EC-Council Certified Incident Handler (ECIH) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. Visit https://eccouncilecih.examzify.com

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. **When should you ask your ISP to implement filtering in a DoS containment strategy?**

   A. After correcting the vulnerability or weakness being exploited

   B. After relocating the affected target

   C. After determining the method of attack

   D. After identifying the attackers

2. **What type of insider attack spreads false information to create confusion among employees?**

   A. Theft of devices

   B. Creation of false dossiers

   C. Wiretapping

   D. Intimidation

3. **What type of tools are Exabeam Advanced Analytics, LogRhythm, Dtex Systems, and ZoneFox classified as?**

   A. Active monitoring

   B. DLP

   C. SIEM

   D. UBA/UEBA

4. **What is the potential outcome of failing to verify an SPF record due to incorrect format?**

   A. Pass

   B. Fail

   C. Neutral

   D. PermError

5. **Dwayne wants to acquire account information from a competitor company, so he sends an illegitimate email to the payroll specialist claiming to be the CEO. What type of security attack would this be?**

   A. Ransomware

   B. Phishing

   C. Web application threats

   D. IoT threats

6. Which type of malware pretends to be a useful program but collects user information for a remote attacker?

A. Spyware

B. Worm

C. Virus

D. Rootkit

7. In an insider threat investigation, what should be prioritized?

A. Public relations impact

B. Legal implications

C. User privacy considerations

D. Data retrieval and evidence collection

8. How is quantitative risk analysis defined?

A. Probability of loss X value of loss

B. Value of loss/ Probability of loss

C. Probability of loss + value of loss

D. Probability of loss - value of loss

9. Spoofing, session hijacking, DoS attacks, firewall and IDS attacks are all considered what type of information security threat?

A. Host threat

B. Network threat

C. System threat

D. Application threat

10. What motivates an insider attack where an employee publicizes sensitive information for a political cause?

A. Hacktivism

B. Corporate Espionage

C. Work-Related Grievance

D. Curiosity

Answers

1. **C**
2. **B**
3. **D**
4. **D**
5. **B**
6. **A**
7. **D**
8. **A**
9. **B**
10. **A**

Explanations

1. When should you ask your ISP to implement filtering in a DoS containment strategy?

- A. After correcting the vulnerability or weakness being exploited
- B. After relocating the affected target
- C. After determining the method of attack
- D. After identifying the attackers

Requesting your ISP to implement filtering in a DoS containment strategy is most effective after determining the method of attack. Understanding the specific nature of the Distributed Denial of Service (DDoS) or Denial of Service (DoS) attack allows for targeted filtering measures. Each attack type may require different strategies for mitigation, and knowing the attack method helps in configuring the right filters to effectively block malicious traffic while allowing legitimate traffic to flow. Implementing filtering too early, without a clear understanding of the attack method, may lead to misconfigurations that could disrupt normal business operations or fail to adequately mitigate the attack. Therefore, ensuring that you have accurately identified how the attack is executed equips you to work with your ISP to put in place the most appropriate filtering measures to protect your network.

2. What type of insider attack spreads false information to create confusion among employees?

- A. Theft of devices
- B. Creation of false dossiers
- C. Wiretapping
- D. Intimidation

The type of insider attack that spreads false information to create confusion among employees is indeed the creation of false dossiers. This involves the deliberate generation and dissemination of misleading or fabricated information that can lead to misunderstandings and conflicts within an organization. By creating false dossiers, an insider can manipulate perceptions and influence the behavior of employees, potentially sowing discord or distrust among team members. This tactic undermines the cohesion of the workforce and can have far-reaching implications for morale and productivity. In contrast, the other options focus on different forms of attacks or malicious actions. Theft of devices refers to the physical removal of company hardware, which does not primarily aim to spread misinformation. Wiretapping involves unlawfully listening to communications, targeting data privacy rather than creating confusion. Intimidation relates to coercive actions that can enforce compliance or silence dissent, rather than specifically distorting information to mislead employees. Each of these options represents a distinct threat vector, but creating false dossiers uniquely aligns with the objective of spreading disinformation and causing confusion among employees.

