Free Questions for 212-82 by ebraindumps

Shared by Hale on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Kayden successfully cracked the final round of interview at an organization. After few days, he received his offer letter through an official company email address. The email stated that the selected candidate should respond within a specified time. Kayden accepted the opportunity and provided e-signature on the offer letter, then replied to the same email address. The company validated the e-signature and added his details to their database. Here, Kayden could not deny company's message, and company could not deny Kayden's signature.

Which of the following information security elements was described in the above scenario?

Options:

A) Availability

B) Non-repudiation

C) Integrity

D) Confidentiality

Answer:

B

Question 2

Question Type: **MultipleChoice**

Thomas, an employee of an organization, is restricted to access specific websites from his office system. He is trying to obtain admin credentials to remove the restrictions. While waiting for an opportunity, he sniffed communication between the administrator and an application server to retrieve the admin credentials. Identify the type of attack performed by Thomas in the above scenario.

Options:

A) Vishing

B) Eavesdropping

C) Phishing

D) Dumpster diving

Answer:

B

Question 3

Question Type: **MultipleChoice**

Karter, a security professional, deployed a honeypot on the organization's network for luring attackers who attempt to breach the network. For this purpose, he configured a type of honeypot that simulates a real OS as well as applications and services of a target network. Furthermore, the honeypot deployed by Karter only responds to preconfigured commands.

Identify the type of Honeypot deployed by Karter in the above scenario.

Options:

A) Low-interaction honeypot

B) Pure honeypot

C) Medium-interaction honeypot

D) High-interaction honeypot

Answer:

A

Question 4

Question Type: **MultipleChoice**

Mark, a security analyst, was tasked with performing threat hunting to detect imminent threats in an organization's network. He generated a hypothesis based on the observations in the initial step and started the threat hunting process using existing data collected from DNS and proxy logs.

Identify the type of threat hunting method employed by Mark in the above scenario.

Options:

A) Entity-driven hunting

B) TTP-driven hunting

C) Data-driven hunting

D) Hybrid hunting

Answer:

C

Question 5

Question Type: **MultipleChoice**

Kayden successfully cracked the final round of interview at an organization. After few days, he received his offer letter through an official company email address. The email stated that the selected candidate should respond within a specified time. Kayden accepted the opportunity and provided e-signature on the offer letter, then replied to the same email address. The company validated the e-signature and added his details to their database. Here, Kayden could not deny company's message, and company could not deny Kayden's signature.

Which of the following information security elements was described in the above scenario?

Options:

A) Availability

B) Non-repudiation

C) Integrity

D) Confidentiality

Answer:

B

Question 6

Question Type: **MultipleChoice**

Thomas, an employee of an organization, is restricted to access specific websites from his office system. He is trying to obtain admin credentials to remove the restrictions. While waiting for an opportunity, he sniffed communication between the administrator and an application server to retrieve the admin credentials. Identify the type of attack performed by Thomas in the above scenario.

Options:

A) Vishing

B) Eavesdropping

C) Phishing

D) Dumpster diving

Answer:

B

Question 7

Question Type: **MultipleChoice**

Karter, a security professional, deployed a honeypot on the organization's network for luring attackers who attempt to breach the network. For this purpose, he configured a type of honeypot that simulates a real OS as well as applications and services of a target network. Furthermore, the honeypot deployed by Karter only responds to preconfigured commands.

Identify the type of Honeypot deployed by Karter in the above scenario.

Options:

A) Low-interaction honeypot

B) Pure honeypot

C) Medium-interaction honeypot

D) High-interaction honeypot

Answer:

A

Question 8

Question Type: **MultipleChoice**

Mark, a security analyst, was tasked with performing threat hunting to detect imminent threats in an organization's network. He generated a hypothesis based on the observations in the initial step and started the threat hunting process using existing data collected from DNS and proxy logs.

Identify the type of threat hunting method employed by Mark in the above scenario.

Options:

A) Entity-driven hunting

B) TTP-driven hunting

C) Data-driven hunting

D) Hybrid hunting

Answer:

C

20%
DISCOUNT