

EC Council

112-52

EC-Council Ethical Hacking Essentials (EHE)

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

- 1. Up to Date products, reliable and verified.**
- 2. Questions and Answers in PDF Format.**



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/112-52>

Latest Version: 6.1

Question: 1

Which of the following types of malware is specifically designed to replicate itself and spread to other computers?

- A. Virus
- B. Trojan
- C. Spyware
- D. Adware

Answer: A

Question: 2

Which of the following is a social engineering technique?

- A. Phishing
- B. Firewalking
- C. port scanning
- D. Traffic analysis

Answer: A

Question: 3

What is the main focus of the General Data Protection Regulation (GDPR)?

- A. Protecting financial data in banking institutions
- B. Ensuring the security of healthcare information
- C. Protecting the privacy and personal data of EU citizens
- D. Establishing cybersecurity standards for critical infrastructure

Answer: C

Question: 4

Which of the following is NOT a type of hacker?

- A. Black Hat
- B. Grey Hat
- C. Green Hat
- D. White Hat

Answer: C

Question: 5

Which of the following BEST helps prevent session hijacking?

- A. Use of HTTPS instead of HTTP
- B. Changing network infrastructure frequently
- C. Clearing browser cookies regularly
- D. Disabling logging mechanisms

Answer: A

Question: 6

Which action MOST improves IoT device security?

- A. Changing default passwords
- B. Disabling firmware updates
- C. Using unencrypted communication channels
- D. Exposing devices directly to the internet

Answer: A

Question: 7

Which stage of the Cyber Kill Chain involves delivering the weaponized payload to the target?

- A. Reconnaissance
- B. Weaponization
- C. Installation
- D. Delivery

Answer: D

Question: 8

What is the primary focus of Operational Technology (OT) systems?

- A. Data analytics and processing
- B. User experience and interface design
- C. Monitoring and controlling physical devices
- D. Enhancing network security

Answer: C

Question: 9

Which phase of penetration testing involves attempting to exploit identified vulnerabilities?

- A. Reconnaissance
- B. Reporting
- C. Exploitation
- D. Remediation

Answer: C

Question: 10

In the context of vulnerability assessment, what is the significance of false positives?

- A. They indicate vulnerabilities that do not actually exist.
- B. They represent accurately identified vulnerabilities.
- C. They are undetected vulnerabilities.
- D. They refer to vulnerabilities that are already mitigated.

Answer: A

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>