Actividad 1

Consigna

> 💡 **Escenario conceptual:** Imagina que estás diseñando un sistema de detección de ciberataques para proteger una plataforma web. Este sistema debe identificar posibles acciones maliciosas que un atacante pueda intentar realizar sobre la plataforma.

1. Indicar algunos ejemplos de Acciones posibles del atacante:
2. Indicar las Funciones del sistema de detección A su vez, el sistema de detección de
   ataques debe reaccionar para intentar evitar o mitigar estas acciones. ¿Qué técnicas o
   herramientas puede usar el sistema para detectar estos ataques?
3. Explicar cómo se aplicaría la poda alfa-beta
4. Construir un árbol de decisión simplificado

1. - Ataque de fuerza bruta
   - Intentar inyectar código malicioso
   - Ataque DDoS
   - XSS
   - Phishing
   - Alteración de privilegios
   - Robo de datos

2. - Implementar herramientas IDS/IPS
   - Revisar ingresos de cuentas y movimientos
   - Limitar intentos de Login
   - Aplicar autenticación Multifactor
   - Usar SQLmap
   - Limitar número de solicitudes que un usuario puede hacer
   - Capacitaciones para el Phishing
   - Control de Acceso Basado en Roles
   - PenTest
   - Implementar Cifrado de datos

3. **Alfa (Daño máximo permitido en la plataforma):** Este valor representa el máximo daño que la plataforma web puede soportar o que el sistema de seguridad considera como un riesgo aceptable en cualquier momento. A medida que se identifican diferentes ataques (fuerza bruta, inyección de código, etc.), el valor alfa se actualiza si el daño potencial aumenta.

   Beta (Nivel mínimo de riesgo aceptable para la plataforma): Este valor representa el nivel más bajo de riesgo que el sistema de seguridad puede garantizar al aplicar sus contramedidas. a medida que el sistema implementa respuestas defensivas, el valor beta refleja cuán bien esas medidas están protegiendo la plataforma. Si una medida de seguridad logra reducir el daño bajo este valor, este sistema deja de analizar más rutas.

   Beneficio: Reduce la cantidad de análisis de ataques y contramedidas necesarias, lo que permite optimizar la detección de ciberataques. Esto es esencial en un entorno web donde múltiples vectores de ataque podrían estar ocurriendo simultáneamente, pero solo algunos representan un riesgo significativo. El sistema se enfoca en los ataques más peligrosos y deja de analizar aquellos que ya están mitigados por las defensas existentes.

4. **Nodos de ataque:** Cada acción representa un posible ataque. Estas acciones se convierten en los nodos del árbol.

   Nodos de decisión: Cada respuesta es una contramedida especifica a un ataque

Crear el árbol:
- El árbol comienza con un nodo raíz que representa el sistema siendo atacado
- Cada nivel del árbol representa un ataque potencial seguido de una respuesta defensiva
- En cada nodo, se evalúa el impacto del ataque y la efectividad de la respuesta, y se continúa con otras posibles acciones del atacante