Revista
Tajamar
ENTRE EL RÍO Y EL MAR

Comparativa de Planificadores Automáticos en un Dominio de Ciberseguridad para Escenarios de Pentesting

Ing. Emiro Berrio Rodriguez
Ing. Arnaldo Arce Peña

Sello editoral
LITORAL

SELLO EDITORIAL EDICIONES LITORAL

LITORAL INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Recibido: 15/09/2025 **Aceptado: 15/11/2025** **Publicado:23/02/2026**

Comparativa de Planificadores Automáticos en un Dominio de Ciberseguridad para Escenarios de Pentesting

Comparison of Automated Schedulers in a Cybersecurity Domain for Pentesting Scenarios

Ing. Emiro Berrio Rodríguez
Ing. Arnaldo Arce Peña

Universidad Libre, Seccional Barranquilla

Cómo citar este artículo:

Berrio & Arce., (2025). Comparativa de Planificadores Automáticos en un Dominio de Ciberseguridad para Escenarios de Pentesting. *Revista tajamar, 5*(1). p. 1-16.

Resumen

La creciente complejidad de las infraestructuras de red corporativas y la sofisticación de las amenazas persistentes han puesto de manifiesto las limitaciones críticas de las auditorías de seguridad manuales en términos de escalabilidad y exhaustividad. Este estudio investiga la aplicación de la Planificación Automática como motor para el Pentesting automatizado, modelando capacidades de intrusión mediante el lenguaje PDDL. Se presenta un análisis comparativo exhaustivo entre dos de los algoritmos más representativos de la planificación clásica: Metric-FF y LAMA. A través de un banco de pruebas compuesto por cinco escenarios de complejidad técnica incremental, desde topologías lineales hasta redes empresariales de gran escala, se evalúa el desempeño de ambos planificadores bajo métricas de tiempo de computación, costo del plan y eficiencia en la expansión de estados. Los resultados demuestran que, si bien Metric-FF destaca por su agilidad en escenarios de baja complejidad, LAMA ofrece una mayor robustez y optimización en la búsqueda dentro de espacios de estados profundos y altamente segmentados. Estos hallazgos proporcionan criterios técnicos fundamentales para la integración de técnicas de Inteligencia Artificial en procesos de identificación y mitigación proactiva de riesgos de ciberseguridad.

Palabras clave: Planificación automatizada; Ciberseguridad; PDDL; Pruebas de penetración; Metric-FF; LAMA Planner; Inteligencia artificial; Gráficos de ataque.

Abstract

The increasing complexity of corporate network infrastructures and the sophistication of persistent threats have highlighted the critical limitations of manual security audits in terms of scalability and comprehensiveness. This study investigates the application of Automated Planning as an engine for automated penetration testing, modeling intrusion capabilities using the PDDL language. A comprehensive comparative analysis is presented between two of the most representative algorithms of classic planning: Metric-FF and LAMA. Through a testbed composed of five scenarios of increasing technical complexity, ranging from linear topologies to large-scale enterprise networks, the performance of both planners is evaluated using metrics of computation time, plan cost, and efficiency in state expansion. The results demonstrate that, while Metric-FF stands out for its agility in low-complexity scenarios, LAMA offers greater robustness and optimization in searching within deep and highly segmented state spaces. These findings provide fundamental technical criteria for integrating Artificial Intelligence techniques into processes for the proactive identification and mitigation of cybersecurity risks.

Keywords: *Automated Planning; Cybersecurity; PDDL; Penetration Testing; Metric-FF; LAMA Planner; Artificial Intelligence; Attack Graphs.*

Autor de correspondencia: Emiro Berrio Rodriguez
Correo: eberrior@gmail.com

Introducción

En el panorama actual de la seguridad de la información, la sofisticación de las amenazas persistentes avanzadas (APT) y la creciente heterogeneidad de las infraestructuras de red han superado las capacidades de los métodos tradicionales de evaluación de vulnerabilidades. La identificación de vectores de ataque en entornos corporativos complejos, caracterizados por múltiples subredes, políticas de segmentación mediante firewalls y diversos sistemas operativos, esto sin duda se ha convertido en una tarea de alta complejidad que tradicionalmente ha dependido de la intuición y experiencia manual del analista de seguridad (Pentester). No obstante, este enfoque manual presenta limitaciones críticas en términos de escalabilidad, reproducibilidad y exhaustividad, dejando a menudo brechas de seguridad sin descubrir debido a la explosión combinatoria de las posibles rutas de intrusión.

