



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



Universidad Abierta Interamericana

Profesor: Pablo Audoglio

Integrantes: Juan Pablo Estelles y Valentín Torassa Colombero

Documentacion Investigacion Ingenieria de Software

Fecha de entrega: 04/06/2024

Indice

1. Introducción.....	5
1.1. Abstract.....	5
1.2. Motivación y objetivos.....	5
1.2.1. Objetivos específicos.....	5
1.2.2. Relevancia del estudio.....	6
1.2.3. Dificultades de la investigación.....	7
1.3. Grupo de trabajo y roles.....	7
2. Estado del Arte.....	9
2.1. Definir la estrategia de búsqueda.....	9
2.2. Identificar las fuentes de información.....	10
2.3. Revisión Bibliográfica.....	12
Fuente 1: "Applied Network Security: Proven Tactics to Detect and Defend Against all Kinds of Network Attack".....	12
Fuente 2: "Cisco Enterprise Wireless. Intuitive Wi-Fi starts here".....	13
Fuente 3: "Hacking redes WiFi: Tecnología, Auditorías y Fortificación".....	14
Fuente 4: "Análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico para el acceso seguro en redes WiFi".....	15
Fuente 5: "Honeypots: Tracking Hackers".....	16
Fuente 6: "Research on WiFi Penetration Testing with Kali Linux".....	17
Fuente 7: "Nmap in the Enterprise: Your Guide to Network Scanning".....	18
Fuente 8: "Using Wireshark to Solve Real-World Network Problems".....	19
Fuente 9: "Firewall Fundamentals".....	20
Fuente 10: "Present and Future of Network Security Monitoring".....	20
Fuente 11: "A Neural Network based System for Intrusion Detection and Attack Classification".....	21
Fuente 12: "Real-time Exploitation of Security Mechanisms of Residential WLAN Access Points".....	22
Fuente 13: "Seguridad en redes WiFi: una guía de aproximación para el empresario".....	23
Fuente 14 "Implementación de un software libre para mejorar las vulnerabilidades de redes inalámbricas en la seguridad de información".....	24
Fuente 15: "The Practice of Network Security Monitoring".....	25
Fuente 16: "Accelerating Linux Security with eBPF iptables".....	26
Fuente 17: "Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos".....	27
Fuente 18: "Kali Linux Revealed".....	28
2.4. Sintetizar la Información.....	29
2.5. Avances, Desafíos y Tendencias.....	31
3. Contexto.....	33

3.1. Contexto Académico del Proyecto.....	33
3.2. Relación del proyecto con el programa académico.....	34
3.3. Antecedentes del problema de investigación.....	34
3.4. Supervisión de la investigación y equipo de trabajo.....	34
3.5. Referencia al CAETI.....	34
4. Áreas de Investigación.....	35
4.1. Seguridad en redes WiFi.....	35
4.2. Tipos de intrusiones.....	35
4.3. Señales de ingreso no deseado.....	35
4.4. Patrones de Tráfico Anómalo.....	36
4.5. Herramientas de análisis de red.....	36
4.6. Medidas Preventivas en Enrutadores.....	40
4.7. Maquina Virtual SEC Pretorian.....	42
4.8. Network Security Monitoring (NSM).....	43
4.9. Intrusion Detection System (IDS).....	43
4.10. Intrusion Prevention System (IPS).....	44
4.11. Modus operandi de intrusos.....	45
4.12. Honeypots.....	45
Funcionamiento de los Honeypots.....	46
4.13. Proxy Server.....	46
Tipos de Proxy Servers.....	47
4.14. Firewalls físicos y firewalls con inteligencia artificial.....	47
Firewall físico.....	48
Firewalls basados en Inteligencia Artificial.....	49
4.15. Desvinculación de IP de administración.....	49
4.16. Modificación de SSID y contraseñas.....	49
4.17. Actualización del Firmware del enrutador.....	49
4.18. Análisis de tráfico en tiempo real.....	50
4.19. Formación y capacitación en ciberseguridad.....	50
5. Metodología de Trabajo.....	51
5.1. Planificación del proyecto y metodología utilizada.....	51
Detalles del plan de trabajo.....	51
Registro de reuniones y decisiones clave.....	52
5.2. Mapeo de la Bibliografía y su Relevancia.....	53
Identificación de las fuentes más relevantes.....	53
6. Descripción del Proceso de Documentación.....	54
6.1. Introducción.....	54
6.2. Metodología.....	54
6.2.1. Descripción Semanal del Proceso.....	55
Sprint 1: Generación de la Estructura de Investigación y Redacción de la Introducción.....	55

Sprint 2: Desarrollo del Estado del Arte y Corrección de Errores.....	58
Sprint 3: Contexto Académico del Proyecto.....	61
Sprint 4: Resumen y Metodología de Trabajo.....	64
Sprint 5: Áreas de Investigación.....	66
6.3. Conclusion.....	68
7. Sección Práctica.....	69
7.1. Montaje Gladiator.....	69
7.1.1. Instalación y Configuración.....	69
7.1.2. Integración de Herramientas.....	69
Wireshark.....	69
Angry IP Scanner.....	70
Netdiscover.....	71
Zenmap.....	71
7.2. Demostraciones Prácticas.....	72
Escenario 1: Detección de Dispositivos no Autorizados con Angry IP Scanner..	72
Escenario 2: Análisis de Tráfico con Wireshark.....	72
Escenario 3: Escaneo y Detección de Servicios con Zenmap.....	72
Escenario 4: Mapeo de la Red con Netdiscover.....	73
7.3. Objetivos de Gladiator.....	73
7.4. Conclusion.....	73
8. Resultados.....	74
8.1. Presentación de Hallazgos.....	74
8.2. Seguridad de Redes WiFi.....	74
8.3. Tipos de Intrusiones.....	74
8.4. Señales de Ingreso no Deseado.....	75
8.5. Implementación y Funcionamiento de los Honeypots.....	75
8.6. Herramientas de Análisis de Red.....	76
8.7. Medidas Preventivas en Enrutadores.....	77
8.8. Network Security Monitoring (NSM).....	78
8.9. Proxy Servers y sus tipos.....	78
8.10. Firewalls.....	79
9. Conclusiones.....	79
9.1. Reflexión.....	79
9.2. Recomendaciones para Futuras Investigaciones.....	80
Bibliografía.....	82

1. Introducción

1.1. Abstract

Este estudio se enfoca en fortalecer la seguridad de las redes WiFi a través de proyectos de investigación y desarrollo. Se exploran diversas técnicas para asegurar y defender estas redes, incluyendo una investigación exhaustiva sobre los tipos de intrusiones e intrusos, así como la identificación de señales indicativas de acceso no autorizado. Además, se analizan y aplican técnicas efectivas para bloquear o expulsar a los intrusos, destacando el uso de herramientas especializadas que revelan su actividad.

La implementación de estos procedimientos se lleva a cabo tanto en routers de red como en sistemas operativos Windows y GNU/Linux (Unix). Se presta especial atención a la identificación y neutralización de conexiones no deseadas en ambos sistemas operativos, utilizando una variedad de herramientas como Wireshark, Netcut, AirCrack, NMap e iptables. Estas medidas fortalecen las defensas de las redes contra posibles amenazas y se complementan con la aplicación de medidas preventivas en los routers para garantizar una protección efectiva.

Además, se persigue el desarrollo de una máquina virtual llamada "PRETORIAN", diseñada para detectar diversos tipos de intrusiones y salvaguardar la integridad de la red en tiempo real. Este sistema se basa en los conocimientos adquiridos durante la investigación y se centra en proporcionar una solución eficaz y centralizada para la detección y expulsión de intrusos.

1.2. Motivación y objetivos

1.2.1. Objetivos específicos

Los objetivos específicos de este estudio se centran naturalmente en la seguridad en las redes WiFi a través de proyectos de investigación y desarrollo que abarcan las distintas líneas de investigación del proyecto. Tales como:

- Analizar exhaustivamente los diferentes tipos de intrusiones que pueden afectar a las redes WiFi, comprendiendo sus características, modus operandi y las herramientas utilizadas por los intrusos para llevar a cabo dichas intrusiones. Permitiendo una comprensión más profunda de las amenazas potenciales que enfrentan estas redes.
- Identificar las señales indicativas de acceso no autorizado en las redes WiFi, investigando patrones de tráfico anómalos y otras irregularidades que puedan sugerir la presencia de un intruso.

- Desarrollar estrategias avanzadas para la detección y expulsión inmediata de intrusos en redes WiFi, aprovechando las funcionalidades específicas de programas desarrollados para sistemas operativos Windows y GNU/Linux. Esto implica la utilización de herramientas especializadas para bloquear o expulsar a los intrusos de manera efectiva.
- Investigar y aplicar medidas preventivas para fortalecer la seguridad de las redes WiFi desde el lado del enrutador, incluyendo la configuración detallada de parámetros de seguridad y la adopción de buenas prácticas para mitigar posibles vulnerabilidades.
- Diseñar y desarrollar la máquina virtual "PRETORIAN", con el objetivo de proporcionar una solución integral para la detección y expulsión de intrusos en redes WiFi. Esta máquina virtual se basará en los conocimientos adquiridos durante la investigación y se centrará en ofrecer una interfaz gráfica intuitiva para facilitar la interpretación de la información y la toma de decisiones en tiempo real.

1.2.2. Relevancia del estudio

La relevancia de este estudio radica en la creciente importancia de fortalecer la seguridad en las redes WiFi en un entorno cada vez más digitalizado y conectado. En la actualidad, las redes inalámbricas juegan un papel fundamental en diversos ámbitos, desde entornos educativos hasta empresariales, facilitando la comunicación, el intercambio de información y el acceso a recursos en línea. Sin embargo, esta conveniencia también conlleva riesgos significativos, ya que son vulnerables a intrusiones y ataques cibernéticos que pueden comprometer la privacidad y la integridad de los datos transmitidos a través de ellas.

Ante este panorama, resulta imperativo desarrollar estrategias efectivas para proteger y mitigar los riesgos asociados a posibles intrusiones. El presente estudio se presenta como una contribución al campo de la ciberseguridad, al abordar de manera integral los desafíos relacionados con la seguridad en las redes inalámbricas.

Una de las principales razones que justifican la relevancia de este estudio es el crecimiento exponencial del uso de redes WiFi en diversos contextos. Con el aumento de dispositivos conectados a Internet y el avance de tecnologías como el Internet de las Cosas (IoT), las redes inalámbricas se han convertido en un componente fundamental de la infraestructura tecnológica moderna. Desde dispositivos móviles y portátiles hasta dispositivos domésticos inteligentes, una amplia gama de dispositivos depende de las redes WiFi para acceder a Internet y compartir datos.

