarities between cybersecurity and information security? Select three.

a. Cybersecurity primarily protects devices.
b. Information security falls under the cybersecurity umbrella.
c. Cybersecurity guarantees more safety than information security.
d. Information security protects using products, people, and procedures.
e. Cybersecurity induces a lot more inconvenience than information security.

ANSWER: a, b, d

9. What type of entity would a threat actor most likely attack to steal design documents for a relatively recently announced government-issued contract to design and build a missile defense system?

a. Individual
b. Government
c. Enterprise
d. For-profit organization

ANSWER: c

10. An attacker hacks into a cell phone with the intent of stealing credit card information. The attacker also tries to extend the nefarious activity to contacts in the victim's phone, and their contacts as well. What entity was the

attacker targeting?

a. An enterprise
b. A competitor
c. An individual
d. A government agency

ANSWER: c

11. A malicious actor lacking technical knowledge uses an attack tool to perform a sophisticated attack. If the attacker is successful penetrating the defenses of the targeted organization, what type of activity are they most likely to perform? Select two.

a. Blackmail
b. Copy data
c. Corrupt data
d. Disrupt service
e. Manipulate data

ANSWER: b, d

12. To bypass institutional overhead, a well-intentioned networking instructor purchases a wireless router and connects it to the network. The goal is to allow students to establish connectivity with each other by connecting through the wireless router. In what activity did the instructor participate?

a. APT
b. Shadow IT
c. Insider threat
d. Ethical hacking

ANSWER: b

13. What would motivate organized crime actors to add cyberattacks to their portfolio of malicious activities?

a. Espionage
b. Create chaos
c. Philosophical beliefs
d. Increased financial gain

ANSWER: d

14. A criminal organization has decided to leave their traditional ways and pursue cyberattacks as their new mode of operation. Why would they do this?

a. Easier to hide their tracks
b. Generate disruption
c. Less competition
d. Political beliefs

ANSWER: a

15. A work-study student works at the registrar's office and is given limited access to a student database. The student is very technologically savvy and figures out a way of gaining additional privileges. The student is not pleased with one of their grades and changes it. Which of the following best describes the type of scenario this activity characterizes?

a. Cyberterrorism
b. Insider threat
c. Shadow IT
d. Revenge

ANSWER: b

16. A group of threat actors has a strong aversion to certain political ideologies. They launch a cyberattack against the organization to which its perceived adversarial counterpart belongs. This type of threat actor could most appropriately be classified under what category?

a. Hacktivist
b. Nation-state actors
c. Brokers
d. Competitors

ANSWER: a

17. A broker launches a variety of attacks to find a weakness that will lead to financial gain. What activity is the broker most likely to engage in?

a. Steal classified information against a competitor
b. Sell information about a discovered vulnerability
c. Create and sell malicious software to the highest bidder
d. Obtain, repackage, and sell pirated software

ANSWER: b

18. Company A wants to be first to market with a product forecasted to be very profitable. A few bad actors in Company A launch an attack against Company B to steal intellectual property that will help them. What type of threat actor would do something like this?

a. Hacker in a hoodie
b. Script kiddie
c. Competitors
d. Revengeful

ANSWER: c

19. An entity is determined and decides to commit to a multiyear intrusion campaign with the goal of obtaining national security information. Which of the following describes the type of attack the entity is most likely to engage in? Select two.

a. Service disruption
b. Data exfiltration
c. Data breach
d. Espionage
e. APT

ANSWER: b, e

20. Which of the following best describes what a nation-state actor is most likely to do if their attacks against a target are not successful?

a. Use different attack tools.
b. Hire more malicious actors.
c. Move on to a different target.
d. Continue trying until successful.

ANSWER: d

21. Which of the following accurately describes the differences or similarities between mainstream attack surfaces and specialized threat vectors? Select three.

a. Both are targeted with the same degree of frequency.
b. A network is an example of a mainstream attack surface.
c. An MSP is a typical example of a mainstream attack surface.
d. An imposter calling the elderly is exploiting a specialized threat vector.
e. One targets client-based software, the other targets supply chain components.

ANSWER: b, d, e

22. You receive a text message indicating your online bank account is locked until you supply the needed credentials via a link included in the message. What type of threat vector is the attacker trying to exploit? Select three.

a. Communications
b. Mainstream
c. Specialized
d. SMS
e. MMS
f. IM

ANSWER: a, c, d

23. Vaani, an IT administrator, discovers her company is using a modular router that will be in an EOL state within six months. Which of the following best describes what the company should do?

a. Replace the modules in the router with newer ones.
b. Upgrade the operating system to the latest version.

c. Update the firmware to patch known threats.
d. Replace the router with a new model.

ANSWER: d

24. A new piece of hardware has a specific IP address and supports Telnet and FTP connections so that it could be configured through a network connection. Leaving the device in this state could lead to a breach due to what type of vulnerability? Select three.

a. Open ports and services
b. Unsecure protocols
c. Default settings
d. Firmware
e. Zero-day

ANSWER: a, b, c

25. An attacker is the first malicious actor to discover a vulnerability in a software application and exploits it for considerable financial gain. What could have been done to prevent this situation?

a. Have the app tested by an external agency before releasing it.
b. Ensure the internal software testing is more comprehensive.
c. When coding, closely follow the security specifications in the requirements.
d. There is a high probability that it could not have been prevented.

ANSWER: d

26. Which of the following best describes the possible impact of an attack where credit card data is stolen from a company and the breach is eventually reported in the news? Select two.

a. Availability loss
b. Loss of reputation
c. Income generating loss
d. Possible prison time for IT personnel

ANSWER: b, d

27. As a security professional Anvi works for an organization authoring documents that define policies and procedures outlining security controls. What type of resource does the organization provide?

a. Standard
b. Regulation
c. Framework
d. Benchmark

ANSWER: c

28. Which of the following best describes the similarities or differences between the NIST RMF and the NIST CSF? Select two.

a. Components of the NIST RMF include respond and recover.
b. Both include a component to help assess and manage risks.
c. They are the result of state and industry-specific regulations.
d. They define tiers based on how well vulnerabilities are addressed.
e. Components of the NIST CSF include protect and detect.

ANSWER: d, e

29. What are some of the challenges an organization may face when trying to be in regulatory compliance as it relates to information security?

a. Virtually every industry has its own set of regulations.
b. A requirement in one regulation may negate one in another.
c. No two states share the same set of regulations.
d. All of these choices.

ANSWER: d

30. Duante needs to research the behavior of attackers as well as how they coordinate their attacks. Where is Duante most likely to look for this type of information?

a. TTP database
b. Data feeds
c. Threat feeds
d. Vulnerability feeds

ANSWER: a