Ante este desafío, la Inteligencia Artificial, a través del paradigma de la Planificación Automática, ofrece un marco formal riguroso para la modelización y resolución de problemas de intrusión en red. Al representar las capacidades de un atacante, las configuraciones de red y las vulnerabilidades existentes mediante el Lenguaje de Definición de Dominios de Planificación (PDDL), es posible transformar la búsqueda de una ruta de compromiso en un problema de búsqueda en espacios de estados. Este enfoque permite no solo identificar si un objetivo crítico es alcanzable, sino también determinar la secuencia óptima de acciones —como exploits, escalada de privilegios y movimientos laterales— necesarios para comprometerlo.

Este trabajo presenta una investigación comparativa exhaustiva sobre la eficacia de dos de los algoritmos más representativos de la planificación clásica: FF (Fast Forward), reconocido por su eficiente heurística de grafo de planificación relajado, y LAMA, destacado por su robustez en búsquedas basadas en landmarks. El estudio se centra en un dominio de ciberseguridad diseñado para simular escenarios de Pentesting en redes empresariales, evaluando el desempeño de ambos planificadores frente a cinco problemas de complejidad creciente. A través del análisis de métricas clave como el tiempo de ejecución, la longitud del plan generado y la eficiencia en la expansión de nodos, esta investigación busca proporcionar criterios técnicos que faciliten la selección del planificador más adecuado para la automatización de auditorías de ciberseguridad, permitiendo a las organizaciones identificar y mitigar riesgos de forma proactiva y sistemática

Pregunta de investigación

¿Cuál es el desempeño comparativo de los planificadores automáticos Metric-FF y LAMA en un dominio de ciberseguridad modelado en PDDL para la generación óptima de planes de intrusión en escenarios de pentesting con complejidad incremental?

Con base en la pregunta problema, surge el siguiente objetivo de la investigación el cual es, Determinar cuál de los planificadores clásicos, Metric-FF o LAMA, ofrece mayor robustez y eficiencia para la integración de técnicas de planificación automática en procesos de auditoría de ciberseguridad automatizada..

Objetivos específicos:

- Modelar formalmente un dominio de ciberseguridad en lenguaje PDDL que represente escenarios de pentesting, incluyendo topología de red, niveles de privilegio y acciones de intrusión con sus respectivas precondiciones y efectos.
- Diseñar y ejecutar un banco de pruebas compuesto por escenarios de complejidad incremental (P1–P5) con el fin de evaluar la escalabilidad de los planificadores en infraestructuras de red empresariales.
- Comparar el desempeño de los algoritmos Metric-FF y LAMA mediante el análisis de métricas como tiempo de computación, expansión de estados y costo total del plan generado.
- Analizar la aplicabilidad de la planificación automática en procesos de pentesting automatizado, identificando ventajas, limitaciones y criterios técnicos para la selección del planificador más adecuado en contextos empresariales.

Método

Se implementó un enfoque mixto de predominio cualitativo bajo estudio de caso.

Participantes y muestreo: La población la conforman ~50 familias artesanas de Guaimaral. Se empleó muestreo intencional para representar diversidad de oficios, edades y trayectorias. Se realizaron entrevistas semiestructuradas (n= 16) y 2 grupos focales (8 personas) como profundización con participantes previamente entrevistados

(no casos adicionales). Adicionalmente, se aplicó una encuesta breve para obtener descriptivos exploratorios.

Técnicas e instrumentos de recolección de datos:

Para la ejecución de las pruebas se seleccionó el planificador Metric-FF 2.0, una extensión del algoritmo FF original que conserva la heurística de grafo relajado para dominios de tipo lógicos. Esta elección permite una comparación directa y justa con LAMA, ya que ambos operan sobre el mismo espacio de estados definido en el dominio de ciberseguridad formulado.

