**1. Ejemplos de Acciones Posibles del Atacante**

Algunas acciones maliciosas que un atacante podría intentar realizar sobre una plataforma web incluyen:

* **Inyección SQL**: Insertar código SQL malicioso en campos de entrada para manipular la base de datos.
* **Cross-Site Scripting (XSS)**: Inyectar scripts maliciosos en páginas web que se ejecutan en el navegador de los usuarios.
* **Ataques de fuerza bruta**: Intentar adivinar contraseñas mediante múltiples intentos de inicio de sesión.
* **Denegación de Servicio (DoS/DDoS)**: Sobrecargar el servidor con tráfico para hacer que el servicio sea inaccesible.
* **Phishing**: Engañar a los usuarios para que revelen información sensible mediante correos electrónicos o sitios web falsos.
* **Explotación de vulnerabilidades**: Aprovechar fallos en el software o configuraciones incorrectas para obtener acceso no autorizado.
* **Manipulación de sesiones**: Robar o manipular cookies de sesión para suplantar a un usuario legítimo.

**2. Funciones del Sistema de Detección y Técnicas de Detección**

El sistema de detección de ciberataques debe realizar las siguientes funciones:

* **Monitoreo continuo**: Observar el tráfico y las actividades en la plataforma en tiempo real.
* **Detección de anomalías**: Identificar comportamientos que se desvían de los patrones normales.
* **Análisis de firmas**: Comparar actividades con patrones conocidos de ataques.
* **Respuesta automática**: Tomar medidas inmediatas para mitigar el impacto de un ataque detectado.
* **Registro y reporte**: Registrar eventos de seguridad y generar informes para análisis posteriores.

**Técnicas o herramientas que puede usar el sistema para detectar estos ataques:**

* **Firewalls**: Para filtrar tráfico malicioso.
* **Sistemas de Detección de Intrusos (IDS)**: Para monitorear y analizar el tráfico en busca de actividades sospechosas.
* **Sistemas de Prevención de Intrusos (IPS)**: Para bloquear automáticamente actividades maliciosas.
* **Análisis de comportamiento**: Usar machine learning para detectar anomalías en el comportamiento de los usuarios.
* **Honeypots**: Sistemas engañosos para atraer y estudiar a los atacantes.
* **Escáneres de vulnerabilidades**: Para identificar y corregir fallos en el sistema antes de que sean explotados.

**3. Aplicación de la Poda Alfa-Beta**

La **poda alfa-beta** es una técnica de optimización utilizada en algoritmos de búsqueda en árboles de decisión, como los utilizados en juegos o en la toma de decisiones automatizada. En el contexto de un sistema de detección de ciberataques, la poda alfa-beta podría aplicarse en un sistema de toma de decisiones basado en reglas o en un sistema de inteligencia artificial que evalúa múltiples posibles respuestas a un ataque.

**Cómo se aplicaría:**

1. **Árbol de decisión**: Se construye un árbol donde cada nodo representa una posible acción o estado del sistema (por ejemplo, bloquear una IP, alertar al administrador, etc.).
2. **Evaluación de nodos**: Cada nodo se evalúa en función de un criterio de utilidad (por ejemplo, minimizar el daño, maximizar la seguridad, etc.).
3. **Poda alfa-beta**: Durante la exploración del árbol, se eliminan ramas que no aportan valor a la decisión final. Por ejemplo, si una rama lleva a una decisión claramente peor que otra ya explorada, se descarta sin necesidad de explorarla completamente.
4. **Decisión final**: El sistema selecciona la acción óptima basándose en los nodos no podados.

**4. Árbol de Decisión Simplificado**

A continuación, se presenta un árbol de decisión simplificado para un sistema de detección de ciberataques:

[Inicio: Detección de Actividad Sospechosa]

/ \

/ \

/ \

/ \

[¿Es un ataque conocido?] [¿Es un comportamiento anómalo?]

/ \ / \

/ \ / \

/ \ / \

[Sí] [No] [Sí] [No]

| | | |

| | | |

[Bloquear IP] [¿Es un falso positivo?] [Alertar Administrador] [Ignorar]

/ \

/ \

/ \

/ \

/ \

[Sí] [No]

| |

| |

[Ignorar] [Investigar más]

**Explicación:**

1. **Inicio**: El sistema detecta una actividad sospechosa.
2. **Primera decisión**: Determina si la actividad coincide con un patrón de ataque conocido.
   * Si es un ataque conocido, se bloquea la IP.
   * Si no es un ataque conocido, se verifica si es un comportamiento anómalo.
3. **Segunda decisión**: Si el comportamiento es anómalo, se alerta al administrador.
   * Si no es anómalo, se ignora.
4. **Falso positivo**: Si se determina que la actividad sospechosa es un falso positivo, se ignora. Si no, se procede a investigar más a fondo.