La relevancia de este estudio se ve resaltada por la creciente sofisticación de las amenazas cibernéticas dirigidas a las redes WiFi. Los intrusos y cibercriminales emplean técnicas cada vez más avanzadas para comprometer la seguridad de las redes inalámbricas y obtener acceso no autorizado a sistemas y datos sensibles. Desde ataques de denegación de servicio (DDoS) hasta técnicas de intrusión como la suplantación de identidad (spoofing) y la interceptación de datos, es fundamental desarrollar estrategias efectivas para detectar, prevenir y responder a estas amenazas de manera proactiva.

Finalmente, la importancia de proteger la integridad y la confidencialidad de la información en entornos educativos y empresariales. Las instituciones educativas y las empresas manejan grandes cantidades de datos sensibles, incluyendo información personal, financiera y comercial, que deben protegerse contra posibles intrusiones y ataques cibernéticos. En este sentido, fortalecer la seguridad de las redes en estos entornos es fundamental para garantizar la continuidad de las operaciones y proteger la reputación y la confianza de los usuarios y clientes.

1.2.3. Dificultades de la investigación

A medida que las redes inalámbricas se convierten en un componente esencial de la infraestructura tecnológica moderna, su exposición a amenazas y ataques se incrementa, lo que plantea desafíos significativos en términos de protección y defensa cibernética.

Uno de los principales problemas identificados es la falta de conciencia y comprensión sobre las vulnerabilidades de las redes WiFi. Muchos usuarios y organizaciones subestiman los riesgos asociados con el uso de redes inalámbricas, lo que los deja vulnerables a ataques cibernéticos y violaciones de seguridad. Sumado a la complejidad de realizar buenas instalaciones y configuraciones seguras de protección, la falta de conciencia sobre el tema, la consideramos el peor de los errores en cuanto a la ciberseguridad en redes, incluso más que el gran problema que representan las vulnerabilidades en sí.

Otro problema relevante es la falta de herramientas y recursos adecuados para detectar, prevenir y responder a intrusiones. Si bien existen diversas soluciones de seguridad disponibles en el mercado, muchas de ellas son costosas, complejas de implementar o requieren conocimientos técnicos especializados para su configuración y uso adecuados. Esto deja a muchas organizaciones y usuarios individuales sin la protección adecuada contra posibles amenazas cibernéticas.

La evolución constante de las tecnologías y las tácticas utilizadas por los intrusos y cibercriminales plantea otro desafío en términos de protección. A medida que las amenazas cibernéticas se vuelven más sofisticadas y difíciles de detectar, se hace necesario adaptar constantemente las estrategias de seguridad y desarrollar nuevas herramientas y técnicas para hacer frente a estas amenazas de manera efectiva.

1.3. Grupo de trabajo y roles

En nuestro equipo de trabajo, nos dividimos las responsabilidades de manera colaborativa para abordar los distintos aspectos de la investigación teórica sobre seguridad en redes WiFi.

Juan Pablo Estelles

Responsabilidades:

- Investigación y recopilación de información sobre técnicas de seguridad en redes WiFi.
- Análisis de herramientas especializadas para la detección y expulsión de intrusos.
- Implementación y configuración de medidas preventivas en enruteadores de red.

- Colaboración en la redacción y revisión del trabajo.

Valentin Torassa Colombero

Responsabilidades:

- Investigación y análisis de intrusiones e intrusos en redes WiFi.
- Evaluación de herramientas para la detección de actividad no autorizada.
- Desarrollo de la máquina virtual "PRETORIAN" para la detección en tiempo real de intrusiones.
- Participación activa en la redacción y edición del documento final.

Santiago Enrique Roatta

Responsabilidades:

- Orientación y asesoramiento en la elaboración del proyecto de investigación.
- Revisión y corrección de los avances presentados por el equipo.
- Apoyo en la identificación de áreas de mejora y sugerencias para la implementación de soluciones.

Breve biografía: Santiago Roatta es un experto en seguridad de redes con una amplia experiencia en la dirección de proyectos de investigación. Su conocimiento profundo del tema y su orientación han sido fundamentales para guiar al equipo hacia soluciones efectivas e innovadoras.

Maria Eugenia Casco

Responsabilidades:

- Supervisión y seguimiento del progreso del trabajo realizado por el equipo.
- Asesoramiento en la metodología de investigación y análisis de datos.
- Contribución con sugerencias y recomendaciones para mejorar la calidad del trabajo.

Breve biografía: Maria Eugenia Casco es una profesional con experiencia en seguridad de la información y seguridad forense. Su capacidad para proporcionar retroalimentación han sido de gran valor para el equipo a lo largo del proyecto.

2. Estado del Arte

2.1. Definir la estrategia de búsqueda

Para llevar a cabo una revisión exhaustiva y detallada del estado del arte en el campo de la seguridad en redes WiFi, se ha definido una estrategia de búsqueda meticulosa que garantiza la inclusión de las fuentes más relevantes y actuales. Esta estrategia de búsqueda se basa en el uso de palabras clave específicas y criterios de inclusión y exclusión claramente delineados, asegurando que se cubran todas las posibles variaciones terminológicas utilizadas en este ámbito de investigación.

Palabras clave: Las palabras clave seleccionadas para la búsqueda son cruciales para identificar la literatura más pertinente. Se han escogido términos que reflejan los diferentes aspectos y enfoques de la seguridad en redes WiFi. Entre las palabras clave utilizadas se encuentran:

- Seguridad en redes WiFi
- Detección de intrusos en redes
- Expulsión de intrusos en redes
- Monitorización de seguridad en red
- Ataques a redes inalámbricas
- Prevención de intrusiones en WiFi
- Auditoría de redes WiFi
- Fortificación de redes inalámbricas
- WiFi penetration testing
- Seguridad Redes en Windows
- Seguridad Redes GNU/Linux

Criterios de inclusión:

1. **Relevancia temática:** Solo se incluyeron documentos que aborden directamente la seguridad en redes WiFi, técnicas de detección y expulsión de intrusos, y el uso de herramientas específicas para la monitorización y defensa de redes inalámbricas.
2. **Actualidad:** Se priorizaron fuentes publicadas en los últimos diez años (2013-2023) para asegurar que la información sea relevante y refleje el estado actual de la tecnología y las amenazas en ciberseguridad.
3. **Autoridad de la fuente:** Se seleccionaron publicaciones de autores reconocidos en el campo, libros de editoriales académicas y profesionales, artículos de revistas científicas de alto impacto, y documentos de conferencias relevantes en el ámbito de la seguridad informática.

Criterios de exclusión:

1. **Irrelevancia temática:** Se excluyeron documentos que, aunque relacionados con la tecnología de redes, no aborden específicamente la seguridad en redes WiFi.
2. **Obsolescencia:** Publicaciones anteriores a 2013 fueron generalmente excluidas a menos que se consideraran seminales o de referencia obligada.

3. **Baja calidad académica:** Fuentes que no cumplieran con los estándares de rigor académico, como artículos de blogs sin revisión por pares o documentos sin referencias adecuadas, fueron excluidos.

Fuentes de información: La búsqueda se realizó en diversas bases de datos académicas y repositorios digitales, incluyendo:

- ø Google Scholar (Academy)
- ø IEEE Xplore
- ø SpringerLink
- ø ACM Digital Library
- ø Elsevier ScienceDirect

Se revisaron publicaciones relevantes de editoriales reconocidas como Packt Publishing, No Starch Press, y Syngress, y se consultaron guías y documentos técnicos de entidades influyentes en el ámbito de la ciberseguridad como Cisco y INCIBE.

También se solicitó la habilitación de la cuenta de Open Athens por el personal de UAI para acceder a material académico de pago de forma gratuita en plataformas como IEEE Xplore.

2.2. Identificar las fuentes de información

En el proceso de investigación sobre la seguridad en redes WiFi, es crucial seleccionar las fuentes de información más relevantes y valiosas. Esto garantiza la calidad y pertinencia del estudio.

Bases de datos académicas:

1. **IEEE Xplore:** Ofrece una amplia gama de artículos científicos y conferencias centradas en tecnología, informática y ciberseguridad; Probablemente el recurso y base de datos académica más importante y basto de investigación académica y de ingeniería.
2. **ACM Digital Library:** Proporciona acceso a publicaciones y trabajos de investigación en ciencias de la computación y tecnologías de la información, se destaca la profesionalidad y nivel de las investigaciones allí radicadas.
3. **SpringerLink:** Incluye libros y artículos revisados por pares en diversas disciplinas científicas y tecnológicas de carácter libre y gratuito en el caso de la mayoría de sus artículos.
4. **Elsevier ScienceDirect:** Contiene una vasta colección de artículos y capítulos de libros sobre tecnología de redes y ciberseguridad, también conocida como ScienceDirect.com, los artículos ofrecen una gran variedad de investigaciones a lo largo y ancho de todo el globo.

Revistas científicas:

1. **IEEE Access**: Publica investigaciones de alta calidad sobre tecnología de la información y ciberseguridad, como el artículo "Present and Future of Network Security Monitoring" de Fuentes-García, M., Camacho, J., y Maciá-Fernández, G. (2021).
2. **National Conference on Communication (NCC)**: Presenta investigaciones relevantes sobre sistemas de comunicación y seguridad, como el trabajo de Subba, B., Biswas, S., y Karmakar, S. (2016) sobre detección de intrusos.
3. **Journal of Network and Computer Applications**: Cubre diversos aspectos de la seguridad en redes y sistemas distribuidos, publicada por ScienceDirect.com.

Libros y monografías:

1. "**Applied Network Security**" por Salmon, A.; Levesque, W.; McLafferty, M. (2017): Este libro ofrece tácticas probadas para detectar y defenderse de ataques a redes, es un libro con información relevante yendo de lo básico a tácticas de ataque y defensa avanzadas, es uno de los recursos y fuentes más valiosos de la investigación.
2. "**Hacking redes WiFi**" por Verdes, F. (2020): Una guía completa sobre tecnología, auditorías y fortificación de redes WiFi, contiene una serie de pautas a tener en cuenta para asegurar la seguridad en redes y configurar modems.
3. "**The Practice of Network Security Monitoring**" por Bejtlich, R. (2013): Proporciona una comprensión profunda de la detección de incidentes y respuesta en redes, abarcando varias capas del modelo OSI.
4. "**Practical Packet Analysis**" por Sanders, C. (2017): Utiliza Wireshark para resolver problemas de redes y análisis de tráfico, es el manual para una de las herramientas más importantes para los profesionales de la seguridad informática.
5. "**Kali Linux Revealed**" por Hertzog, R., & O'Gorman, J. (2017): Una referencia esencial para pruebas de penetración en el Sistema Operativo especializado en seguridad informática basado en Debian Kali Linux.

