312-38 Q&As

Certified Network Defender (CND)

Pass EC-COUNCIL 312-38 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/312-38.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Simran is a network administrator at a start-up called Revolution. To ensure that neither party in the company can deny getting email notifications or any other communication, she mandates authentication before a connection establishment or message transfer occurs. What fundamental attribute of network defense is she enforcing?

A. Integrity

B. Non-repudiation

C. Confidentiality

D. Authentication

Correct Answer: B

QUESTION 2

David is working in a mid-sized IT company. Management asks him to suggest a framework that can be used effectively to align the IT goals to the business goals of the company. David suggests the _____ framework, as it provides a set of controls over IT and consolidates them to form a framework.

A. COBIT

B. ITIL

C. ISO 27007

D. RMIS

Correct Answer: A

QUESTION 3

Which of the following is a communication protocol multicasts messages and information of all the member IP multicast group?

A. IGMP

B. ICMP

C. BGP

D. None

E. EGP

Correct Answer: A

QUESTION 4

Which of the following is an electronic device that helps in forwarding data packets along networks?

A. Router

B. Hub

C. Repeater

D. Gateway

Correct Answer: A

QUESTION 5

Adam, a malicious hacker, has just succeeded in stealing a secure cookie via a XSS attack. He is able to replay the cookie even while the session is valid on the server. Which of the following is the most likely reason of this cause?

A. Encryption is performed at the network layer (layer 1 encryption).

B. Encryption is performed at the application layer (single encryption key).

C. No encryption is applied.

D. Two way encryption is applied.

Correct Answer: B

Single key encryption uses a single word or phrase as the key. The same key is used by the sender to encrypt and the receiver to decrypt. Sender and receiver initially need to have a secure way of passing the key from one to the other. With TLS or SSL this would not be possible. Symmetric encryption is a type of encryption that uses a single key to encrypt and decrypt data. Symmetric encryption algorithms are faster than public key encryption. Therefore, it is commonly used when a message sender needs to encrypt a large amount of data. Data Encryption Standard (DES) uses the symmetric encryption key algorithm to encrypt data.

QUESTION 6

Will is working as a Network Administrator. Management wants to maintain a backup of all the company data as soon as it starts operations. They decided to use a RAID backup storage technology for their data backup plan. To implement

the RAID data backup storage, Will sets up a pair of RAID disks so that all the data written to one disk is copied automatically to the other disk as well. This maintains an additional copy of the data.

Which RAID level is used here?

A. RAID 3

B. RAID 1

C. RAID 5

D. RAID 0

Correct Answer: B

QUESTION 7

Which of the following is a process that detects a problem, determines its cause, minimizes the damages, resolves the problem, and documents each step of response for future reference?

A. Incident response

B. Incident handling

C. Incident management

D. Incident planning

Correct Answer: A

Incident response is a process that detects a problem, determines its cause, minimizes the damages, resolves the problem, and documents each step of response for future reference. One of the primary goals of incident response is to "freeze the scene". There is a close relationship between incident response, incident handling, and incident management. The primary goal of incident handling is to contain and repair any damage caused by an event and to prevent any further damage. Incident management manages the overall process of an incident by declaring the incident and preparing documentation and post-mortem reviews after the incident has occurred. Answer option B is incorrect. The primary goal of incident handling is to contain and repair any damage caused by an event and to prevent any further damage. Answer option C is incorrect. It manages the overall process of an incident by declaring the incident and preparing documentation and post-mortem reviews after the incident has occurred. Answer option D is incorrect. This is an invalid option.

QUESTION 8

Which of the following is a software tool used in passive attacks for capturing network traffic?

A. Intrusion prevention system

B. Intrusion detection system

C. Warchalking

D. Sniffer

Correct Answer: D

A sniffer is a software tool that is used to capture any network traffic. Since a sniffer changes the NIC of the LAN card into promiscuous mode, the NIC begins to record incoming and outgoing data traffic across the network. A sniffer attack is

a passive attack because the attacker does not directly connect with the target host. This attack is most often used to grab logins and passwords from network traffic. Tools such as Ethereal, Snort, Windump, EtherPeek, Dsniff are some good

examples of sniffers. These tools provide many facilities to users such as graphical user interface, traffic statistics graph, multiple sessions tracking, etc. Answer option A is incorrect. An intrusion prevention system (IPS) is a network security

device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities.

When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass.

Answer option B is incorrect. An IDS (Intrusion Detection System) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.

Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging

information about them, attempting to stop them, and reporting them to security administrators.

Answer option C is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the

pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

QUESTION 9

Which of the Windows security component is responsible for controlling access of a user to Windows resources?

A. Network Logon Service (Netlogon)

B. Security Accounts Manager (SAM)

C. Security Reference Monitor (SRM)

D. Local Security Authority Subsystem (LSASS)

Correct Answer: D

QUESTION 10

Chris is a senior network administrator. Chris wants to measure the Key Risk Indicator (KRI) to assess the organization. Why is Chris calculating the KRI for his organization? It helps Chris to:

A. Identifies adverse events

B. Facilitates backward viewing

C. Notifies when risk has reached threshold levels

D. Facilitates post incident management

Correct Answer: C

QUESTION 11

Which of the following incident handling stage removes the root cause of the incident?

A. Eradication

B. Recovery

C. Detection

D. Containment

Correct Answer: A

QUESTION 12

Which BC/DR activity includes action taken toward resuming all services that are dependent on business-critical applications?

A. Response

B. Recovery

C. Resumption

D. Restoration

Correct Answer: B

QUESTION 13

Identity the method involved in purging technique of data destruction.

A. Incineration

B. Overwriting

C. Degaussing

D. Wiping

Correct Answer: B

QUESTION 14

Which of the following is virtually unsolicited e-mail messages, often with commercial content, in large quantities of indiscriminate set of recipients? Each correct answer represents a complete solution.

A. E-mail scam

B. spam

C. E-mail harassment

Correct Answer: B

QUESTION 15

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

A. icmp.type==8

B. icmp.type==13

C. icmp.type==17

D. icmp.type==15

Correct Answer: A