# Seguridad en Redes WiFi: Estrategias de Detección y Expulsión de Intrusos

Valentin Torassa Colombero; Juan Pablo Estelles; Santiago Enrique Roatta; Maria Eugenia Casco

CAETI – Universidad Abierta Interamericana
DV. Montes de Oca 725 – Buenos Aires - Argentina
{Valentin.TorassaColombero. JuanPablo.Estelles, Santiago.Roatta, MariaEugenia.Casco}@uai.edu.ar

## RESUMEN

Nuestro trabajo se concentra en robustecer la seguridad en redes WiFi mediante proyectos I+D que aborden diversas técnicas para asegurar y defender redes Wi-Fi. Esto implica una exploración profunda de los tipos de intrusiones e intrusos, así como la identificación de señales que podrían indicar la presencia de un ingreso no deseado. Se analizan técnicas efectivas para bloquear o expulsar a los visitantes no deseados, con especial énfasis en la utilización de herramientas que desvelan la actividad de los mismos.

Esto incluye también la implementación de estos procedimientos tanto en enrutadores de red como en sistemas operativos Windows y GNU/Linux (Unix). El objetivo primordial es descubrir conexiones no deseadas mediante el empleo de herramientas especializadas de análisis de red y la vigilancia de patrones de tráfico anomalos. En el caso de sistemas operativos Windows, la atención se centra en la identificación y neutralización de conexiones indeseadas mediante la utilización de herramientas especializadas, como Wireshark y Netcut. En contraste, para la salvaguarda de sistemas Unix, se recurrirá a herramientas como AirCrack, NMap e iptables, fortaleciendo así la defensa de las redes contra posibles amenazas. A su vez, se abordarán medidas preventivas del lado del enrutador para consolidar la seguridad de la red, llevándose a cabo configuraciones detalladas con el fin de robustecer las defensas y garantizar una protección efectiva.

Uno de nuestros objetivos es la construcción de una máquina virtual denominada que denominaremos "PRETORIAN". Esta máquina se fundamenta en los conocimientos adquiridos durante la investigación y es capaz de detectar los distintos tipos de intromisiones posibles. Su propósito es permitir la detección y expulsión con una interfaz simple y centralizada, salvaguardando la integridad de la red en tiempo real.

***Palabras clave: Redes, WiFi, Ciberdefensa***

## CONTEXTO

Los proyectos radicados en el CAETI se clasifican en tres líneas prioritarias Automatización y Robótica, Ingeniería de Software y Sociedad del Conocimiento y Tecnologías Aplicadas a la Educación. Este proyecto se enmarca en la rama de Ingeniería de Software y más específicamente en la subdivisión de Ciberseguridad, conceptos y aplicaciones.

## 1. INTRODUCCIÓN

Vivimos en un mundo en constante evolución, impulsado por los avances en las tecnologías de red. A medida que nos sumergimos en la era de la conectividad, impulsada por fenómenos como el Internet de las Cosas (IoT), experimentamos una transformación en la forma en que interactuamos con la información. Sin embargo, esta rápida adopción de nuevas tecnologías viene acompañada de desafíos relacionados con la seguridad. La conveniencia ofrecida por las redes puede eclipsar el gran riesgo y responsabilidad que un avance de este tipo conlleva.[1]

En la era de la digitalización, donde los requisitos y oportunidades de movilidad, la nube y el Internet de las cosas (IoT) son los principales temas de discusión para las empresas, existe una tendencia a menospreciar la red como un simple medio de transporte [2]. Cuando este acontecimiento se combina con el hecho que los responsables de seguridad IT consideran las redes inalámbricas corporativas como el punto débil de las organizaciones, no hace falta recalcar la importancia de conocer y dominar el ámbito inalámbrico para poder aplicar las medidas de seguridad más robustas y restrictivas posibles. De no ser así, el riesgo es elevado y el resultado es potencialmente catastrófico. [3]