Tesis doctorales y proyectos de investigación:

1. "**Análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico para el acceso seguro en redes WiFi**" por Ramos Valencia, M. V. (2012): Un estudio detallado sobre las vulnerabilidades de los protocolos WiFi comunes como la vulneración a partir de TCP y HTTP.
2. "**Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos**" por Medina Rojas, J. D., & Rivas Montalvo, Y. Y. (2020): Evaluación de sistemas de detección de intrusos en redes inalámbricas y una guía práctica para notar patrones de intrusión.

Guías y documentos técnicos:

1. **Cisco Enterprise Wireless**: Una de las empresas líderes en cuanto a módems, routers y redes en general, Cisco ofrece una guía conocida como Cisco Systems (2018) que proporciona información técnica y estrategias de implementación para la defensa de redes WiFi empresariales.

2. **INCIBE:** "Seguridad en redes WiFi: una guía de aproximación para el empresario" (2019), que ofrece recomendaciones prácticas para mejorar la seguridad de las redes inalámbricas lanzado por la Instituto Nacional de Ciberseguridad de España, es una empresa pública española.

Conferencias y simposios:

1. **SIGCOMM Conference:** Basado en las ciencias de computación y redes, contiene una sección para la publicaciones sobre seguridad, como el trabajo sobre iptables en Linux de Bertrone, M., Miano, S., Rissi, F., Tumolo, M..
2. **iCoMET (International Conference on Computing, Mathematics and Engineering Technologies):** Explora temas de ciencias duras e ingeniería en general, de aquí se extrajo el artículo "Real-time Exploitation of Security Mechanisms of Residential WLAN Access Points" de Akram, Z., Saeed, M. A., y Daud, M. (2018), centrado en la ciberseguridad en redes hogareñas WLAN.

Estas fuentes han sido seleccionadas por su relevancia y calidad, asegurando que el estudio se base en información robusta y actualizada, evitando el exceso de datos irrelevantes y manteniendo un enfoque claro y atractivo para el lector.

2.3. Revisión Bibliográfica

Fuente 1: "Applied Network Security: Proven Tactics to Detect and Defend Against all Kinds of Network Attack"

Referencia bibliográfica (formato APA): Salmon, A., Levesque, W., & McLaugherty, M. (2017). *Applied Network Security: Proven Tactics to Detect and Defend Against all Kinds of Network Attack*. Packt Publishing.

Objetivos

El objetivo principal de este libro es proporcionar a los profesionales de la seguridad de redes tácticas y estrategias prácticas para detectar y defenderse contra diversos tipos de ataques de red. Los autores buscan equipar a los lectores con conocimientos aplicables que puedan ser implementados en entornos reales para mejorar la seguridad de las redes.

Metodología

Los autores emplean una combinación de estudios de casos reales, análisis técnico detallado y guías paso a paso para explicar diferentes tácticas de seguridad de red. La metodología incluye la evaluación de amenazas contemporáneas, la implementación de soluciones de defensa y la simulación de ataques para probar la eficacia de las defensas propuestas.

Resultados

El libro proporciona un amplio repertorio de tácticas defensivas aplicables a diversas situaciones de seguridad de red. Los lectores obtienen conocimientos sobre la identificación de vulnerabilidades, la implementación de medidas preventivas y la respuesta a incidentes de seguridad. Las estrategias cubren tanto ataques comunes como amenazas emergentes.

Conclusiones

Salmon, Levesque y Mcclafferty concluyen que una defensa eficaz contra los ataques de red requiere una comprensión profunda de las tácticas de los atacantes y una implementación proactiva de medidas de seguridad. Subrayan la importancia de la vigilancia continua y la adaptación a nuevas amenazas para mantener la seguridad de las redes.

Análisis de Relevancia

Este libro es esencial para la investigación sobre robustecimiento de la seguridad en redes WiFi y detección de intrusos, ya que ofrece tácticas prácticas y actualizadas para proteger eficazmente las redes inalámbricas. Su enfoque en la identificación de amenazas y la implementación de medidas preventivas es fundamental para entender y abordar los desafíos específicos asociados con la seguridad de las redes WiFi.

Fuente 2: "Cisco Enterprise Wireless. Intuitive Wi-Fi starts here"

Referencia bibliográfica (formato APA): Cisco Systems. (2018). *Cisco Enterprise Wireless. Intuitive Wi-Fi starts here*. Retrieved from <https://www.booksprints.net/book/cisco-enterprise-wireless-intuitive-wifi/>

Objetivos

El objetivo de este libro es proporcionar una guía completa sobre las soluciones inalámbricas empresariales ofrecidas por Cisco. Busca educar a los profesionales de TI sobre cómo implementar, gestionar y optimizar redes Wi-Fi empresariales utilizando las tecnologías y productos de Cisco.

Metodología

La metodología empleada por Cisco Systems incluye la descripción técnica detallada de sus productos y soluciones, junto con casos de uso prácticos y estudios de caso reales. El libro utiliza una combinación de instrucciones paso a paso, diagramas técnicos, y ejemplos de configuraciones para ilustrar cómo implementar y gestionar redes inalámbricas efectivas.

Resultados

El libro ofrece una visión integral de las soluciones de Wi-Fi empresarial de Cisco, destacando las características innovadoras y las ventajas de su tecnología intuitiva. Proporciona a los lectores

las herramientas necesarias para diseñar, implementar y optimizar redes Wi-Fi que mejoren la conectividad y el rendimiento en entornos empresariales.

Conclusiones

Cisco Systems concluye que una red Wi-Fi empresarial efectiva no solo depende de la tecnología utilizada, sino también de una correcta implementación y gestión continua. Enfatizan la importancia de utilizar soluciones avanzadas y herramientas de monitoreo para asegurar una conectividad robusta y segura en las organizaciones.

Análisis de Relevancia

Este libro proporciona una guía completa sobre las soluciones inalámbricas empresariales ofrecidas por Cisco, lo cual es relevante para la investigación sobre robustecimiento de la seguridad en redes WiFi y la detección de intrusos. Aunque se centra en aspectos de implementación y gestión de redes WiFi empresariales, la comprensión de estas soluciones puede ser útil para comprender cómo las organizaciones pueden fortalecer la seguridad de sus redes inalámbricas.

Fuente 3: "Hacking redes WiFi: Tecnología, Auditorías y Fortificación"

Referencia bibliográfica (formato APA): Verdes, F. (2020). *Hacking redes WiFi: Tecnología, Auditorías y Fortificación*. Editorial 0xWORD.

Objetivos

El objetivo de este libro es proporcionar una comprensión profunda de las técnicas y herramientas utilizadas en la auditoría y fortificación de redes WiFi. Verdes busca capacitar a los profesionales de la seguridad informática para que puedan identificar y mitigar vulnerabilidades en las redes inalámbricas.

Metodología

Verdes utiliza una metodología práctica y técnica, combinando teoría con ejercicios prácticos. El libro incluye explicaciones detalladas de diferentes tecnologías WiFi, métodos de ataque, y técnicas de fortificación. Se emplean estudios de caso y ejemplos de auditorías reales para ilustrar cómo llevar a cabo evaluaciones de seguridad y aplicar medidas correctivas.

Resultados

El libro proporciona a los lectores un conjunto completo de conocimientos y habilidades para realizar auditorías de seguridad en redes WiFi. Los lectores aprenden a identificar puntos débiles, ejecutar pruebas de penetración, y aplicar soluciones de fortificación para proteger las redes inalámbricas contra ataques potenciales.

Conclusiones

Verdes concluye que la seguridad de las redes WiFi es un proceso continuo que requiere una comprensión detallada de las amenazas y las contramedidas disponibles. Enfatiza la importancia de mantenerse actualizado con las nuevas tecnologías y métodos de ataque para asegurar que las redes WiFi permanezcan protegidas y seguras.

Análisis de Relevancia

Este libro es crucial para la investigación sobre seguridad en redes WiFi. Proporciona una comprensión profunda de las técnicas y herramientas utilizadas en la auditoría y fortificación de estas redes, lo cual es fundamental para identificar y mitigar vulnerabilidades. La capacidad de realizar auditorías de seguridad y aplicar medidas correctivas es crucial para proteger datos sensibles y garantizar una operación continua sin interrupciones causadas por brechas de seguridad.

Fuente 4: "Análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico para el acceso seguro en redes Wifi"

Referencia bibliográfica (formato APA): 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.

Objetivos

El objetivo de este libro es analizar las vulnerabilidades presentes en los protocolos de protección y autenticación utilizados en redes WiFi para asegurar un acceso seguro. El autor busca identificar las debilidades de los protocolos más comunes y proponer medidas para mejorar la seguridad de las redes inalámbricas.

Metodología

Ramos Valencia emplea una metodología analítica y experimental. Realiza un estudio detallado de los principales protocolos de seguridad WiFi, como WEP, WPA y WPA2, mediante la revisión de literatura y la realización de pruebas de vulnerabilidad en entornos controlados. El análisis incluye la evaluación de la efectividad de estos protocolos frente a diferentes tipos de ataques.

Resultados

El estudio revela varias vulnerabilidades críticas en los protocolos de seguridad WiFi analizados. Se destacan las debilidades inherentes del WEP, la susceptibilidad de WPA a ataques de diccionario, y algunas vulnerabilidades presentes en WPA2. El autor proporciona un conjunto de recomendaciones para mitigar estos riesgos, incluyendo la implementación de configuraciones seguras y el uso de métodos de autenticación robustos.

Conclusiones

Ramos Valencia concluye que, aunque los protocolos de seguridad WiFi han mejorado significativamente con el tiempo, aún existen vulnerabilidades que pueden ser explotadas por atacantes. Subraya la importancia de una configuración adecuada y el uso de medidas adicionales de seguridad para proteger las redes inalámbricas de accesos no autorizados y mantener la integridad de los datos transmitidos.

Análisis de Relevancia

Este libro es sumamente valioso para la investigación sobre seguridad en redes WiFi. Ofrece un análisis exhaustivo de las vulnerabilidades en los protocolos de protección y autenticación utilizados en redes WiFi, lo que contribuye directamente a la comprensión de las amenazas potenciales y a la propuesta de medidas para mejorar la seguridad. La identificación de debilidades en los protocolos más comunes, como WEP, WPA y WPA2, es fundamental para implementar medidas efectivas de protección y garantizar un acceso seguro a las redes inalámbricas.

