Security Principles

Learn about the security triad and common security models and principles.

Resumen de los principios de seguridad:

En esta sala de TryHackMe aprenderás sobre los pilares de la seguridad, sus principios, conceptos fundamentales y diferencias.

Tarea 1: Introducción.

- **Respuesta: No requiere una respuesta**, haz clic en enviar.

Tarea 2: CIA

Conociendo la famosa tríada CIA, conceptos de confidencialidad, integridad y disponibilidad, su consideración en diferentes casos y como podemos ir más allá de la misma y el conjunto de seis elementos de seguridad de Héxada Parkeriana.

Clic en “Ver Sitio” y responde las 5 preguntas para obtener la flag de respuesta.

P 1/5: As the troops got deployed, the leader stressed that they should not communicate their location to anyone while the mission was ongoing. Which security function did the leader want to have?

R: Confidentiality.

P 2/5: At a police checkpoint, the police officer suspected that the vehicle registration papers were fake. Which security function does the officer think is lacking?

R: Integrity

P 3/5: Two companies are negotiating a certain agreement; however, they want to keep the details of the agreement secret. Which security pillar are they emphasizing?

R: Confidentiality

P 4/5: One hotel is stressing that the Internet over its WiFi network must be accessible 24 hours a day, seven days a week. Which security pillar is the hotel requiring?

R: Availability

P 5/5: You went to cash out a cheque, and the bank teller made you wait for five minutes as they confirmed the signature of the cheque's issuer. Which security function is the bank teller checking?

R: Integrity

- **Respuesta: THM{CIA_TRIAD}**

Tarea 3: DAD

Nos adentramos en el opuesto de la Tríada CIA conocida como la Tríada DAD conociendo sus conceptos con ejemplos sobre la divulgación, alteración y destrucción/negación.

- **Pregunta:** The attacker managed to gain access to customer records and dumped them online. What is this attack?
- **Respuesta: Disclosure**

- **Pregunta:** A group of attackers were able to locate both the main and the backup power supply systems and switch them off. As a result, the whole network was shut down. What is this attack?
- **Respuesta: Destruction/Denial**

Tarea 4: Conceptos fundamentales de los modelos de seguridad

Presentación de los modelos Bell-LaPadula, Integridad de Biba y Clark-Wilson, concepto de las reglas de los diferentes modelos, que pretenden lograr cada modelo para garantizar un sistema con una o más funciones de seguridad y otros ejemplos de modelos de seguridad.

Clic en “Ver Sitio” y responde las 5 preguntas para obtener la flag de respuesta.

P 1/4: Which model dictates “no read down”?

R: Biba

P 2/4: Which model states “no read up”?

R: Bell-LaPadula

P 3/4: Which model teaches “no write down”?

R: Bell-LaPadula

P 4/4: Which model forces “no write up”?

R: Biba

- **Respuesta: THM{SECURITY_MODELS}**

Tarea 5: Defensa en profundidad

Aprenderemos sobre la creación de una defensa en profundidad con seguridad de múltiples niveles o multinivel con el objetivo de asegurar uno o más objetos de valor.

- **Respuesta:** No requiere una respuesta, haz clic en enviar.

Tarea 6: ISO/IEC 19249

Empezamos con tener en cuenta la norma ISO/IEC 19249, su objetivo de comprender mejor lo que enseñarían las organizaciones internaciones con respecto a los principios de seguridad, su enumeración de cinco principios arquitectónicos y la enseñanza de diseño por parte de la normativa.

- **Pregunta:** Which principle are you applying when you turn off an insecure server that is not critical to the business?
- **Respuesta:** 2

- **Pregunta:** Your company hired a new sales representative. Which principle are they applying when they tell you to give them access only to the company products and prices?
- **Respuesta:** 1

- **Pregunta:** While reading the code of an ATM, you noticed a huge chunk of code to handle unexpected situations such as network disconnection and power failure. Which principle are they applying?
- **Respuesta:** 5

Tarea 7: Confianza Cero vs Confiar pero verificar

Nos adentramos en una situación donde la confianza en nuestro mundo es un tema complejo y que para ello vamos a necesitar aprender como se aplican dos principios relacionados con la confianza los cuales son Zero Trust (Confianza cero) y Trust but Verify (Confiar pero verificar).

- **Respuesta:** No requiere una respuesta, haz clic en enviar.

Tarea 8: Amenaza vs Riesgo

En esta tarea aprenderemos sobre los términos de Vulnerabilidad, Amenaza y Riesgo, sus significados y en que se diferencian en dos ejemplos muy interesantes.

- **Respuesta:** **No requiere una respuesta**, haz clic en enviar.

Tarea 9: Conclusión

Hemos logrado en esta sala obtener conocimiento de muchos conceptos clave de seguridad como la confidencialidad, integridad, disponibilidad, amenazas y riesgos, además de modelos y principios como defensa en profundidad, tener en normas como la ISO/IEC 19249 y confianza cero. También se destacó la importancia del Modelo de Responsabilidad Compartida en entornos de nube.

- **Respuesta:** **No requiere una respuesta**, haz clic en enviar.