

*Facultad de Ingeniería y Ciencias Exactas*

**Segundo Cuatrimestre 2024**

Clase 12 - Diseño y Análisis de Algoritmos

Alumna: Giorgetta Agustina

**Consignas**

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.

En este contexto, nuestro atacante podría realizar acciones de **fuerza bruta** para tratar de descifrar usuarios y acceder a la plataforma; podría intentar realizar **inyecciones SQL** para acceder a la base de datos de la plataforma en cuestión salteándose la necesidad de permisos; o incluso podría ejecutar ataques de **denegación de servicio** (DoS), con el fin de hacer fallar el sistema y provocar vulnerabilidades.

1. 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?

El sistema de detección a diseñar debería tener como base funciones de **análisis en tiempo real** (para identificar cualquier patrón inusual en el tráfico de la plataforma) y de **respuesta automática** (para bloquear el acceso de cualquier IP dudosa al servicio). Para este fin, podría implementar un **IDS** (sistema de detección de intrusos) como Snort, también optar por el uso de algoritmos **machine learning** para la identificación de patrones y con la intención de lidiar con ataques de fuerza bruta se podrían **limitar las solicitudes** según cierto umbral de tiempo para que, si una IP lo superase, se tomen medidas.

1. Explicar cómo se aplicaría la poda alfa-beta

La poda se aplicaría en función de las posibles acciones y respuestas de los involucrados, con la intención de reducir justamente el número de posibilidades a evaluar. Para ello, lo principal sería definir un de decisiones que el sistema podría tomar ante las amenazas y basándonos en él podemos definir a alfa y a beta, siendo alfa la acción que representa menor criticidad y beta lo contrario.

Con esto en mente, se evalúa cada nodo del árbol (estado del atacante o del sistema) y según su estado se toma una rama del árbol (se poda la otra).

Ejemplo:

**Sistema** 🡪 establece un limite de tasa de solicitudes

**Atacante 🡪** aumenta la cantidad de solicitudes hacia la plataforma

**Sistema 🡪** bloquea la IP por 5 minutos

1. Construir un árbol de decisión simplificado

BIBLIOGRAFIA

Mas información sobre ciberataques: <https://www.ibm.com/es-es/topics/cyber-attack>