Fuente 5: "Honeypots: Tracking Hackers"

Referencia bibliográfica (formato APA): Spitzner, L. (2002). *Honeypots: Tracking Hackers*. Addison Wesley.

Objetivos

El objetivo principal de este libro es proporcionar una comprensión profunda de la tecnología de los honeypots y su aplicación en el seguimiento y la detección de hackers. Spitzner busca educar a los profesionales de la seguridad informática sobre cómo implementar y utilizar honeypots de manera efectiva para recopilar información sobre actividades maliciosas en las redes.

Metodología

Spitzner utiliza una metodología práctica y técnica, combinando teoría con ejemplos de casos reales. El libro incluye una descripción detallada de los diferentes tipos de honeypots, sus características y sus aplicaciones. Se proporcionan instrucciones paso a paso para la implementación y el mantenimiento de honeypots, así como técnicas para analizar y responder a la información recopilada.

Resultados

El libro ofrece a los lectores una visión completa de los honeypots y su potencial para rastrear y detectar actividades maliciosas. Se destacan los beneficios de utilizar honeypots como herramientas de inteligencia de seguridad, incluyendo la identificación de amenazas, la recopilación de información sobre tácticas de ataque y la mejora de la postura de seguridad general de una organización.

Conclusiones

Spitzner concluye que los honeypots son una herramienta valiosa en la defensa cibernética, proporcionando una forma efectiva de recopilar información sobre amenazas y mejorar la capacidad de respuesta a incidentes. Subraya la importancia de integrar los honeypots en la estrategia de seguridad global de una organización y mantenerlos actualizados para garantizar su eficacia.

Análisis de Relevancia

Este libro es importante para el tema de investigación sobre la seguridad de redes y la detección de actividades maliciosas, ya que proporciona información detallada sobre una técnica específica, como son los honeypots, que puede ser utilizada para proteger y monitorear redes inalámbricas y otros entornos de red.

Fuente 6: "Research on WiFi Penetration Testing with Kali Linux"

Referencia bibliográfica (formato APA): Lu, H.-J., & Yu, Y. (2021). "Research on WiFi Penetration Testing with Kali Linux." <https://doi.org/10.1155/2021/5570001>..

Objetivos

El objetivo de este libro es investigar y proporcionar información detallada sobre las técnicas y metodologías de prueba de penetración en redes WiFi utilizando la distribución de Kali Linux. Los autores buscan analizar las vulnerabilidades de las redes inalámbricas y demostrar cómo pueden ser explotadas con herramientas y técnicas específicas disponibles en Kali Linux.

Metodología

Lu y Yu emplean una metodología experimental y práctica. Utilizan la distribución de Kali Linux como plataforma de pruebas y realizan una serie de experimentos para evaluar la seguridad de las redes WiFi. La metodología incluye la identificación de puntos débiles, la realización de pruebas de penetración y la documentación de los hallazgos y las técnicas utilizadas.

Resultados

El libro presenta los resultados de la investigación, que incluyen la identificación de vulnerabilidades comunes en redes WiFi y la demostración de cómo pueden ser explotadas utilizando herramientas disponibles en Kali Linux. Se destacan las técnicas de ataque más efectivas y se proporcionan recomendaciones para fortalecer la seguridad de las redes inalámbricas.

Conclusiones

Lu y Yu concluyen que las pruebas de penetración en redes WiFi son fundamentales para evaluar y mejorar la seguridad de estas redes. Recomiendan a los profesionales de la seguridad

informática utilizar herramientas como Kali Linux para realizar pruebas de manera efectiva y adoptar medidas proactivas para mitigar las vulnerabilidades identificadas.

Análisis de Relevancia

Este libro es fundamental para la investigación sobre seguridad de redes WiFi, ya que proporciona información detallada sobre técnicas específicas de prueba de penetración utilizando una herramienta ampliamente utilizada en el campo de la ciberseguridad. La comprensión de estas técnicas es crucial para evaluar y mejorar la seguridad de las redes inalámbricas en diversos contextos.

Fuente 7: "Nmap in the Enterprise: Your Guide to Network Scanning"

Referencia bibliográfica (formato APA): Orebaugh, A., & Pinkard, B. (2011). Nmap in the Enterprise: Your Guide to Network Scanning, 1st Edition. Syngress.

Objetivos

El objetivo de este libro es proporcionar una guía exhaustiva sobre el uso de Nmap en entornos empresariales para realizar escaneos de redes. Los autores buscan educar a los lectores sobre cómo utilizar Nmap de manera efectiva para descubrir y evaluar la seguridad de dispositivos y servicios en una red corporativa.

Metodología

Orebaugh y Pinkard emplean una metodología práctica y orientada a la aplicación. Utilizan ejemplos y casos de estudio para demostrar cómo configurar y utilizar Nmap en diversas situaciones empresariales. La metodología incluye la explicación detallada de los comandos y opciones de Nmap, así como las mejores prácticas para maximizar la eficacia de los escaneos de red.

Resultados

El libro presenta los resultados de la investigación en forma de consejos prácticos, ejemplos de escenarios empresariales y tutoriales paso a paso sobre cómo utilizar Nmap para realizar escaneos de red efectivos. Se destacan las características clave de Nmap y se proporcionan recomendaciones para su implementación y configuración en entornos corporativos.

Conclusiones

Orebaugh y Pinkard concluyen que Nmap es una herramienta invaluable para la seguridad de redes en entornos empresariales, ya que permite a los administradores de sistemas detectar y mitigar posibles vulnerabilidades de manera proactiva. Recomiendan a los profesionales de seguridad familiarizarse con Nmap y utilizarlo como parte integral de sus estrategias de defensa cibernética.

Análisis de Relevancia

Este libro es valioso para la investigación sobre seguridad de redes, ya que proporciona una guía detallada sobre el uso de una herramienta fundamental para realizar escaneos de red. La comprensión de Nmap es crucial para evaluar la postura de seguridad de una red y detectar posibles amenazas y vulnerabilidades.

Fuente 8: "Using Wireshark to Solve Real-World Network Problems"

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

Objetivos

El libro tiene como objetivo proporcionar una guía práctica para el análisis de paquetes utilizando Wireshark, una herramienta fundamental en la resolución de problemas de redes del mundo real. El autor busca capacitar a los lectores para comprender y solucionar problemas de red mediante el análisis detallado de paquetes de datos.

Metodología

Sanders adopta una metodología práctica y orientada a la aplicación. Utiliza ejemplos reales y casos de estudio para enseñar a los lectores cómo utilizar Wireshark de manera efectiva en diversas situaciones de red. La metodología incluye la explicación detallada de conceptos de análisis de paquetes y la demostración de técnicas para resolver problemas comunes de red.

Resultados

El libro presenta los resultados de la investigación en forma de consejos prácticos, tutoriales paso a paso y ejemplos de análisis de paquetes utilizando Wireshark. Se destacan las capacidades de Wireshark para identificar problemas de red y se proporcionan recomendaciones para maximizar su utilidad en la resolución de problemas.

Conclusiones

Sanders concluye que el análisis de paquetes con Wireshark es una habilidad esencial para los profesionales de redes y seguridad informática. Recomienda a los lectores familiarizarse con Wireshark y utilizarlo como una herramienta integral para diagnosticar y solucionar problemas de red en entornos reales.

Análisis de Relevancia

Este libro es altamente relevante para la investigación sobre seguridad y resolución de problemas en redes, ya que proporciona una guía detallada sobre el uso de Wireshark, una herramienta fundamental en el análisis de paquetes de red. La comprensión de Wireshark es esencial para identificar y solucionar problemas de red en entornos del mundo real.

Fuente 9: "Firewall Fundamentals"

Referencia bibliográfica (formato APA): Noonan, W., & Dubrawsky, I. (2006). Firewall Fundamentals, 1st Edition. Cisco.

Objetivos

El objetivo de este libro es proporcionar una comprensión fundamental de los firewalls y su papel en la seguridad de redes. Los autores buscan educar a los lectores sobre los principios básicos de los firewalls, incluyendo su diseño, implementación y administración en entornos de red.

Metodología

Noonan y Dubrawsky emplean una metodología educativa y descriptiva. Utilizan ejemplos prácticos y explicaciones detalladas para enseñar a los lectores los conceptos esenciales relacionados con los firewalls. La metodología incluye la exploración de diferentes tipos de firewalls, sus características y configuraciones típicas.

Resultados

El libro presenta los resultados de la investigación en forma de explicaciones claras y ejemplos ilustrativos sobre el funcionamiento de los firewalls. Se cubren temas como filtrado de paquetes, inspección de estado, políticas de seguridad y tecnologías de firewall emergentes. Se proporcionan recomendaciones prácticas para la implementación y administración efectiva de firewalls.

Conclusiones

Noonan y Dubrawsky concluyen que los firewalls son componentes esenciales en la protección de redes contra amenazas externas e internas. Recomiendan a los profesionales de seguridad informática adquirir un conocimiento sólido sobre los fundamentos de los firewalls y utilizarlos como parte integral de la estrategia de seguridad de red de una organización.

Análisis de Relevancia

Este libro es fundamental para la investigación sobre seguridad de redes, ya que proporciona una introducción detallada a uno de los elementos clave en la protección de redes: los firewalls. La comprensión de los fundamentos de los firewalls es crucial para diseñar e implementar estrategias efectivas de seguridad de red en diversas organizaciones.

Fuente 10: "Present and Future of Network Security Monitoring"

Referencia bibliográfica (APA): Fuentes-García, M., Camacho, J., & Maciá-Fernández, G. (2021). Present and Future of Network Security Monitoring. IEEE Access, 9, 112744-112760. <https://doi.org/10.1109/ACCESS.2021.3067106>.

Objetivos

El objetivo de este artículo es analizar el estado actual y futuro de la monitorización de seguridad de redes. Los autores buscan proporcionar una visión general de las tendencias, tecnologías y desafíos en el campo de la monitorización de seguridad de redes, así como identificar áreas de investigación futuras.

Metodología

Fuentes-García, Camacho y Maciá-Fernández emplean una metodología de revisión bibliográfica y análisis de tendencias. Recopilan información de estudios previos, artículos académicos y documentos técnicos para identificar las principales áreas de interés en la monitorización de seguridad de redes y analizar su evolución.

