ECCouncil

212-82 Exam

Certified Cybersecurity Technician

Question: 1

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.

A. Vishing
B. Eavesdropping
C. Phishing
D. Dumpster diving

Answer: B

Explanation:

Question: 2

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?

A. Availability
B. Non-repudiation
C. Integrity
D. Confidentiality

Answer: B

Explanation:

Question: 3

Sam, a software engineer, visited an organization to give a demonstration on a software tool that helps in business development. The administrator at the organization created a least privileged account on a system and allocated that system to Sam for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file

in the system.
Which of the following type of accounts the organization has given to Sam in the above scenario?

A. Service account
B. Guest account
C. User account
D. Administrator account

Answer: B

Explanation:

Question: 4

Myles, a security professional at an organization, provided laptops for all the employees to carry out the business processes from remote locations. While installing necessary applications required for the business, Myles has also installed antivirus software on each laptop following the company's policy to detect and protect the machines from external malicious events over the Internet.
Identify the PCI-DSS requirement followed by Myles in the above scenario.

A. PCI-DSS requirement no 1.3.2
B. PCI-DSS requirement no 1.3.5
C. PCI-DSS requirement no 5.1
D. PCI-DSS requirement no 1.3.1

Answer: C

Explanation:

Question: 5

Ashton is working as a security specialist in SoftEight Tech. He was instructed by the management to strengthen the Internet access policy. For this purpose, he implemented a type of Internet access policy that forbids everything and imposes strict restrictions on all company computers, whether it is system or network usage.
Identify the type of Internet access policy implemented by Ashton in the above scenario.

A. Paranoid policy
B. Prudent policy
C. Permissive policy
D. Promiscuous policy

Answer: A