Vendor: EC-Council

Exam Code: 312-38

Exam Name: EC-Council Network Security Administrator
(ENSA)

Version: DEMO

QUESTION 1
Identify the method involved in purging technique of data destruction.

A. Degaussing
B. Wiping
C. Incineration
D. Overwriting

Answer: B

QUESTION 2
Which type of modulation technique is used in local area wireless networks (LAWNs)?

A. FHSS
B. DSSS
C. MIMO-OFDM
D. OFDM

Answer: B

QUESTION 3
How is the chip-level security of an IoT device achieved?

A. Closing insecure network services
B. Changing the password of the router
C. Encrypting JTAG interface
D. Keeping the device on a flat network

Answer: C

QUESTION 4
Which RAID level system provides very good data performance but does not offer fault tolerance and data redundancy?

A. RAID level 5
B. RAID level 3
C. RAID level 0
D. RAID level 1

Answer: C

QUESTION 5
Which of the following is a data destruction technique that protects the sensitivity of information against a laboratory attack where an unauthorized individual uses signal processing recovery tools in a laboratory environment to recover the information?

A. Purging
B. Disposal
C. Destroying

D. Clearing

Answer: A

QUESTION 6
Hacktivists are threat actors, who can be described as _____ .

A. People motivated by monetary gains
B. People motivated by religious beliefs
C. People having political or social agenda
D. Disgruntled/terminated employees

Answer: C

QUESTION 7
Which of the following filters can be applied to detect an ICMP ping sweep attempt using Wireshark?

A. icmp.type==17
B. icmp.type==8
C. icmp.type==15
D. icmp.type==13

Answer: B

QUESTION 8
Who offers formal experienced testimony in court?

A. Evidence documenter
B. Attorney
C. Expert witness
D. Incident analyzer

Answer: C

QUESTION 9
Which type of training can create awareness among employees regarding compliance issues?

A. Training on data classification
B. Physical security awareness training
C. Social engineering awareness training
D. Security policy training

Answer: D

QUESTION 10
Which among the following options represents professional hackers with an aim of attacking systems for profit?

A. Organized hackers
B. Script kiddies
C. Hacktivists
D. Cyber terrorists

Answer: A

QUESTION 11
Which of following are benefits of using IoT devices in IoT-enabled environments?

I) IoT device can be connected anytime
II) IoT device can be connected at any place
III) IoT devices connected to anything

A. I and II
B. II
C. I, II, and III
D. I

Answer: C

QUESTION 12
Identify the correct order for a successful black hat operation.

A. Reconnaissance, Gaining Access, Scanning, Maintaining Access, and Covering Tracks
B. Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Covering Tracks
C. Reconnaissance, Scanning, Gaining Access, Covering Tracks, and Maintaining Access
D. Scanning, Reconnaissance, Gaining Access, Maintaining Access, and Covering Tracks

Answer: B

QUESTION 13
Which of the following indicators are discovered through an attacker's intent, their end goal or purpose, and a series of actions that they must take before being able to successfully launch an attack?

A. Indicators of compromise
B. Key risk indicators
C. Indicators of exposure
D. Indicators of attack

Answer: D

QUESTION 14
Which of the following is a drawback of traditional perimeter security?

A. Traditional VPNs follow identity-centric instead of trust-based network-centric approach
B. Traditional firewalls are static in nature

C. Traditional firewalls are dynamic in nature
D. Traditional perimeter security is identity-centric

Answer: B

QUESTION 15
According to standard IoT security practice, IoT Gateway should be connected to a _____ .

A. Secure router
B. Router that is connected to internal servers
C. Router that is connected to other subnets
D. Border router

Answer: D

QUESTION 16
Who is responsible for executing the policies and plans required for supporting the information technology and computer systems of an organization?

A. Chief Information Officer (CIO)
B. Business and functional managers
C. Senior management
D. IT security practitioners

Answer: A

QUESTION 17
Which of the following refers to the clues, artifacts, or evidence that indicate a potential intrusion or malicious activity in an organization's infrastructure?

A. Indicators of attack
B. Key risk indicators
C. Indicators of compromise
D. Indicators of exposure

Answer: C

QUESTION 18
Which of the following provides enhanced password protection, secured IoT connections, and encompasses stronger encryption techniques?

A. WEP
B. WPA3
C. WPA
D. WPA2

Answer: B

QUESTION 19
In _____ method, windows event logs are arranged in the form of a circular buffer.

A. Out-of Band Method
B. Overwriting Method
C. Non-Wrapping method
D. Wrapping method

Answer: D

QUESTION 20
Which of the following is a database encryption feature that secures sensitive data by encrypting it in client applications without revealing the encrypted keys to the data engine in MS SQL Server?

A. Always Encrypted
B. IsEncrypted Enabled
C. Allow Encrypted
D. NeverEncrypted disabled

Answer: A

QUESTION 21
Clement is the CEO of an IT firm. He wants to implement a policy allowing employees with a preapproved set of devices from which the employees choose devices (laptops, smartphones, and tablets) to access company data as per the organization's access privileges. Which among the following policies does Clement want to enforce?

A. CYOD policy
B. BYOD policy
C. COPE policy
D. COBO policy

Answer: A

QUESTION 22
Which of the following filters can be used to detect UDP scan attempts using Wireshark?

A. icmp.type==8 or icmp.type==0
B. icmp.type==15
C. icmp.type==3 and icmp.code==3
D. icmp.type==13

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**