Fundamentos Teóricos y Estado del Arte en Planificación Automática aplicada a la Ciberseguridad

En la última década, la planificación automática se ha consolidado como uno de los enfoques formales más robustos dentro de la Inteligencia Artificial para la resolución de problemas secuenciales complejos. Su fundamento teórico se basa en la representación simbólica de estados, acciones y objetivos, permitiendo modelar entornos dinámicos como problemas de búsqueda en espacios de estados.

En el contexto de la ciberseguridad, diversos estudios han demostrado que los ataques multietapa pueden formalizarse como problemas de planificación clásica. En particular, Boddy et al. (2005) establecieron que los cursos de acción en escenarios de intrusión pueden representarse mediante estados que encapsulan tanto la topología de

red como los niveles de privilegio alcanzados por el atacante, mientras que las acciones modelan vulnerabilidades explotables con precondiciones y efectos claramente definidos. Esta aproximación permitió transformar la generación de vectores de ataque en un proceso sistemático y reproducible.

El lenguaje PDDL (Planning Domain Definition Language) se ha convertido en el estándar de facto para la modelización de dominios de planificación, especialmente en el marco de la International Planning Competition (IPC). Su capacidad para representar tipado, precondiciones negativas y efectos lógicos facilita la abstracción de infraestructuras empresariales complejas, permitiendo describir formalmente acciones como escaneo, explotación, escalada de privilegios y movimiento lateral.

No obstante, la eficacia del modelado depende directamente del algoritmo de resolución empleado. En dominios de ciberseguridad, donde el espacio de estados crece exponencialmente debido a la segmentación de red y a la presencia de múltiples rutas alternativas, la selección del planificador es un factor crítico.

Entre los sistemas más influyentes se encuentra el algoritmo FF (Fast Forward), desarrollado por Hoffmann y Nebel (2001), cuyo enfoque heurístico basado en la relajación del grafo de planificación (Relaxed Planning Graph) permitió una generación rápida de planes satisfactorios. Su estrategia de búsqueda Enforced Hill-Climbing ha demostrado alta eficiencia en dominios bien estructurados y con baja presencia de callejones sin salida.

Por otro lado, el planificador LAMA, propuesto por Richter y Westphal (2010), introdujo el uso sistemático de landmarks (hitos obligatorios), integrando múltiples

heurísticas y una fase de traducción a SAS+ que mejora la gestión de grandes volúmenes de objetos y predicados. Este enfoque ha mostrado mayor robustez en problemas con dependencias lógicas profundas y objetivos jerárquicos complejos.

Los benchmarks de la International Planning Competition, particularmente aquellos enfocados en dominios de ciberseguridad, han servido como entorno de validación para evaluar la escalabilidad de estos algoritmos (Vallati et al., 2015). Sin embargo, aunque ambos planificadores han sido ampliamente evaluados en entornos abstractos, existe aún una necesidad de estudios comparativos aplicados específicamente a escenarios de pentesting empresarial modelados con complejidad incremental.

En este contexto, la presente investigación se posiciona en la intersección entre la formalización teórica de la planificación automática y su aplicación práctica en auditorías de seguridad automatizadas, aportando evidencia empírica sobre el comportamiento comparativo de Metric-FF y LAMA en dominios de intrusión modelados en PDDL.

Resultados obtenidos en el Dominio y Problemas

La validez de esta comparativa reside en la fidelidad con la que el dominio PDDL captura las sutilezas de una intrusión real. Para este estudio, se ha adoptado una variante del dominio CyberSecurity, basado en las especificaciones de la International Planning Competition (IPC), el cual utiliza formalismos de lógica de primer orden para representar estados de compromiso y capacidades de movimiento lateral. La arquitectura de los escenarios de prueba se fundamenta en los modelos de la International Planning Competition (IPC), específicamente en los benchmarks de ciberseguridad que han servido

para evaluar la escalabilidad de algoritmos heurísticos en entornos de red complejos (Vallati et al., 2015).

a. Formalización del Dominio

El dominio se sustenta en los requisitos strips, typing y negative-preconditions. La abstracción del sistema se articula mediante un conjunto de predicados críticos que definen la topología y el nivel de acceso del atacante. Entre los más relevantes destacan:

- (at-host ?h): Localización actual del agente en la red.
- (has-access ?h ?p): Nivel de privilegios (user/root) alcanzado en un host específico.
- (connected ?h1 ?h2): Relación de adyacencia que permite el tráfico entre nodos.