La interconexión cada vez mayor de dispositivos a través de redes WiFi ha abierto nuevas posibilidades, pero también ha ampliado la superficie de ataque para posibles intrusiones cibernéticas. En este contexto, se introduce la investigación centrada en los principios de monitoreo de seguridad de redes, por sus siglas en ingles NSM (Network Security Monitoring), que abarca la recopilación, análisis y escalada de indicios y alertas para detectar y responder a intrusiones. NSM proporciona una vía para identificar intrusos en la red y tomar medidas antes de que causen daños a la empresa.[4] Su objetivo es supervisar el estado de una red dada para detectar eventos anómalos y, cuando se detectan, gestionarlos de manera oportuna. Esto representa un desafío significativo, ya que las redes de comunicación generan un volumen masivo de datos a un ritmo elevado.[5]

El origen de NSM se remonta a 1988, cuando Todd Heberlein desarrolló el Monitor de Seguridad de Red, el primer sistema de detección de intrusiones que utilizó el tráfico de red como fuente principal de datos para generar alertas.[4]

Este trabajo se presenta como una contribución a la comprensión y aplicación de NSM, proporcionando herramientas y procesos necesarios para iniciar la identificación de adversarios en redes WiFi. Reconociendo que la respuesta a incidentes debe ser un proceso empresarial continuo, NSM se destaca como una de las mejores maneras de avanzar desde defensas nulas hacia una capacidad defensiva. Asegurando un fortalecimiento en la seguridad en redes WiFi mediante estrategias de detección y expulsión de intrusos, abordando una amplia gama de técnicas para asegurar y defender estas redes.

## 2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

La investigación propuesta se estructura en tres líneas fundamentales con el propósito de fortalecer la seguridad en redes WiFi a través de estrategias de detección y expulsión de intrusos. Cada línea aborda aspectos específicos del proceso, contribuyendo de manera integral al objetivo general:

### 2.1 Estrategias de Detección y prevención de Intrusos:

En el ámbito de esta línea de investigación, nos adentraremos en primer lugar en la comprensión detallada de las señales características de intrusión en redes WiFi y sistemas, explorando diferentes técnicas empleadas por los intrusos, analizando su modus operandi y que herramientas se pueden utilizar para realizar la intrusión.[6] El enfoque principal estará en el desarrollo de estrategias avanzadas para detectar ingresos de manera inmediata, aprovechando las funcionalidades específicas de sistemas operativos como Windows y GNU Linux. De esta manera, se ofrecerá una perspectiva integral al abordar la detección de intrusos desde distintos sistemas operativos.

Se hará uso de herramientas especializadas para la detección, expulsión y bloqueo de atacantes dentro de la red. Para esto emplearemos técnicas avanzadas que incluyen el análisis detallado de paquetes de tráfico y la desautenticación de sesiones.[7] Mediante el análisis exhaustivo de los paquetes de tráfico, se busca entender la naturaleza de la actividad intrusiva, proporcionando así información esencial para la implementación de estrategias efectivas de bloqueo y fortalecimiento.

Profundizaremos en el modus operandi de los intrusos en redes Wi-Fi, centrándonos en aspectos como las vulnerabilidades explotadas, desde el ESSID WLAN_xxx hasta el abuso de enrutadores de red con Firmware desactualizado que presentan fallas de seguridad ya conocidas. [8]

Se estudiará el uso de Honeypots como una herramienta complementaria para fortalecer la seguridad; Sistemas diseñados intencionalmente para simular vulnerabilidades y atraer a posibles intrusos, permitiendo estudiar sus tácticas y recopilar información sobre posibles amenazas y patrones de ataque. [9]

La segunda subdivisión de esta línea de investigación se concentraría en la prevención de intrusiones a nuestra red. Para ello, se proponen diversas medidas proactivas para fortalecer la seguridad de la red WiFi. En primer lugar, se sugiere desvincular la IP de administración, para dificultar el acceso no autorizado y la modificación de la configuración de red. Asimismo, se recomienda cambiar la contraseña de acceso al router y modificar el nombre de la red WiFi (SSID) para aumentar la complejidad de un ataque.[10]