3. What type of tools are Exabeam Advanced Analytics, LogRhythm, Dtex Systems, and ZoneFox classified as?

A. Active monitoring

B. DLP

C. SIEM

D. UBA/UEBA

Exabeam Advanced Analytics, LogRhythm, Dtex Systems, and ZoneFox are classified as User Behavior Analytics (UBA) or User and Entity Behavior Analytics (UEBA) tools. These solutions focus on analyzing user and entity behaviors to detect abnormal activities that could indicate potential security threats or breaches. UBA/UEBA tools monitor and analyze patterns of user behavior and interactions within an IT environment. By establishing a baseline of normal activity, these tools can pinpoint deviations that may signify malicious activity, insider threats, or compromised accounts. They accomplish this through advanced analytics and machine learning techniques, which enhance their ability to identify sophisticated attacks that traditional security monitoring tools might miss. Active monitoring involves continuous surveillance of systems and networks, which is broader than just user behavior contexts. DLP (Data Loss Prevention) focuses on safeguarding sensitive information from unauthorized access and exfiltration. SIEM (Security Information and Event Management) is designed for real-time monitoring, correlation, and analysis of security events, but it doesn't focus specifically on user or entity behavior as UBA/UEBA does. Therefore, the classification of Exabeam Advanced Analytics, LogRhythm, Dtex Systems, and ZoneFox as UBA/UEBA tools accurately reflects their primary capabilities in enhancing security

4. What is the potential outcome of failing to verify an SPF record due to incorrect format?

A. Pass

B. Fail

C. Neutral

D. PermError

The correct outcome of failing to verify an SPF (Sender Policy Framework) record due to incorrect format is represented as "PermError." This result indicates that the SPF record could not be processed because it has fundamental errors, such as syntactical issues or incorrect formatting, rendering it invalid. When an SPF record is not properly formatted, the server cannot interpret the policy correctly, which may cause the SPF validation process to produce a permanent error. This is a critical failure point because it means that any email sent from that domain will not pass SPF checks, leading to potential email delivery issues since receiving mail servers rely on these records to confirm the legitimacy of email sources. In contrast, a "Pass" outcome signifies that the SPF record was valid and the source was authorized, while a "Fail" outcome indicates that the source was not authorized by the domain's SPF policy. A "Neutral" result means that the record does not explicitly allow or deny the email’s legitimacy. Therefore, the most significant implication of an incorrectly formatted SPF record is the permanently failing state, denoted as "PermError," which presents severe repercussions for domain reputability and email deliverability.

5. Dwayne wants to acquire account information from a competitor company, so he sends an illegitimate email to the payroll specialist claiming to be the CEO. What type of security attack would this be?

- A. Ransomware
- B. Phishing
- C. Web application threats
- D. IoT threats

The scenario described demonstrates a classic example of phishing. Phishing is a type of social engineering attack where an individual impersonates a trusted entity—in this case, the CEO—to trick the target into disclosing sensitive information, such as account details.   In phishing attacks, the attacker often creates a sense of urgency or employs a trustworthy persona to manipulate the victim into providing confidential information that they would not normally share. By sending an illegitimate email that supposedly comes from a high-ranking official, Dwayne exploits the authority and recognition of the CEO to gain the trust of the payroll specialist, making it more likely for the specialist to fall for this deception. The other options are not applicable in this context. Ransomware involves malicious software designed to block access to a computer system until a sum of money is paid. Web application threats refer to vulnerabilities in website applications that can be exploited for data theft or service disruption. IoT threats pertain to attacks targeting Internet of Things devices. None of these categories fit the nature of Dwayne's actions as accurately as phishing does.

6. Which type of malware pretends to be a useful program but collects user information for a remote attacker?

- A. Spyware
- B. Worm
- C. Virus
- D. Rootkit

The type of malware that pretends to be a useful program while specifically collecting user information for a remote attacker is spyware. Spyware is designed to secretly gather information about a user, such as browsing habits, login credentials, and other personal data, often without their knowledge or consent. It can be bundled with legitimate software, leading users to believe they are installing a helpful application when, in fact, they are introducing malicious code that tracks and transmits their information to an external party. In contrast to spyware, worms and viruses are primarily focused on self-replication and spreading across networks or systems, rather than the stealthy collection of personal data. Rootkits, on the other hand, are intended to hide the existence of certain processes or programs from normal methods of detection, primarily allowing other malicious activities to be concealed rather than actively gathering user information. Therefore, spyware is the most accurate descriptor for malware that masquerades as a useful application while stealing data for an attacker.

