Vendor: EC-Council

Exam Code: 112-52

Exam Name: EC-Council Ethical Hacking Essentials (EHE)

Version: DMEO

QUESTION 1
Which technique is commonly used to enable packet sniffing on a network?

A. Promiscuous mode
B. Session timeout exploitation
C. SQL injection
D. DNS tunneling

Answer: A

QUESTION 2
Which mobile-specific attack can be performed through public Wi-Fi networks?

A. Rogue AP attack
B. Buffer overflow
C. Social engineering
D. Brute force attack

Answer: A

QUESTION 3
Which of the following best describes a zero-day vulnerability?

A. A vulnerability that is exploited before the vendor has issued a patch
B. A vulnerability that affects all versions of a software
C. A vulnerability that exists for zero days before being detected
D. A vulnerability that does not require user interaction to be exploited

Answer: A

QUESTION 4
What is a critical countermeasure for protecting OT environments?

A. Implementing deep packet inspection
B. Enforcing strict data retention policies
C. Applying comprehensive patch management
D. Using a strong social media policy

Answer: C

QUESTION 5
What is a primary security measure to prevent Cross-Site Scripting (XSS) attacks?

A. Implementing Content Security Policy (CSP)
B. Using database encryption
C. Enabling CORS on the server
D. Using parameterized queries

Answer: A

QUESTION 6
Which strategy is crucial for enhancing the security of IoT devices?

A. Enabling Wi-Fi Protected Setup (WPS)
B. Conducting penetration testing regularly
C. Using non-standard communication protocols
D. Avoiding the use of encryption

Answer: B

QUESTION 7
Which security measure MOST effectively reduces unauthorized access in cloud environments?

A. Enforcing strong access control policies
B. Disabling encryption for performance
C. Allowing unrestricted access
D. Using shared administrator accounts

Answer: A

QUESTION 8
What is the primary purpose of packet sniffing in a network security context?

A. To increase the bandwidth of the network
B. To monitor and analyze network traffic
C. To enhance the speed of network packet transmission
D. To distribute network traffic evenly across the network

Answer: B

QUESTION 9
What is the role of containerization in cloud security?

A. To improve system uptime
B. To isolate applications and improve security
C. To allow unregulated access to shared resources
D. To ensure high network bandwidth

Answer: B

QUESTION 10
Which deployment model in cloud computing is owned, managed, and operated by a business, organization, or entity exclusively?

A. Public cloud
B. Private cloud
C. Hybrid cloud

D. Community cloud

Answer: B

QUESTION 11
Which technique involves trying all possible combinations of characters until the correct password is found?

A. Phishing
B. Brute force attack
C. Dictionary attack
D. Social engineering

Answer: B

QUESTION 12
Which of the following best describes a vulnerability in the context of information security?

A. An unauthorized attempt to access a system
B. A weakness in a system that could be exploited
C. A method for encrypting data
D. A tool used to assess security posture

Answer: B

QUESTION 13
Which phase of the ethical hacking cycle involves gathering information about the target?

A. Reconnaissance
B. Data Encryption
C. Risk Acceptance
D. Server Monitoring

Answer: A

QUESTION 14
Which of the following is a common wireless network-specific attack technique?

A. SQL injection
B. IV attack
C. Phishing
D. Cross-site scripting

Answer: B

QUESTION 15
Which of the following is considered a physical threat?

A. SQL injection
B. Phishing
C. Tailgating
D. Cross-site scripting

Answer: C

QUESTION 16
What is the best way to mitigate social engineering attacks in an organization?

A. Implement stronger passwords
B. Conduct regular employee security awareness training
C. Install antivirus software on all machines
D. Use encryption for sensitive data

Answer: B

QUESTION 17
What is the main goal of a Bluetooth attack?

A. To disrupt wireless communication
B. To gain unauthorized access to a device through its Bluetooth connection
C. To decrypt Wi-Fi traffic
D. To steal credentials from Wi-Fi networks

Answer: B

QUESTION 18
What is an effective countermeasure against wireless sniffing?

A. Using strong encryption protocols like WPA3
B. Employing MAC address filtering
C. Setting up hidden SSIDs
D. Regular password changes

Answer: A

QUESTION 19
Which attack involves overwhelming a web server with traffic, making it inaccessible to legitimate users?

A. SQL Injection
B. Cross-Site Scripting (XSS)
C. Denial of Service (DoS)
D. Cross-Site Request Forgery (CSRF)

Answer: C

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**