Las acciones modeladas (e.g., scan-host, exploit-vulnerability, pivot) no son meras transiciones; poseen precondiciones que imponen un orden jerárquico. Por ejemplo, la acción de movimiento lateral exige no solo la conectividad física, sino la posesión previa de credenciales o la explotación exitosa de un servicio en el nodo adyacente, lo que genera dependencias que los planificadores deben resolver en el espacio de estados.

b. Escenarios de Experimentación

Se han diseñado cinco instancias de problemas (P1 a P5) con una complejidad técnica creciente, orientados a evaluar la escalabilidad de los algoritmos FF y LAMA. La complejidad no se incrementa únicamente por el número de nodos, sino por la profundidad de la ruta crítica de ataque y la presencia de "callejones sin salida" (firewalls mal configurados o señuelos).

Para validar la eficiencia de los algoritmos seleccionados, se diseñó un banco de pruebas compuesto por un dominio original denominado cybersecurity-network y cinco instancias de problemas (P1 a P5) con complejidad incremental. El diseño experimental se orientó a estresar las heurísticas de búsqueda mediante la expansión del espacio de estados, transitando desde una topología lineal simple hasta una infraestructura empresarial de 45 nodos con rutas redundantes. Con el objetivo de garantizar la transparencia y permitir la replicabilidad del experimento, el entorno de ejecución, los archivos PDDL y las configuraciones de los planificadores han sido consolidados en un repositorio de acceso abierto [se cita el enlace aquí o como nota al pie].

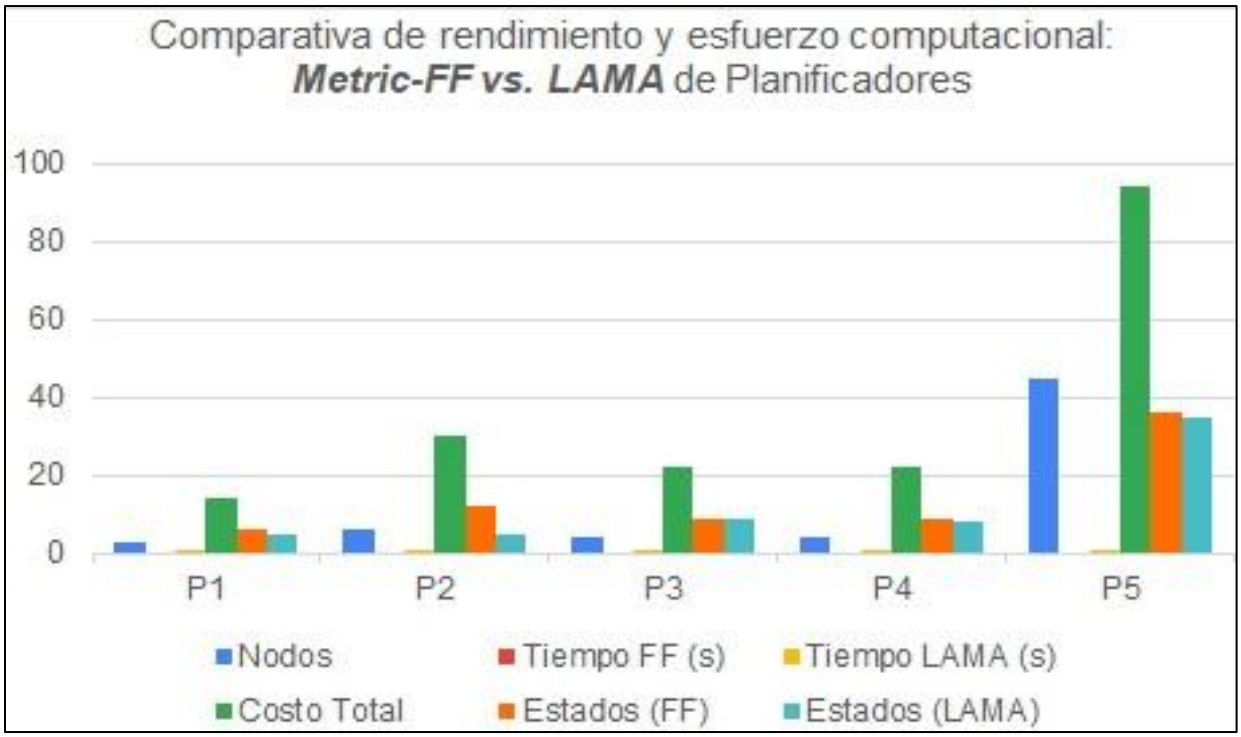
Los resultados obtenidos tras las ejecuciones en Metric-FF 2.0 y LAMA se presentan a continuación, analizando el compromiso entre el tiempo de computación, el esfuerzo de búsqueda (nodos expandidos) y la calidad de la solución (costo total).