Resultado

El artículo presenta los resultados de la investigación en forma de tendencias actuales en la monitorización de seguridad de redes, como el uso de inteligencia artificial y aprendizaje automático para la detección de amenazas, la adopción de tecnologías de nube para el almacenamiento y análisis de datos, y la importancia creciente de la monitorización en tiempo real.

Conclusiones

Los autores concluyen que la monitorización de seguridad de redes es un campo en constante evolución, impulsado por avances tecnológicos y nuevas amenazas ciberneticas. Recomiendan a los profesionales de seguridad informática mantenerse al día con las últimas tendencias y adoptar enfoques innovadores en la monitorización de redes para proteger eficazmente los sistemas de información.

Análisis de Relevancia

Este artículo es muy útil para la investigación sobre seguridad de redes, ya que proporciona una visión general actualizada en la monitorización de seguridad de redes. La comprensión de las tendencias actuales y futuras en este campo es esencial para diseñar y mantener estrategias efectivas de seguridad cibernetica.

Fuente 11: “A Neural Network based System for Intrusion Detection and Attack Classification”

Referencia bibliográfica (APA): Subba, B., Biswas, S., & Karmakar, S. (2016). A Neural Network based System for Intrusion Detection and Attack Classification. En 2016 Twenty Second National Conference on Communication (NCC).

Objetivos

El objetivo de este artículo es presentar un sistema basado en redes neuronales para la detección de intrusiones y la clasificación de ataques en redes de computadoras. Los autores buscan

desarrollar y evaluar un sistema de detección de intrusiones basado en inteligencia artificial que pueda identificar y clasificar ataques de manera efectiva.

Metodología

Subba, Biswas y Karmakar emplean una metodología experimental y de modelado. Desarrollan un sistema de detección de intrusiones utilizando redes neuronales artificiales y lo evalúan utilizando conjuntos de datos de pruebas estándar. La metodología incluye el diseño, implementación y evaluación del sistema propuesto.

Resultados

El artículo presenta los resultados de la investigación en forma de rendimiento del sistema propuesto en términos de precisión de detección y clasificación de intrusiones. Se destacan las capacidades de las redes neuronales para identificar patrones de tráfico malicioso y distinguir entre diferentes tipos de ataques.

Conclusiones

Los autores concluyen que el sistema propuesto basado en redes neuronales es prometedor para la detección de intrusiones y la clasificación de ataques en redes de computadoras. Recomiendan su uso como una herramienta complementaria en los sistemas de seguridad cibernética para mejorar la capacidad de respuesta ante amenazas.

Análisis de Relevancia

Este artículo es relevante para la investigación sobre seguridad de redes, ya que presenta un enfoque innovador para la detección de intrusiones utilizando redes neuronales artificiales. La comprensión de este tipo de sistemas es crucial para desarrollar técnicas avanzadas de detección de amenazas y fortalecer la seguridad cibernética en entornos de red.

Fuente 12: "Real-time Exploitation of Security Mechanisms of Residential WLAN Access Points"

Referencia bibliográfica (APA): Akram, Z., Saeed, M. A., & Daud, M. (2018). Real-time Exploitation of Security Mechanisms of Residential WLAN Access Points. En 2018 iCoMET.

Objetivos

El objetivo de este artículo es investigar y analizar la explotación en tiempo real de los mecanismos de seguridad de puntos de acceso WLAN residenciales. Los autores buscan identificar vulnerabilidades en estos dispositivos y demostrar cómo pueden ser explotadas para comprometer la seguridad de la red inalámbrica.

Metodología

Akram, Saeed y Daud emplean una metodología experimental y de prueba de concepto. Realizan

pruebas de penetración en puntos de acceso WLAN residenciales utilizando herramientas y técnicas de hacking disponibles. La metodología incluye la identificación de vulnerabilidades, la explotación de estas vulnerabilidades en tiempo real y la evaluación de los riesgos asociados.

Resultados

El artículo presenta los resultados de la investigación en forma de demostraciones de explotación exitosas de vulnerabilidades en puntos de acceso WLAN residenciales. Se destacan los mecanismos de seguridad comprometidos, como la autenticación débil o la falta de actualizaciones de firmware, y se proporcionan recomendaciones para mitigar estos riesgos.

Conclusiones

Los autores concluyen que los puntos de acceso WLAN residenciales son vulnerables a una variedad de ataques debido a la falta de medidas de seguridad adecuadas. Recomiendan a los usuarios y administradores de redes tomar medidas proactivas para proteger sus redes inalámbricas, como la actualización regular de firmware y la configuración adecuada de contraseñas.

Análisis de Relevancia

Este artículo es importante para la investigación sobre seguridad de redes inalámbricas, ya que destaca las vulnerabilidades en puntos de acceso WLAN residenciales y demuestra cómo pueden ser explotadas en tiempo real. La comprensión de estas vulnerabilidades es esencial para proteger eficazmente las redes inalámbricas contra posibles ataques y compromisos de seguridad.

Fuente 13: "Seguridad en redes WiFi: una guía de aproximación para el empresario"

Referencia bibliográfica (APA): INCIBE. (2019). Seguridad en redes WiFi: una guía de aproximación para el empresario.

Objetivos

El objetivo de esta guía es proporcionar a los empresarios una aproximación a la seguridad en redes WiFi, ofreciendo información y consejos prácticos para proteger sus redes inalámbricas y los datos sensibles de su empresa. INCIBE busca educar a los empresarios sobre las amenazas comunes en redes WiFi y cómo mitigarlas.

Metodología

INCIBE emplea una metodología educativa y orientada a la práctica. Utiliza un lenguaje claro y accesible para explicar conceptos de seguridad en redes WiFi y ofrece recomendaciones específicas para implementar medidas de seguridad efectivas. La metodología incluye ejemplos de casos reales y consejos prácticos basados en las mejores prácticas de seguridad.

Resultados

La guía presenta los resultados de la investigación en forma de consejos prácticos y recomendaciones para mejorar la seguridad en redes WiFi empresariales. Se cubren temas como la configuración segura de puntos de acceso, el uso de cifrado adecuado, la gestión de contraseñas y la detección de intrusiones. Se proporcionan recomendaciones específicas para empresarios de todos los sectores.

Conclusiones

INCIBE concluye que la seguridad en redes WiFi es un aspecto crítico para la protección de la información empresarial y la privacidad de los clientes. Recomienda a los empresarios tomar medidas proactivas para proteger sus redes inalámbricas y mantenerse al tanto de las últimas amenazas y soluciones de seguridad.

Análisis de Relevancia

Esta guía es fundamental para la investigación sobre seguridad de redes WiFi, especialmente para empresarios y propietarios de pequeñas y medianas empresas. Proporciona una visión general clara y práctica de las medidas de seguridad que deben implementarse para proteger las redes inalámbricas empresariales. La comprensión y aplicación de las recomendaciones de esta guía es fundamental para garantizar la seguridad de la red y los datos empresariales.

Fuente 14 “Implementación de un software libre para mejorar las vulnerabilidades de redes inalámbricas en la seguridad de información”

Referencia bibliográfica (APA): Carrasco, J., & Gustavo, L. (2021). Implementación de un software libre para mejorar las vulnerabilidades de redes inalámbricas en la seguridad de información. ULADECH Católica.

Objetivos

El objetivo de este artículo es presentar la implementación de un software libre destinado a mejorar las vulnerabilidades de redes inalámbricas para fortalecer la seguridad de la información. Los autores buscan proponer una solución práctica y accesible para mitigar riesgos en redes inalámbricas.

Metodología

Carrasco y Gustavo emplean una metodología de implementación y evaluación. Desarrollan e implementan un software libre diseñado para identificar y remediar vulnerabilidades en redes inalámbricas. Luego, evalúan la efectividad de esta solución en entornos de prueba.

Resultados

El artículo presenta los resultados de la implementación del software libre en términos de mejora de la seguridad de las redes inalámbricas y la protección de la información. Se destacan las

vulnerabilidades identificadas y abordadas por el software, así como los beneficios obtenidos en términos de seguridad de la información.

Conclusiones

Los autores concluyen que la implementación de un software libre para mejorar las vulnerabilidades de redes inalámbricas es una medida efectiva para fortalecer la seguridad de la información. Recomiendan a las organizaciones considerar el uso de esta solución como parte de su estrategia de seguridad cibernética.

Análisis de Relevancia

Este artículo es útil para la investigación sobre seguridad de redes inalámbricas y seguridad de la información, ya que presenta una solución práctica para mejorar las vulnerabilidades en redes inalámbricas. La implementación de software libre para fortalecer la seguridad de la información es un tema importante en el campo de la ciberseguridad y puede proporcionar beneficios significativos para la protección de datos y redes empresariales.

Fuente 15: "The Practice of Network Security Monitoring"

Referencia bibliográfica (APA): Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*, 1st Edition. No Starch Press.

Objetivos

El objetivo de este libro es proporcionar una comprensión profunda de la monitorización de seguridad de redes y cómo detectar e responder a incidentes de seguridad. El autor busca educar a los lectores sobre las mejores prácticas en el monitoreo de redes para identificar amenazas y responder de manera efectiva a ellas.

Metodología

Bejtlich emplea una metodología educativa y descriptiva. Utiliza ejemplos prácticos y casos de estudio para enseñar a los lectores los principios fundamentales de la monitorización de seguridad de redes. La metodología incluye la explicación detallada de herramientas y técnicas utilizadas en la detección de incidentes de seguridad.

Resultados

El libro presenta los resultados de la investigación en forma de estrategias efectivas para implementar y mantener un programa de monitorización de seguridad de redes. Se destacan las herramientas y técnicas clave para la detección proactiva de amenazas y se proporcionan recomendaciones para mejorar la capacidad de respuesta ante incidentes.

Conclusiones

Bejtlich concluye que la monitorización de seguridad de redes es una parte crucial de cualquier estrategia de ciberseguridad efectiva. Recomienda a los profesionales de seguridad informática

adoptar un enfoque proactivo hacia la detección de amenazas y responder de manera rápida y eficiente a los incidentes de seguridad.

Análisis de Relevancia

Este libro es esencial para la investigación sobre seguridad de redes, ya que se centra en la monitorización de seguridad de redes y la detección de incidentes. La comprensión de estas prácticas es esencial para proteger eficazmente las redes contra amenazas ciberneticas y responder de manera efectiva a posibles incidentes de seguridad.

Fuente 16: “Accelerating Linux Security with eBPF iptables”

Referencia bibliográfica (APA): Bertrone, M., Miano, S., Risso, F., & Tumolo, M. (2018). Accelerating Linux Security with eBPF iptables. En SIGCOMM Conference.

