Herramienta de Diagnóstico Unificado para el Análisis de Seguridad y Geolocalización Aproximada de Direcciones IP en el Contexto Colombiano

Juan Manuel Serrano Rodríguez
Código: 20211020091
Facultad de Ingeniería
Universidad Distrital Francisco José de Caldas
Bogotá, Colombia
jmserranor@correo.udistrital.edu.co

***Resumen*—En la actualidad, la evaluación de la legitimidad y seguridad de direcciones IP requiere consultar múltiples plataformas dispersas, generando un proceso manual lento e ineficiente. Este trabajo propone el desarrollo de una herramienta web unificada de diagnóstico que integra datos de reconocimiento pasivo, geolocalización aproximada, reputación y contexto de red para direcciones IP. La plataforma utiliza fuentes de datos gratuitas incluyendo los conjuntos de datos de Censys en Google BigQuery, la base de datos GeoLite2 de MaxMind, consultas WHOIS a registros regionales, y la API de AbuseIPDB. Se implementa un modelo algorítmico de puntuación de riesgo que procesa los datos recolectados para generar una evaluación integral de amenazas. La herramienta democratiza el acceso a inteligencia de amenazas cibernéticas mediante una interfaz web intuitiva que presenta informes consolidados con recomendaciones de seguridad contextuales. Los resultados esperados incluyen una plataforma funcional de acceso público y documentación técnica para replicación del proyecto, contribuyendo significativamente a la mejora de las capacidades de diagnóstico de seguridad en Colombia.**

***Palabras clave*—reconocimiento pasivo, geolocalización IP, inteligencia de amenazas cibernéticas, análisis de seguridad de red, plataforma unificada de diagnóstico.**

***Abstract*—Currently, evaluating the legitimacy and security of IP addresses requires consulting multiple dispersed platforms, creating a slow and inefficient manual process. This work proposes the development of a unified web diagnostic tool that integrates passive reconnaissance data, approximate geolocation, reputation, and network context for IP addresses. The platform utilizes free data sources including Censys datasets in Google BigQuery, MaxMind's GeoLite2 database, WHOIS queries to regional registries, and the AbuseIPDB API. An algorithmic risk scoring model is implemented to process collected data and generate comprehensive threat assessments. The tool democratizes access to cyber threat intelligence through an intuitive web interface that presents consolidated reports with contextual security recommendations. Expected results include a functional public access platform and technical documentation for project replication, significantly contributing to improved security diagnostic capabilities in Colombia.**

***Index Terms*—passive reconnaissance, IP geolocation, cyber threat intelligence, network security analysis, unified diagnostic platform.**

I. Introducción

La creciente sofisticación de las amenazas cibernéticas y la necesidad de evaluaciones de seguridad precisas han convertido el análisis de direcciones IP en una actividad fundamental para profesionales de ciberseguridad, administradores de sistemas y usuarios técnicos [**Barni2024**]. En el contexto actual, donde los ataques cibernéticos se han incrementado exponencialmente y las organizaciones enfrentan desafíos sin precedentes para proteger su infraestructura digital, la capacidad de evaluar rápida y efectivamente la legitimidad y el nivel de riesgo asociado a una dirección IP específica se ha vuelto crítica.

El reconocimiento pasivo, definido como el proceso de recolección de información sin interactuar directamente con los sistemas objetivo, representa una metodología fundamental en el arsenal de herramientas de ciberseguridad [**Alqahtani2020**]. A diferencia del reconocimiento activo, que implica el envío de consultas directas y puede ser detectado por sistemas de seguridad, el reconocimiento pasivo permite obtener información valiosa manteniendo un perfil bajo y minimizando el riesgo de detección. Esta aproximación es particularmente relevante en evaluaciones de seguridad donde la discreción es fundamental y en contextos donde se requiere un análisis preliminar antes de proceder con técnicas más invasivas.