La modificación de la encriptación y cifrado del WiFi, junto con el establecimiento de una contraseña robusta, contribuirán a incrementar los tiempos de crackeo que pueden ir desde minutos hasta años dependiendo de los factores anteriormente mencionados.[11] Otra recomendación es mantener actualizado el firmware del enrutador de forma regular, eliminando así posibles vulnerabilidades conocidas. [10]

En situaciones donde la seguridad de la red es una prioridad absoluta, especialmente en entornos empresariales, es crucial implementar medidas más restrictivas. Estas incluyen la randomización del canal de transmisión del WiFi para complicar los ataques de puntos de acceso falsos, la habilitación de la multibanda para obstaculizar ciertos scripts de crackeo automático y la verificación de un ESSID limpio para garantizar que no ha sido suplantado. [8]

En casos, incluso más extremos, donde cualquier filtración podría desencadenar una crisis, se recomienda tomar medidas como activar el filtrado por dirección MAC y reducir los rangos de direcciones IP permitidas para ejercer controles ultra restrictivos de acceso, Así como limitar la potencia de emisión de las antenas,

desactivar la administración remota y deshabilitar la tecnología PnP(Plug and Play). [10]

### 2.2 Desarrollo de Contramedidas y Expulsión de Intrusos:

En esta línea de investigación, nos enfocaremos en el desarrollo y aplicación de contramedidas efectivas para bloquear y expulsar intrusos tanto en entornos Windows como en sistemas GNU Linux. A continuación, se detallan los aspectos clave de esta investigación:

- Desde Windows:

Exploraremos estrategias para contrarrestar intrusiones en sistemas operativos Windows. Para bloquear el acceso no autorizado, se emplearán herramientas como cortafuegos avanzados.[12] se llevarán a cabo expulsiones inmediatas mediante la terminación de sesiones y procesos no autorizados; para esto, nos valdremos de herramientas como Wireshark, el analizador de paquetes más conocido y utilizado en todo el mundo y Netcut, una aplicación destinada a la gestión de redes. La primera será fundamental para analizar el tráfico de red, por otro lado, para la desconexión inmediata, se hará uso de la funcionalidad proporcionada por Netcut, que permite cortar y controlar las conexiones no deseadas en tiempo real. [13-14]

- Desde GNU Linux:

Para fortalecer la seguridad de redes WiFi desde sistemas operativos basados en GNU/Linux, se hará uso de herramientas avanzadas de cortafuegos y monitoreo del tráfico de red. La implementación de medidas de seguridad incluirá la utilización de iptables, una herramienta de filtrado de paquetes que permitirá establecer reglas específicas para el control de acceso. [15] Para esto, se emplearán utilidades como Nmap, conocida por su capacidad de realizar escaneos de red para descubrir dispositivos y servicios activos.[16] También se utilizara Wireshark para analizar el tráfico en tiempo real y detectar posibles amenazas y finalmente, se realizarán expulsiones de red recurriendo a herramientas como el scripts de Aircrack-ng para poner interfaces de red inalámbricas en modo monitor, permitiendo así la captura y análisis de paquetes en el aire.[13-17] Con la información recopilada, se utilizará otros scripts de la misma suite para inyectar paquetes falsos y desautenticar dispositivos no deseados, forzándolos a desconectarse de la red.

### 2.3 Desarrollo de una Máquina Virtual PRETORIAN:

Durante el proceso de construcción de la Máquina Virtual "PRETORIAN", hemos decidido utilizar como base una imagen del sistema operativo Kali Linux, reconocido por su solidez en materia de seguridad y análisis forense. Esta elección nos permitirá utilizar las herramientas para la detección y respuesta a intrusiones en redes que ofrece Kali Linux.[18]

La funcionalidad principal de PRETORIAN se centrará en la detección de intrusos en tiempo real en redes WiFi. PRETORIAN implementara un detector con interfaz gráfica (GUI), posibilitando la interpretación inmediata de información. Este sistema permitirá la extracción detallada de información sobre las actividades del atacante en la red mediante el análisis exhaustivo de paquetes, proporcionando funcionalidades para el bloqueo y expulsión. PRETORIAN se convertirá en una solución completa, conveniente y funcional como Intrusion Detection System (IDS) especializado en redes WiFi.