Objetivos

El objetivo de este artículo es presentar una solución para mejorar la seguridad en sistemas Linux utilizando eBPF (extended Berkeley Packet Filter) en conjunto con iptables. Los autores buscan acelerar y mejorar el rendimiento de las reglas de seguridad en Linux mediante esta técnica innovadora.

Metodología

Bertrone, Miano, Risso y Tumolo emplean una metodología experimental y de evaluación de rendimiento. Implementan eBPF junto con iptables en sistemas Linux y realizan pruebas de rendimiento para evaluar la eficacia y la velocidad de esta solución en comparación con enfoques tradicionales.

Resultados

El artículo presenta los resultados de la investigación en forma de mejoras significativas en el rendimiento y la eficacia de las reglas de seguridad en sistemas Linux utilizando eBPF iptables. Se destacan los beneficios en términos de velocidad de procesamiento de paquetes y reducción de la carga del sistema.

Conclusiones

Los autores concluyen que la combinación de eBPF e iptables representa una solución efectiva para acelerar la seguridad en sistemas Linux. Recomiendan su adopción para mejorar el rendimiento y la eficiencia en la aplicación de reglas de seguridad en entornos Linux.

Análisis de Relevancia

Este artículo es muy interesante para la investigación en seguridad de sistemas Linux, ya que presenta una solución innovadora para mejorar la eficacia y el rendimiento de las reglas de seguridad utilizando eBPF iptables. La optimización de la seguridad en sistemas Linux es un

tema importante en el campo de la ciberseguridad, y las técnicas como eBPF pueden proporcionar mejoras significativas en la protección de sistemas y redes.

Fuente 17: “Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos”

Referencia bibliográfica (APA): 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.

Objetivos

El objetivo de este artículo es evaluar el rendimiento de un sistema de detección de intrusos diseñado para redes inalámbricas 802.11 frente a ataques informáticos. Los autores buscan determinar la eficacia y la capacidad de detección de este sistema en entornos reales.

Metodología

Medina Rojas y Rivas Montalvo emplean una metodología experimental y de evaluación de rendimiento. Implementan y prueban un sistema de detección de intrusos en redes inalámbricas 802.11 utilizando conjuntos de datos de ataques simulados y reales. Luego, evalúan el rendimiento del sistema en términos de detección y eficacia de respuesta.

Resultados

El artículo presenta los resultados de la evaluación del rendimiento del sistema de detección de intrusos en redes inalámbricas 802.11. Se destacan las capacidades de detección del sistema frente a una variedad de ataques informáticos, así como su eficacia en la identificación y respuesta a amenazas.

Conclusiones

Los autores concluyen que el sistema de detección de intrusos evaluado es efectivo para proteger redes inalámbricas 802.11 contra ataques informáticos. Recomiendan su implementación en entornos empresariales y académicos para fortalecer la seguridad de las redes inalámbricas.

Análisis de Relevancia

Este artículo es fundamental para la investigación en seguridad de redes inalámbricas y detección de intrusos, ya que presenta una evaluación del rendimiento de un sistema de detección de intrusos diseñado específicamente para redes WiFi 802.11. La comprensión del rendimiento de estos sistemas es fundamental para garantizar la protección efectiva de las redes inalámbricas contra amenazas informáticas.

Fuente 18: "Kali Linux Revealed"

Referencia bibliográfica (APA): Hertzog, R., & O'Gorman, J. (2017). Kali Linux Revealed. Offsec Press.

Objetivos

El objetivo de este libro es proporcionar una guía completa sobre Kali Linux, una distribución especializada en seguridad informática y pruebas de penetración. Los autores buscan enseñar a los lectores sobre las características, herramientas y técnicas disponibles en Kali Linux para realizar evaluaciones de seguridad de sistemas.

Metodología

Hertzog y O'Gorman emplean una metodología educativa y descriptiva. Presentan información detallada sobre la instalación, configuración y uso de Kali Linux, así como tutoriales paso a paso sobre cómo utilizar sus herramientas para llevar a cabo pruebas de penetración y evaluaciones de seguridad.

Resultados

El libro presenta los resultados en forma de conocimientos adquiridos por los lectores sobre el uso efectivo de Kali Linux en el campo de la seguridad informática. Se destacan las capacidades de la distribución para realizar pruebas de penetración, auditorías de seguridad y análisis forense, entre otras tareas relacionadas con la seguridad.

Conclusiones

Los autores concluyen que Kali Linux es una herramienta poderosa y versátil para profesionales de seguridad informática y entusiastas de la tecnología interesados en realizar evaluaciones de seguridad de sistemas. Recomiendan a los lectores explorar y experimentar con las herramientas y técnicas presentadas en el libro para mejorar su comprensión y habilidades en seguridad informática.

Análisis de Relevancia

Este libro es muy útil para la investigación y la práctica en seguridad informática, ya que proporciona una guía exhaustiva sobre el uso de Kali Linux, una herramienta ampliamente utilizada en pruebas de penetración y evaluaciones de seguridad. La comprensión y el dominio de Kali Linux son fundamentales para llevar a cabo actividades de seguridad informática efectivas y proteger sistemas contra posibles amenazas.

2.4. Sintetizar la Información

Una vez realizada la revisión bibliográfica, es fundamental sintetizar la información extraída de los documentos relevantes. Este proceso implica agrupar la información según temas y subtemas, identificar las tendencias actuales y los vacíos en la investigación. A continuación, se presentan los resultados de la revisión bibliográfica de manera organizada y lógica, utilizando subtemas y secciones claras y concisas.

Subtemas y Estructura de la Síntesis

1. Tipos de Intrusiones en Redes WiFi

- **Intrusiones Pasivas**
 - **Escucha Pasiva (Sniffing)**
 - **Objetivos:** Capturar tráfico de red para analizar datos sensibles.
 - **Metodologías:** Uso de herramientas como Wireshark.
 - **Resultados:** Alta efectividad en la recolección de datos sin detección inmediata.
 - **Conclusiones:** Es esencial implementar cifrado robusto para mitigar este riesgo.
- **Intrusiones Activas**
 - **Ataques de Interferencia (Jamming)**
 - **Objetivos:** Interrumpir el funcionamiento normal de la red.
 - **Metodologías:** Emisión de señales de interferencia.
 - **Resultados:** Puede causar interrupciones significativas en la red.
 - **Conclusiones:** La detección temprana y la configuración adecuada del hardware pueden minimizar el impacto.
 - **Ataques de Suplantación (Spoofing)**
 - **Objetivos:** Falsificar la identidad para acceder a recursos restringidos.
 - **Metodologías:** Utilización de herramientas de spoofing para asumir la identidad de dispositivos legítimos.
 - **Resultados:** Puede llevar al acceso no autorizado y la filtración de datos.
 - **Conclusiones:** La autenticación multifactorial y el monitoreo continuo son críticos para la defensa.

2. Señales Indicativas de Acceso No Autorizado

- **Patrones de Tráfico Anómalos**
 - **Objetivos:** Identificar comportamientos inusuales en el tráfico de red.
 - **Metodologías:** Análisis de patrones de tráfico con herramientas como NMap.
 - **Resultados:** Identificación efectiva de accesos no autorizados.
 - **Conclusiones:** La implementación de sistemas de detección de intrusos (IDS) mejora significativamente la seguridad.
- **Irregularidades en el Uso de Recursos**
 - **Objetivos:** Detectar picos inesperados en el uso de ancho de banda.
 - **Metodologías:** Monitoreo constante de la red.

- **Resultados:** Alta correlación entre picos de uso y actividades maliciosas.
- **Conclusiones:** La configuración de alertas para uso inusual puede ayudar a la detección temprana.

3. Herramientas para la Detección y Expulsión de Intrusos

- **Wireshark**
 - **Objetivos:** Análisis de paquetes de red.
 - **Metodologías:** Captura y análisis detallado del tráfico.
 - **Resultados:** Identificación de intentos de intrusión y análisis de vulnerabilidades.
 - **Conclusiones:** Crucial para la identificación de intrusiones pasivas.
- **Netcut**
 - **Objetivos:** Gestión y control del acceso a la red.
 - **Metodologías:** Desconexión de dispositivos no autorizados.
 - **Resultados:** Eficaz en la expulsión rápida de intrusos.
 - **Conclusiones:** Útil en combinación con otras herramientas para una defensa completa.
- **AirCrack**
 - **Objetivos:** Auditoría de seguridad de redes WiFi.
 - **Metodologías:** Cracking de contraseñas y análisis de vulnerabilidades.
 - **Resultados:** Identificación de debilidades en la seguridad de la red.
 - **Conclusiones:** Esencial para pruebas de penetración y auditorías de seguridad.
- **NMap**
 - **Objetivos:** Mapeo y escaneo de redes.
 - **Metodologías:** Escaneo de puertos y servicios activos.
 - **Resultados:** Detección de dispositivos y servicios no autorizados.
 - **Conclusiones:** Fundamental para el reconocimiento y la seguridad preventiva.
- **iptables**
 - **Objetivos:** Control de acceso y filtrado de paquetes.
 - **Metodologías:** Configuración de reglas de firewall.
 - **Resultados:** Control granular sobre el tráfico de red.
 - **Conclusiones:** Indispensable para la configuración de políticas de seguridad robustas.

4. Medidas Preventivas y Mejoras en la Seguridad del Router

- **Configuración de Parámetros de Seguridad**
 - **Objetivos:** Fortalecer la configuración del router para prevenir intrusiones.
 - **Metodologías:** Uso de WPA3, desactivación de WPS, y configuración de contraseñas fuertes.
 - **Resultados:** Reducción significativa del riesgo de intrusión.
 - **Conclusiones:** La actualización constante del firmware y la configuración adecuada son claves para la seguridad.
- **Buenas Prácticas**
 - **Objetivos:** Adoptar hábitos que mejoren la seguridad de la red.

- **Metodologías:** Implementación de segmentación de redes y monitorización continua.
- **Resultados:** Mejoras en la resiliencia contra ataques.
- **Conclusiones:** La educación del usuario y la implementación de políticas de seguridad estrictas son esenciales.

5. Desarrollo de la Máquina Virtual "PRETORIAN"

- **Objetivos:** Proporcionar una solución integral para la detección y expulsión de intrusos.
- **Metodologías:** Integración de herramientas de detección y análisis en una interfaz gráfica intuitiva.
- **Resultados:** Mejora en la detección en tiempo real de intrusiones y facilitación de la toma de decisiones.
- **Conclusiones:** La máquina virtual "PRETORIAN" representa un avance significativo en la centralización y simplificación de la seguridad de redes WiFi.