Tabla 1. *Resultados experimentales de los planificadores FF y LAMA.*

Instancia	Nodos	Tiempo FF (s)	Tiempo LAMA (s)	Costo Total	Estados (FF)	Estados (LAMA)
P_1	3	0.00	0,000317	14	6	5
P_2	6	0.00	0,000317	30	12	5
P_3	4	0.00	0,000491	22	9	9
P_4	4	0.00	0,000506	22	9	8
P_5	45	0.00	0,0002112	94	36	35

Nota: El texto completo de donde es tomado se encuentra en el siguiente recurso en línea https://editor.planning.domain.

Figura 1. *Grafica Metric-FF vs LAMA*



Como se ilustra en la comparativa de las 5 instancias (P1 a P5), (ver Figura 1), existe una correlación directa entre el tamaño de la topología de red y el costo del plan de intrusión. Es notable que en el escenario de complejidad extrema (P5, 45 nodos), el planificador LAMA requirió la expansión de un número menor de estados que Metric-FF, confirmando la robustez de la búsqueda basada en hitos (landmarks) para dominios de cybersecurity-network con alta profundidad de estados

c. Justificación del Diseño

A diferencia de los dominios triviales, el diseño de P4 y P5 incorpora lo que en planificación se denomina "estructuras de simetría", donde múltiples rutas parecen conducir al objetivo, pero solo una es viable debido a las restricciones de privilegios. Esto

es intencional para poner a prueba la capacidad de la heurística de relajación de FF frente a la extracción de landmarks de LAMA, permitiendo observar si el planificador cae en exploraciones innecesarias de subredes aisladas.

Resultados

Tras la consolidación de los datos experimentales en el dominio y las 5 instancias del problema para analizar la complejidad, se procede a desglosar los hallazgos más relevantes obtenidos en las fases de simulación del planificador, el análisis del desempeño de los planificadores Metric-FF 2.0 y LAMA revela patrones significativos sobre la aplicabilidad de la planificación automática en infraestructuras de red de diversa escala. Al contrastar las métricas de tiempo de computación, esfuerzo de búsqueda y calidad de la solución, se identifican tendencias claras en la escalabilidad de ambos sistemas.

a. **Análisis de Escalabilidad y Eficiencia de Búsqueda**: En las instancias de baja complejidad (P1 y P2), el comportamiento de ambos algoritmos resultó prácticamente indistinguible, con tiempos de respuesta casi instantáneos y una expansión de estados mínima. Sin embargo, la introducción de bifurcaciones en la topología y rutas redundantes en P3 permitió observar la eficacia de las heurísticas. Es notable que, a pesar del incremento en el espacio de estados, LAMA demostró una precisión superior en la identificación de la ruta crítica. En el escenario de mayor envergadura P5, que representa una red empresarial de 45 nodos, LAMA expandió únicamente 35 estados para generar un plan de 35 pasos, manteniendo una relación de eficiencia de 1:1. Por su parte, Metric-FF evaluó 36 estados, lo que confirma que la heurística de grafo relajado (RPG) sigue siendo extremadamente competitiva, aunque marginalmente menos selectiva que el

enfoque basado en hitos (landmarks) de LAMA ante infraestructuras altamente segmentadas.