7. In an insider threat investigation, what should be prioritized?

A. Public relations impact

B. Legal implications

C. User privacy considerations

D. Data retrieval and evidence collection

In an insider threat investigation, prioritizing data retrieval and evidence collection is essential because it forms the backbone of a thorough investigation. Gathering reliable and relevant data allows investigators to understand the scope and impact of the threat. This includes identifying what data was accessed or altered, the methods used by the insider, and any potential vulnerabilities that were exploited. Proper evidence collection is crucial for legal proceedings, as it ensures that all steps taken in the investigation can withstand scrutiny in court. It also aids in preserving the integrity of the data so that it cannot be disputed later. Without strong evidence, any findings may be deemed inconclusive, and the organization may miss an opportunity to prevent future incidents. While public relations impact, legal implications, and user privacy considerations are important factors to address during the aftermath of an incident, they come into play after the immediate concern of identifying and mitigating the insider threat through effective data collection and analysis. A focus on evidence collection enables organizations to act decisively and effectively respond to the threat, which can ultimately inform how they handle legal and public relations aspects later on.

8. How is quantitative risk analysis defined?

A. Probability of loss X value of loss

B. Value of loss/ Probability of loss

C. Probability of loss + value of loss

D. Probability of loss - value of loss

Quantitative risk analysis is a method that evaluates risk in numerical terms to provide a more empirical basis for decision-making. The formula that defines this analysis is the probability of loss multiplied by the value of loss. This approach allows organizations to understand the potential financial impact of various risks they may face. By using this formula, organizations can prioritize risks based on their potential cost if they were to occur, enabling more effective allocation of resources towards risk management and mitigation strategies. This quantitative assessment is particularly valuable for decision-makers as it translates potential risks into concrete financial terms, making it easier to justify investments in risk management initiatives. The other options do not accurately represent the formula used in quantitative risk analysis. They do not provide a direct relationship between the probability of loss and the value of loss as intended in this analysis framework. Understanding the correct definition is crucial for professionals involved in risk assessment and management, ensuring they can make informed decisions based on solid, quantifiable data.

9. Spoofing, session hijacking, DoS attacks, firewall and IDS attacks are all considered what type of information security threat?

A. Host threat

B. Network threat

C. System threat

D. Application threat

The correct classification for spoofing, session hijacking, denial-of-service (DoS) attacks, and attacks on firewalls and intrusion detection systems (IDS) is that they are all network threats. This categorization is appropriate because these types of threats primarily target the integrity, confidentiality, and availability of networked systems and the data transmitted across networks. Spoofing involves impersonating another entity to manipulate or deceive communication over a network, while session hijacking specifically refers to exploiting a valid computer session to gain unauthorized access. DoS attacks aim to disrupt service availability by overwhelming network resources, and attacks on firewalls and IDS are designed to bypass security mechanisms meant to protect networked environments. In contrast, host threats generally involve issues related to individual devices, such as malware or physical theft of hardware. System threats may encompass issues affecting an entire system's operational integrity or performance, but they do not specifically target the network domain. Application threats pertain to vulnerabilities and attacks directed specifically at software applications, making them less relevant for the scenarios listed. Thus, identifying these threats as network threats is critical for building appropriate defenses and response strategies in cybersecurity.

10. What motivates an insider attack where an employee publicizes sensitive information for a political cause?

A. Hacktivism

B. Corporate Espionage

C. Work-Related Grievance

D. Curiosity

The motivation behind an insider attack where an employee publicizes sensitive information for a political cause is best described as hacktivism. Hacktivism is a blend of hacking and activism, where individuals or groups leverage technology and the internet to promote political agendas or social change. In this context, the employee is using insider knowledge and access to highlight issues, often motivated by strong political beliefs or a desire to bring attention to perceived injustices. This action aligns with the principles of hacktivism, as it not only involves breaking ethical or legal boundaries but also aims to incite change or raise awareness regarding a particular cause. It's characterized by the idea that the individual believes they are fighting for a just cause, regardless of the legal ramifications of their actions. Other motivations such as corporate espionage typically involve gaining a competitive advantage or financial benefit, while work-related grievances might manifest as internal sabotage rather than publicizing information for broader political ends. Curiosity denotes a desire to know more, which doesn't inherently have the same activist aim as hacktivism.