Actividad 1: Sistema de Detección de Ciberataques

1. Acciones posibles del atacante

Un atacante puede realizar diversas acciones maliciosas para comprometer la seguridad de una plataforma web. Algunos ejemplos incluyen:

- **SQL Injection (SQLi):** Intentar inyectar código SQL malicioso en formularios de entrada.
- **Cross-Site Scripting (XSS):** Inyectar scripts maliciosos en páginas web para robar información.
- **Fuerza bruta:** Intentar acceder a cuentas mediante múltiples intentos de contraseña.
- **DDoS (Denegación de Servicio Distribuida):** Enviar una gran cantidad de tráfico para colapsar la plataforma.
- **Phishing:** Engañar a los usuarios para que proporcionen credenciales de acceso.
- **Subida de archivos maliciosos:** Cargar archivos que contengan malware o exploits.
- **Escaneo de vulnerabilidades:** Utilizar herramientas como **Nmap** o **Nikto** para encontrar fallos de seguridad.

---

2. Funciones del sistema de detección y herramientas utilizadas

El sistema de detección debe identificar y mitigar los ataques a través de diversas estrategias. Algunas de sus funciones incluyen:

- **Monitoreo de tráfico en tiempo real:** Analizar patrones de tráfico para detectar anomalías (por ejemplo, un aumento repentino en las solicitudes HTTP puede indicar un ataque DDoS).
- **Análisis de logs:** Registrar y analizar eventos sospechosos, como intentos fallidos de acceso repetidos.
- **Sistemas de detección de intrusos (IDS/IPS):** Herramientas como **Snort, Suricata o Wazuh** permiten detectar y bloquear tráfico malicioso.
- **Cortafuegos Web (WAF):** Como **ModSecurity** para prevenir SQLi y XSS.
- **Autenticación robusta:** Implementar 2FA para evitar ataques de fuerza bruta.
- **Rate limiting:** Limitar el número de intentos de inicio de sesión por usuario/IP.
- **Machine Learning para detección de anomalías:** Algoritmos que aprenden el comportamiento normal del tráfico y alertan sobre anomalías.

---

3. Aplicación de la poda alfa-beta

La poda alfa-beta puede optimizar el proceso de detección de ataques, reduciendo la cantidad de escenarios evaluados sin afectar la precisión.

Ejemplo de aplicación:

Supongamos que el sistema de detección tiene que decidir si una actividad sospechosa es un ataque real o un falso positivo. Se usa un **árbol de decisión**, donde:

1. **El atacante** elige entre diferentes acciones maliciosas (SQLi, XSS, DDoS, etc.).
2. **El sistema de detección** responde con contramedidas (bloqueo de IP, desafío CAPTCHA, alerta al administrador, etc.).

La poda alfa-beta ayuda a **reducir la cantidad de escenarios a evaluar** al descartar automáticamente caminos que no pueden mejorar la decisión. Por ejemplo:

- Si ya se detectó que una IP ha realizado múltiples intentos de SQLi en un corto tiempo, no es necesario evaluar si también intentó XSS, porque el sistema ya la bloquearía.
- Si un usuario legítimo falla su contraseña dos veces pero la tercera es correcta, no es necesario aplicar detección de fuerza bruta.

Esto **acelera la toma de decisiones** en tiempo real sin comprometer la seguridad.

Ejemplo de Arbol