

PassTest

Bessere Qualität , bessere Dienstleistungen!



Q&A

<http://www.passtest.de>

Einjährige kostenlose Aktualisierung

Exam : **212-82**

Title : Certified Cybersecurity
Technician(C|CT)

Version : DEMO

1. Thomas, an employee of an organization, is restricted from accessing 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:

The correct answer is B, as it identifies the type of attack performed by Thomas in the above scenario. Eavesdropping is a type of attack that involves intercepting and listening to the communication between two parties without their knowledge or consent. Thomas performed eavesdropping by sniffing communication between the administrator and an application server to retrieve the admin credentials. Option A is incorrect, as it does not identify the type of attack performed by Thomas in the above scenario. Vishing is a type of attack that involves using voice calls to trick people into revealing sensitive information or performing malicious actions. Thomas did not use voice calls but sniffed network traffic. Option C is incorrect, as it does not identify the type of attack performed by Thomas in the above scenario. Phishing is a type of attack that involves sending fraudulent emails or messages that appear to be from legitimate sources to lure people into revealing sensitive information or performing malicious actions. Thomas did not send any emails or messages but sniffed network traffic. Option D is incorrect, as it does not identify the type of attack performed by Thomas in the above scenario. Dumpster diving is a type of attack that involves searching through trash or discarded items to find valuable information or resources. Thomas did not search through trash or discarded items but sniffed network traffic.

Reference: Section 2.2

2. Kayden successfully cracked the final round of interviews at an organization. After a 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 an 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 the company's message, and the 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:

The correct answer is B, as it describes the information security element that was described in the above scenario. Non-repudiation is an information security element that ensures that a party cannot deny sending or receiving a message or performing an action. In the above scenario, non-repudiation was described, as Kayden could not deny company's message, and company could not deny Kayden's signature. Option A is incorrect, as it does not describe the information security element that was

described in the above scenario. Availability is an information security element that ensures that authorized users can access and use information and resources when needed. In the above scenario, availability was not described, as there was no mention of access or use of information and resources. Option C is incorrect, as it does not describe the information security element that was described in the above scenario. Integrity is an information security element that ensures that information and resources are accurate and complete and have not been modified by unauthorized parties. In the above scenario, integrity was not described, as there was no mention of accuracy or completeness of information and resources. Option D is incorrect, as it does not describe the information security element that was described in the above scenario. Confidentiality is an information security element that ensures that information and resources are protected from unauthorized access and disclosure. In the above scenario, confidentiality was not described, as there was no mention of protection or disclosure of information and resources.

Reference: , Section 3.1

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 types 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:

The correct answer is B, as it identifies the type of account that the organization has given to Sam in the above scenario. A guest account is a type of account that allows temporary or limited access to a system or network for visitors or users who do not belong to the organization. A guest account typically has minimal privileges and permissions and can only access certain files or applications. In the above scenario, the organization has given Sam a guest account 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. Option A is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. A service account is a type of account that allows applications or services to run on a system or network under a specific identity. A service account typically has high privileges and permissions and can access various files or applications. In the above scenario, the organization has not given Sam a service account for the demonstration. Option C is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. A user account is a type of account that allows regular access to a system or network for employees or members of an organization. A user account typically has moderate privileges and permissions and can access various files or applications depending on their role. In the above scenario, the organization has not given Sam a user account for the demonstration. Option D is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. An administrator account is a type of account that allows full access to a system or network for administrators or managers of an organization. An administrator account typically has the highest privileges and permissions and can

access and modify any files or applications. In the above scenario, the organization has not given Sam an administrator account for the demonstration.

Reference: , Section 4.1

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:

The correct answer is C, as it identifies the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS is a set of standards that aims to protect cardholder data and ensure secure payment transactions. PCI-DSS has 12 requirements that cover various aspects of security such as network configuration, data encryption, access control, vulnerability management, monitoring, and testing. PCI-DSS requirement no 5.1 states that "Protect all systems against malware and regularly update anti-virus software or programs". In the above scenario, Myles followed this requirement by installing antivirus software on each laptop to detect and protect the machines from external malicious events over the Internet. Option A is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.2 states that "Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet". In the above scenario, Myles did not follow this requirement, as there was no mention of outbound traffic or cardholder data environment. Option B is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.5 states that "Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment". In the above scenario, Myles did not follow this requirement, as there was no mention of inbound or outbound traffic or cardholder data environment. Option D is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.1 states that "Implement a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data". In the above scenario, Myles did not follow this requirement, as there was no mention of firewall configuration or publicly accessible servers or system components storing cardholder data.

Reference: Section 5.2

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

Explanation:

The correct answer is A, as it identifies the type of Internet access policy implemented by Ashton in the above scenario. An Internet access policy is a set of rules and guidelines that defines how an organization's employees or members can use the Internet and what types of websites or services they can access.

There are different types of Internet access policies, such as:

Paranoid policy: This type of policy forbids everything and imposes strict restrictions on all company computers, whether it is system or network usage. This policy is suitable for organizations that deal with highly sensitive or classified information and have a high level of security and compliance requirements.

Prudent policy: This type of policy allows some things and blocks others and imposes moderate restrictions on company computers, depending on the role and responsibility of the user. This policy is suitable for organizations that deal with confidential or proprietary information and have a medium level of security and compliance requirements.

Permissive policy: This type of policy allows most things and blocks few and imposes minimal restrictions on company computers, as long as the user does not violate any laws or regulations. This policy is suitable for organizations that deal with public or general information and have a low level of security and compliance requirements.

Promiscuous policy: This type of policy allows everything and blocks nothing and imposes no restrictions on company computers, regardless of the user's role or responsibility. This policy is suitable for organizations that have no security or compliance requirements and trust their employees or members to use the Internet responsibly.

In the above scenario, Ashton implemented a paranoid policy that forbids everything and imposes strict restrictions on all company computers, whether it is system or network usage. Option B is incorrect, as it does not identify the type of Internet access policy implemented by Ashton in the above scenario. A prudent policy allows some things and blocks others and imposes moderate restrictions on company computers, depending on the role and responsibility of the user. In the above scenario, Ashton did not implement a prudent policy, but a paranoid policy. Option C is incorrect, as it does not identify the type of Internet access policy implemented by Ashton in the above scenario. A permissive policy allows most things and blocks few and imposes minimal restrictions on company computers, as long as the user does not violate any laws or regulations. In the above scenario, Ashton did not implement a permissive policy, but a paranoid policy. Option D is incorrect, as it does not identify the type of Internet access policy implemented by Ashton in the above scenario. A promiscuous policy allows everything and blocks nothing and imposes no restrictions on company computers, regardless of the user's role or responsibility. In the above scenario, Ashton did not implement a promiscuous policy, but a paranoid policy.

Reference: , Section 6.2