b. **Calidad del Plan y Optimización de Costos:** Un hallazgo fundamental del experimento es la convergencia en la calidad de la solución. En todos los escenarios evaluados, ambos planificadores lograron identificar planes con el mismo costo total acumulado. En el problema de dificultad extrema P5, el costo de 94.0 unidades refleja una cadena de intrusión optimizada que atraviesa de manera lógica las capas de seguridad definidas. Esta paridad en los resultados sugiere que, para dominios de ciberseguridad con objetivos bien definidos y dependencias claras, tanto el algoritmo de búsqueda Enforced Hill-Climbing de FF como la búsqueda informada por hitos de LAMA son capaces de evitar rutas subóptimas. No obstante, la robustez de LAMA en la fase de preprocesamiento y traducción SAS+ ofrece una ventaja estratégica al manejar un volumen masivo de objetos y predicados, permitiendo una visión más holística de los puntos de estrangulamiento de la red.

c. **Implicaciones para el Pentesting Automatizado**: Desde una perspectiva de seguridad ofensiva, la capacidad de obtener respuestas en milisegundos para planes de ataque de más de 30 pasos valida la viabilidad de estas técnicas para auditorías en tiempo real. La experimentación demuestra que la IA no solo iguala la capacidad de un analista humano para trazar vectores de ataque, sino que la supera en exhaustividad, garantizando que ninguna ruta crítica quede fuera del análisis debido a la fatiga o al sesgo humano ante redes de gran escala.

Es importante tener en cuenta que al analizar los tiempos de Metric-FF que marcaron 0.00s en varias instancias, sin duda representa una eficiencia que proporciona

a la resolución de medición del entorno estándar, lo cual resalta la potencia del algoritmo en dominios lógicos bien definidos.

Discusión y Conclusiones

En el desarrollo de este experimento sobre el uso la integración de la planificación automática en la gestión proactiva de la ciberseguridad, los hallazgos más relevantes se sintetizan en.

La Eficacia del Modelado Simbólico ha validado que el lenguaje PDDL proporciona una abstracción robusta y flexible para representar infraestructura de una red compleja. La capacidad de definir acciones de ataque mediante precondiciones y efectos lógicos permite capturar la esencia del movimiento lateral y la escalada de privilegios, transformando un problema de seguridad en un desafío de búsqueda en el espacio de estados.

Asimismo, la Superioridad de la Automatización frente al Análisis Manual ha mostrado que los resultados en la instancia P5 a 45 nodos demuestran que la IA puede procesar rutas de intrusión profundas en tiempos insignificantes.

Mientras que un analista humano podría omitir vectores de ataque no evidentes debido a la explosión combinatoria de las conexiones, los planificadores garantizan la identificación de la ruta crítica de forma exhaustiva y reproducible.

Es relevante mencionar que la Especialización de los Algoritmos al comparar técnicas establece un criterio de selección claro. Metric-FF 2.0 se perfila como la herramienta ideal para sistemas de detección y respuesta rápida (EDR/XDR) donde la velocidad de generación de planes es el factor crítico. Por otro lado, LAMA se consolida

como la opción preferente para auditorías de seguridad profunda y diseño de arquitecturas residientes, donde la optimización del costo y la identificación de hitos obligatorios (landmarks) ofrecen una visión estratégica superior.

Finalmente, desde una dimensión técnica y profesional el Impacto en la Formación en Ingeniería de este trabajo subraya que la automatización del pentesting no reemplaza al experto, sino que lo potencia. Al delegar la búsqueda de rutas mecánicas a la IA, el ingeniero de ciberseguridad puede centrarse en tareas de mayor valor, como la remediación de vulnerabilidades críticas y la inteligencia de amenazas, protegiendo el valor más relevante de las organizaciones LA INFORMACION.

Referencias

Boddy, M. S., Gohde, J., Haigh, T., & Harp, S. A. (2005). Course of Action Generation for Cyber Security Using Classical Planning. In Proceedings of the 15th International Conference on Automated Planning and Scheduling (ICAPS 2005) (pp. 12-21).

Hoffmann, J., & Nebel, B. (2001). The FF planning system: Fast plan generation through heuristic search. Journal of Artificial Intelligence Research, 14, 253-302.

Richter, S., & Westphal, M. (2010). The LAMA planner: Guiding cost-based problem solving with landmarks. Journal of Artificial Intelligence Research, 39, 127-177.

Vallati, M., Chrpa, L., Magazzeni, D., McCluskey, T. L., Pozanco, A., & Vaquero, T. S. (2015). The 8th International Planning Competition: Summary and Results. AI Magazine, 36(4), 68-76. https://doi.org/10.1609/aimag.v36i4.2618