La geolocalización de direcciones IP, aunque inherentemente aproximada debido a las limitaciones técnicas de los métodos disponibles, proporciona información contextual valiosa para el análisis de seguridad [**Dong2012**]. Los avances recientes en técnicas de geolocalización han demostrado mejoras significativas en la precisión, particularmente cuando se combinan múltiples fuentes de datos y se implementan algoritmos de machine learning para procesar la información recolectada. Sin embargo, la fragmentación de la información en múltiples plataformas y bases de datos presenta desafíos significativos para los analistas de seguridad.

La inteligencia de amenazas cibernéticas ha evolucionado considerablemente en los últimos años, transitioning from manual analysis to sophisticated automated systems powered by artificial intelligence [**Ferrag2019**]. Esta evolución ha sido impulsada por la necesidad de procesar volúmenes masivos de datos en tiempo real y la complejidad creciente de los patrones de ataque. Las plataformas modernas de inteligencia de amenazas integran múltiples fuentes de datos, utilizan algoritmos avanzados de análisis y proporcionan capacidades predictivas que permiten a las organizaciones adoptar una postura proactiva frente a las amenazas emergentes [**Lin2023**].

En Colombia, como en muchos países en desarrollo, existe una brecha significativa en el acceso a herramientas avanzadas de análisis de seguridad cibernética. Esta situación se ve agravada por los costos asociados a plataformas comerciales especializadas y la falta de soluciones adaptadas al contexto local. La democratización del acceso a estas capacidades representa una oportunidad fundamental para fortalecer la postura de ciberseguridad del país y contribuir al desarrollo de una comunidad técnica más preparada para enfrentar los desafíos actuales.

El problema central que aborda esta investigación es la fragmentación de la información necesaria para realizar un diagnóstico completo de seguridad de direcciones IP. Actualmente, los analistas deben consultar múltiples plataformas: una para verificar puertos abiertos, otra para geolocalización, una tercera para información de reputación, y una cuarta para identificar el propietario de la red. Este proceso manual no solo es ineficiente en términos de tiempo, sino que también aumenta la probabilidad de errores y dificulta la correlación efectiva de información de múltiples fuentes.

La presente investigación propone el desarrollo de una herramienta web unificada que integre estas funcionalidades dispersas en una plataforma coherente y accesible. La solución propuesta se basa en la utilización exclusiva de fuentes de datos gratuitas, garantizando la sostenibilidad y replicabilidad del proyecto. La implementación incluye la integración de datos de Censys a través de Google BigQuery, la base de datos GeoLite2 de MaxMind para geolocalización, consultas WHOIS para información de contexto de red, y la API de AbuseIPDB para datos de reputación.

La contribución principal de este trabajo radica en la creación de una plataforma que no solo consolida información dispersa, sino que también implementa un modelo de puntuación de riesgo que procesa y analiza los datos recolectados para proporcionar evaluaciones comprensivas y contextualizadas. Esta aproximación va más allá de la simple agregación de datos, incorporando lógica de análisis que facilita la toma de decisiones informadas por parte de los usuarios.

REFERENCES

[1] M. Barni, P. Campisi, E. J. Delp, G. Doërr, J. Fridrich, N. Memon, F. Pérez-González, A. Rocha, L. Verdoliva, and M. Wu, "Information Forensics and Security: A quarter-century-long journey," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2856-2893, 2024.

[2] P.-C. Lin, W.-H. Hsu, Y.-D. Lin, R.-H. Hwang, H.-K. Wu, Y.-C. Lai, and C.-K. Chen, "Correlation of cyber threat intelligence with sightings for intelligence assessment and augmentation," *Computer Networks*, vol. 229, art. 109751, Jun. 2023.

[3] A. Saad Alqahtani, "Security threats and countermeasures in software defined network using efficient and secure trusted routing mechanism," *Computer Networks*, vol. 177, pp. 102-115, Mar. 2020.

[4] Z. Dong, R. D. W. Perera, R. Chandramouli, and K. P. Subbalakshmi, "Network measurement based modeling and optimization for IP geolocation," *Computer Networks*, vol. 56, no. 1, pp. 85-98, Jan. 2012.

[5] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Network and Computer Applications*, vol. 50, pp. 41-65, Feb. 2019.