Conclusión

La síntesis de la información revisada demuestra que la seguridad en redes WiFi es un campo complejo y en constante evolución. Las amenazas varían desde intrusiones pasivas como el sniffing hasta ataques activos como el spoofing y el jamming. Las herramientas especializadas como Wireshark, Netcut, AirCrack, NMap e iptables son fundamentales para detectar y expulsar intrusos, mientras que las medidas preventivas y configuraciones adecuadas en los routers son esenciales para fortalecer la seguridad.

El desarrollo de la máquina virtual "PRETORIAN" se presenta como una solución integral y efectiva para la detección y expulsión de intrusos en tiempo real, consolidando diversas herramientas y ofreciendo una interfaz amigable. La investigación resalta la necesidad de una continua actualización y adaptación de las estrategias de seguridad para enfrentar las amenazas emergentes y garantizar la integridad de las redes WiFi.

2.5. Avances, Desafíos y Tendencias

Resumen de los Principales Temas Tratados en la Literatura

La literatura sobre la seguridad en redes WiFi ha abordado una variedad de temas clave. Un tema recurrente es la identificación y categorización de los tipos de intrusiones en redes WiFi. Las intrusiones pasivas, que se centran en la captura de tráfico de red sin interferir directamente con el flujo de datos, y las intrusiones activas, que involucran la interrupción del servicio a través de métodos como el jamming y el spoofing, son áreas de interés significativo. Estos estudios proporcionan una base sólida para entender cómo operan los intrusos y qué técnicas utilizan para comprometer las redes.

Otro tema central en la literatura es la detección de señales indicativas de acceso no autorizado. Los patrones de tráfico anómalos y las irregularidades en el uso de recursos se citan con frecuencia como indicadores de actividad maliciosa. Herramientas como Wireshark, Netcut,

AirCrack, NMap e iptables han sido objeto de numerosos estudios, destacando su utilidad en la identificación y expulsión de intrusos. Estas herramientas ofrecen diversas funcionalidades que permiten a los administradores de red monitorear y proteger sus sistemas de manera más efectiva.

Además, las medidas preventivas y las mejoras en la seguridad del router son temas ampliamente discutidos. La configuración de parámetros de seguridad avanzados, como el uso de WPA3 y la desactivación de WPS, así como la implementación de buenas prácticas de seguridad, son estrategias esenciales para fortalecer las defensas de las redes WiFi. Estos estudios subrayan la importancia de una configuración adecuada y un monitoreo continuo para mitigar las vulnerabilidades.

Finalmente, el desarrollo de soluciones integrales, como la máquina virtual "PRETORIAN", ha sido un enfoque emergente en la literatura. Esta herramienta busca integrar diversas funcionalidades de detección y respuesta en una interfaz gráfica intuitiva, mejorando la capacidad de los administradores de red para gestionar la seguridad de manera más eficiente y en tiempo real.

Identificación de Lagunas en el Conocimiento Existente

A pesar de los avances en la investigación sobre la seguridad en redes WiFi, persisten varias lagunas significativas. Una de las principales áreas de preocupación es la eficacia de las herramientas existentes frente a nuevas amenazas. Las herramientas actuales, aunque efectivas contra muchas amenazas conocidas, requieren actualizaciones constantes para mantenerse relevantes frente a la evolución rápida de las técnicas de intrusión.

Además, la implementación y usabilidad de medidas preventivas sigue siendo un desafío. Muchas soluciones de seguridad son complejas y requieren conocimientos técnicos avanzados para su configuración y uso, lo que puede ser una barrera para usuarios no técnicos. Esto resalta la necesidad de desarrollar soluciones más accesibles y fáciles de usar, que permitan una implementación efectiva sin requerir una experiencia técnica considerable.

El monitoreo continuo y la detección en tiempo real también enfrentan desafíos significativos. Aunque herramientas como "PRETORIAN" representan un avance, la precisión y velocidad de la detección de intrusiones siguen siendo áreas de mejora. Es crucial optimizar estas soluciones para reducir los falsos positivos y negativos, mejorando así la eficacia general de la seguridad de la red.

Finalmente, la falta de conciencia y educación sobre la seguridad en redes WiFi es un problema crítico. Muchas organizaciones y usuarios subestiman los riesgos asociados con el uso de redes inalámbricas, lo que los deja vulnerables a ataques. Es necesario implementar iniciativas educativas y programas de concientización para mejorar el conocimiento y la aplicación de mejores prácticas de seguridad.

Avances y Tendencias Actuales

El desarrollo de tecnologías de inteligencia artificial (IA) y aprendizaje automático (ML) es una tendencia emergente en la seguridad de redes WiFi. Estas tecnologías pueden analizar grandes

volúmenes de datos en tiempo real, detectando patrones anómalos con mayor precisión que las técnicas tradicionales. Esto representa un avance significativo en la capacidad de respuesta y la prevención de intrusiones.

Las soluciones integrales y automatizadas, como "PRETORIAN", están ganando tracción en el campo de la seguridad de redes WiFi. Estas soluciones buscan centralizar las funciones de detección, análisis y respuesta, facilitando una gestión más eficiente de la seguridad de la red. La integración de múltiples herramientas en una interfaz única y accesible es una tendencia que promete mejorar significativamente la protección contra intrusiones.

La evolución de los protocolos de seguridad, como el despliegue de WPA3, también representa un avance importante. Estos nuevos estándares ofrecen un cifrado mejorado y una mayor protección contra ataques de fuerza bruta y otras técnicas de intrusión. La adopción de estos protocolos es fundamental para mejorar la seguridad de las redes WiFi en diversos entornos.

Con el crecimiento del Internet de las Cosas (IoT), la seguridad de los dispositivos conectados a redes WiFi se ha convertido en un área de investigación crítica. La protección de estos dispositivos y la garantía de la integridad de las redes en las que operan son cada vez más relevantes. La investigación en esta área se centra en desarrollar estrategias y herramientas que puedan asegurar la vasta cantidad de dispositivos conectados, desde dispositivos móviles hasta electrodomésticos inteligentes.

En conclusión, aunque se han logrado avances significativos en la seguridad de redes WiFi, la rápida evolución de las amenazas y la complejidad de las soluciones necesarias subrayan la importancia de una investigación continua. La implementación de nuevas tecnologías y prácticas de seguridad es esencial para mantenerse a la vanguardia en la protección de redes inalámbricas. Las tendencias actuales, como el uso de IA y ML, así como el desarrollo de soluciones integrales y la mejora de protocolos de seguridad, representan pasos importantes hacia un futuro más seguro para las redes WiFi.

3. Contexto

3.1. Contexto Académico del Proyecto

Este estudio se lleva a cabo en un contexto académico enfocado en la investigación y el desarrollo de soluciones de ciberseguridad para redes WiFi. El proyecto se enmarca dentro del campo de la ingeniería en sistemas, donde se busca abordar problemas prácticos mediante la aplicación de conocimientos teóricos y metodológicos avanzados. La seguridad de las redes inalámbricas es una preocupación creciente, especialmente en disciplinas relacionadas con la informática y las tecnologías de la información.

3.2. Relación del proyecto con el programa académico

El proyecto está alineado con los objetivos y áreas de investigación del programa académico de Ingeniería en Sistemas en la institución. La investigación en ciberseguridad es un área prioritaria para el programa, dado el impacto crítico que tiene en la protección de datos y la integridad de las comunicaciones digitales. Este estudio específico contribuye al fortalecimiento de las competencias de los estudiantes en temas de seguridad de redes, análisis de vulnerabilidades y desarrollo de soluciones tecnológicas innovadoras.

3.3. Antecedentes del problema de investigación

El problema de la seguridad en las redes ha sido un tema recurrente de estudio en el ámbito académico debido a la proliferación de dispositivos conectados y la creciente dependencia de las comunicaciones inalámbricas. Investigaciones previas han identificado diversas vulnerabilidades en estos sistemas, desde la falta de configuración segura de los routers hasta la sofisticación de las técnicas de intrusión utilizadas por ciberdelincuentes. Este proyecto se basa en un análisis exhaustivo de la literatura existente y busca avanzar en el desarrollo de medidas preventivas y de detección más efectivas.

3.4. Supervisión de la investigación y equipo de trabajo

La investigación es supervisada por Santiago Enrique Roatta y María Eugenia Casco, ambos expertos en seguridad de redes. Santiago proporciona orientación, revisa y corrige los avances del equipo, asegurando la calidad académica del proyecto. María Eugenia supervisa el progreso, asesora en metodología y análisis de datos, y sugiere mejoras.

El equipo de investigación incluye a Juan Pablo Estelles y Valentín Torassa Colombero. Juan Pablo investiga técnicas de seguridad en redes WiFi, analiza herramientas para detectar y expulsar intrusos, implementa medidas preventivas en enrutadores, y colabora en la redacción del trabajo. Valentín analiza intrusiones en redes WiFi, evalúa herramientas de detección, desarrolla la máquina virtual "PRETORIAN" para la detección en tiempo real, y contribuye en la redacción del documento final.

3.5. Referencia al CAETI

El proyecto se desarrolla en colaboración con el Centro de Altos Estudios en Tecnología Informática (CAETI), una entidad reconocida por su enfoque en la innovación y la excelencia académica en el ámbito de la tecnología de la información. La colaboración con el CAETI proporciona al equipo acceso a recursos avanzados y conocimientos especializados que son cruciales para el desarrollo y la implementación de soluciones de ciberseguridad eficaces.

4. Áreas de Investigación

4.1. Seguridad en redes WiFi

La seguridad en redes, especialmente en redes WiFi, es una fuente de preocupación constante y un desafío para las organizaciones, empresas e individuos de la actualidad. A medida que las organizaciones y los hogares adoptan la conectividad inalámbrica, se incrementa la exposición a riesgos cibernéticos. La protección de estas redes se centra en implementar medidas preventivas y reactivas que aseguren la confidencialidad, integridad y disponibilidad de los datos transmitidos. Con el fin de evitar accesos no deseados y salvaguardar la infraestructura de red contra posibles ataques,

Las redes WiFi presentan desafíos únicos debido a su transmisión inalámbrica. Esto hace que la detección y respuesta a amenazas sea una prioridad para mantener una red segura y funcional.