## 3. RESULTADOS ESPERADOS

Se espera que esta investigación demuestre una alternativa eficiente en la seguridad de redes WiFi, focalizándose en la detección y expulsión de intrusos. Esto implica el desarrollo de nuevas estrategias, herramientas y técnicas para fortalecer la seguridad en entornos educativos y empresariales. Además de contribuciones prácticas, como recomendaciones específicas para implementar medidas de seguridad y el desarrollo de herramientas efectivas, se prevé que tenga un impacto educativo al proporcionar recursos y conocimientos que puedan ser utilizados para capacitar a estudiantes y docentes en este ámbito.

## 4. FORMACION DE RECURSOS HUMANOS

El equipo está compuesto por tres profesores/investigadores y aproximadamente diez estudiantes de la carrera de Ingeniería en Sistemas.

Con esta estructura, el equipo de trabajo busca impactar positivamente en la formación y capacitación en seguridad de redes WiFi, tanto a nivel estudiantil como profesional, contribuyendo así al fortalecimiento de la seguridad informática en diversos ámbitos.

## BIBLIOGRAFIA


[1] Salmon, A.; Levesque, W.; Mclafferty, M. (2017). Applied Network Security: Proven Tactics to Detect and Defend Against all Kinds of Network Attack. Packt Publishing.

[2] Cisco Systems. (2018). Cisco Enterprise Wireless. Intuitive Wi-Fi starts here. https://www.booksprints.net/book/cisco-enterprise-wireless-intiutive-wifi/

[3] Verdes, F. (2020). Hacking redes WiFi: Tecnología, Auditorías y Fortificación. Editorial 0xWORD.

[4] Bejtlich, R. (2013). The Practice of Network Security Monitoring: Understanding Incident Detection and Response, 1st Edition. No Starch Press.

[5] Fuentes-García, M.; Camacho, J.; Maciá-Fernández, G. (2021). "Present and Future of Network Security Monitoring." IEEE Access, Volume: 9. IEEE. Pages: 112744 - 112760. DOI: 10.1109/ACCESS.2021.3067106

[6] Subba, B.; Biswas, S.; Karmakar, S. (2016). "A Neural Network based System for Intrusion Detection and Attack Classification." 2016 Twenty Second National Conference on Communication (NCC).

[7] Ramos Valencia, M. V. (2012). Análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico para el acceso seguro en redes Wifi. Escuela Superior Politécnica de Chimborazo. Riobamba, Ecuador. UDCTEPEC;20T00461.

[8] Akram, Z.; Saeed, M. A.; Daud, M. (2018). "Real-time Exploitation of Security Mechanisms of Residential WLAN Access Points." 2018 iCoMET.

[9] Spitzner, L. (2002). Honeypots: Tracking Hackers. Addison Wesley.

[10] INCIBE. (2019). Seguridad en redes wifi: una guía de aproximación para el empresario.

[11] Lu, H.-J., & Yu, Y. (2021). "Research on WiFi Penetration Testing with Kali Linux." https://doi.org/10.1155/2021/5570001.

[12] Noonan, W., & Dubrawsky, I. (2006). Firewall Fundamentals, 1st Edition. Cisco.

[13] Sanders, C. (2017). Practical Packet Analysis, 3rd Edition: Using Wireshark to Solve Real-World Network Problems. No Starch Press.

[14] Carrasco, J., Gustavo, L. (2021). Implementación de un software libre para mejorar las vulnerabilidades de redes inalámbricas en la seguridad de información. ULADECH Catolica.

[15] Bertrone, M., Miano, S., Risso, F., Tumolo, M. (2018). Accelerating Linux Security with eBPF iptables. SIGCOMM Conference.

[16] Orebaugh, A., & Pinkard, B. (2011). Nmap in the Enterprise: Your Guide to Network Scanning, 1st Edition. Syngress.

[17] Medina Rojas, J. D.; Rivas Montalvo, Y. Y. (2020). Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos. UNPRG.

[18] Hertzog, R., & O'Gorman, J. (2017). Kali Linux Revealed. Offsec Press.