4.2. Tipos de intrusiones

Dentro de las intrusiones en redes WiFi, el spoofing y el sniffing son dos técnicas comunes utilizadas por los atacantes. El spoofing implica suplantar la identidad de un dispositivo legítimo en la red para ganar acceso no autorizado. Esto se logra alterando las direcciones MAC o IP, engañando a otros dispositivos y permitiendo al atacante interceptar o manipular la comunicación.

Por otro lado, el sniffing se refiere a la captura y análisis del tráfico de red sin el conocimiento de los usuarios. Utilizando herramientas especializadas, los atacantes pueden extraer información sensible, como credenciales y datos personales.

A su vez, se encuentran los ataques de fuerza bruta para descifrar contraseñas, la explotación de vulnerabilidades en el firmware del enrutador, y los ataques de intermediario (man-in-the-middle), donde el intruso intercepta y manipula la comunicación entre dos partes.

4.3. Señales de ingreso no deseado

Detectar señales de ingreso no deseado es vital para la seguridad. Entre estas señales, se encuentran picos inesperados en el tráfico de la red, la aparición de dispositivos desconocidos en la lista de conexiones, y patrones anómalos de uso. Técnicamente, estas señales pueden ser monitoreadas a través de herramientas de análisis de paquetes, que permiten a los observar en detalle el flujo de datos en la red.

La identificación de conexiones intermitentes o inusuales es otra señal de advertencia. Estos pueden ser indicativos de intentos de fuerza bruta o de dispositivos tratando de establecer una

conexión sin éxito repetidamente. La implementación de sistemas de monitoreo continuo, como los Sistemas de Detección de Intrusos (IDS), ayuda a identificar estos patrones y permite una respuesta oportuna.

El uso de métricas y algoritmos de aprendizaje automático puede mejorar aún más la capacidad de detección, permitiendo una defensa heurística contra las amenazas a la seguridad de la red.

4.4. Patrones de Tráfico Anómalo

Los patrones de tráfico anómalos son indicadores de posibles intrusiones o actividades maliciosas. Estos patrones incluyen un aumento inesperado en el volumen de tráfico, conexiones frecuentes y rápidas a múltiples puntos de la red, y el uso inusual de protocolos o servicios. La detección de estos patrones es crucial para la identificación temprana de amenazas.

El análisis de estos patrones se puede realizar mediante herramientas avanzadas de monitoreo de red que aplican algoritmos de aprendizaje automático para identificar desviaciones del comportamiento normal de la red. Estas herramientas pueden detectar y alertar a los administradores sobre picos en el tráfico que podrían indicar un ataque de denegación de servicio (DoS) o intentos de intrusión mediante fuerza bruta.

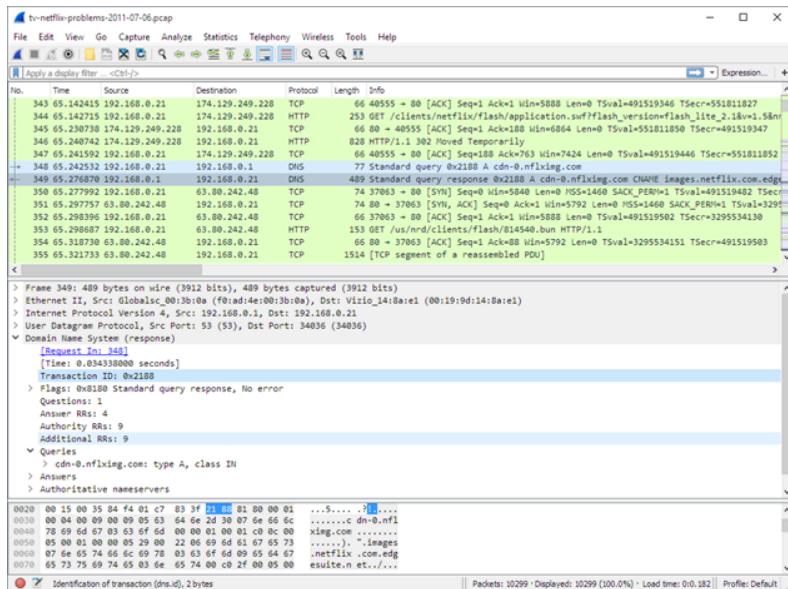
4.5. Herramientas de análisis de red

Las herramientas de análisis de red son claves, proporcionando la capacidad de monitorear, diagnosticar y solucionar problemas de red en tiempo real. Entre las más destacadas se encuentran herramientas capaces de capturar y analizar paquetes que permiten a los usuarios inspeccionar cada bit de tráfico de red, facilitando la detección de anomalías y potenciales amenazas.

Estas herramientas son fundamentales para el mantenimiento de una red segura, proporcionando una línea de defensa proactiva y facilitando la implementación de medidas correctivas en tiempo real. Algunos ejemplos de ellas serían:

1. **Wireshark:**

Wireshark es una herramienta de análisis de protocolos de red, conocida por su capacidad para capturar y examinar datos en tiempo real. Su interfaz gráfica intuitiva permite a los usuarios filtrar y analizar paquetes específicos. Un uso típico es la identificación de paquetes maliciosos que podrían indicar un ataque.



Por ejemplo, para capturar tráfico de una interfaz específica y guardar la captura en un archivo para un análisis posterior, se puede ejecutar:

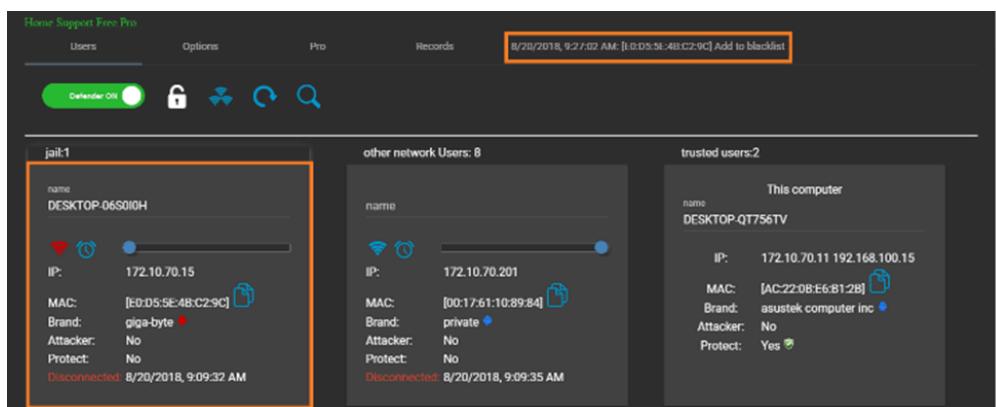
```
wireshark -i eth0 -w capture.pcap
```

Este comando captura el tráfico de la interfaz `eth0` y lo guarda en `capture.pcap`.

Posteriormente, se pueden aplicar filtros en Wireshark para buscar patrones específicos, como intentos de intrusión o tráfico sospechoso.

2. Netcut:

Netcut es una herramienta diseñada para controlar las conexiones de red en una LAN. Permite a los usuarios identificar todos los dispositivos conectados y gestionar el tráfico hacia ellos. Es especialmente útil en situaciones donde se necesita desconectar dispositivos no autorizados de la red. En su interfaz, se puede ver la lista de dispositivos conectados, y al seleccionar uno, se puede cortar su acceso a la red con un solo clic, lo que es útil para mantener la seguridad en entornos con múltiples usuarios.



3. AirCrack-ng:

AirCrack-ng es un conjunto de herramientas para evaluar la seguridad de redes WiFi. Es conocido por su capacidad para descifrar claves WEP y WPA/WPA2. El proceso de auditoría comienza capturando paquetes, seguido de un ataque de fuerza bruta para obtener la clave de la red. Un ejemplo de uso es la captura de paquetes de una red específica:

```
airodump-ng -c <channel> --bssid <BSSID> -w output mon0
```

Aquí, `<channel>` es el canal de la red WiFi, `<BSSID>` es la dirección MAC del punto de acceso, y `output` es el archivo donde se almacenarán los paquetes capturados. Después de capturar suficientes paquetes, se puede usar `aircrack-ng` para intentar descifrar la clave.

```
E4:A7:C5:70:7F:E2 11 -26 37 Aircrack-ng 1.3 5 34
00:14:BF:AE:15:6C 11 -48 59 0 0 0 0 0
00:00:CA:92:63:AE 11 -36 74446 333 0 0 0 0
00:9D:AB:47:C7:D1 1 [00:00:00] Tested 3 keys (got 47448 IVs) 8
04:00:30:2A:00:00 11 -26 0 0 0 0 0 5
04:01:20:00:00:00 11 -26 0 0 0 0 0 1
KB depth 0: byte(vote)
04:00:10:00:00:00 DC(66304) F5(58368) F4(56576) 1F(55808) EF(55040) 28(54272)
 1 0/ 1 3F(71424) 7C(59648) A2(56320) AB(56320) 11(55296) E0(55296)
pot kali 0/wifi# 73(64000) 5F(56064) 15(55552) 29(55552) 32(55040) 36(54784)
 3 0/ 1 7A(67840) D1(54784) 0E(54272) 25(54272) 49(53760) 99(53760)
 4 0/ 1 05(64000) B1(57600) B0(57088) 39(56576) 34(55040) 63(54272)
 5 0/ 1 FE(60160) 38(57088) CC(56576) FB(55552) E4(54528) E6(54528)
 6 0/ 1 6C(61696) AE(56576) 88(56320) B6(56320) 8B(55808) EE(55040)
 7 0/ 1 BF(62208) D8(60672) FC(56320) 14(55808) 73(55808) 7C(55296)
 8 0/ 1 68(65024) 09(56064) 31(56064) 30(55296) A0(55040) 8D(54528)
 9 0/ 1 A6(60160) 72(57856) 4F(56320) 5B(56320) 7F(56064) 88(56064)
10 0/ 2 07(58112) AF(57344) 27(56320) BB(56320) 4A(55040) 42(54528)
11 0/ 1 2F(57856) E6(56832) BD(56320) B5(55040) 1F(54272) DF(54272)
12 0/ 1 DF(67072) 27(57088) 35(56832) FB(56832) 07(56576) 57(55040)

KEY FOUND! [ DC:3F:73:7A:05:FE:6C:BF:68:A6:6B:2F:DF ]
Decrypted correctly: 100%
```

4. NMap:

NMap (Network Mapper) es una herramienta de escaneo de redes utilizada para descubrir hosts y servicios en una red. Es altamente configurable y puede realizar escaneos detallados, desde detección de sistemas operativos hasta la identificación de puertos abiertos.

```
(kali㉿kali)-[~/Desktop]
$ nmap -v -sT 10.10.2.144
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-04 07:03 EDT
Initiating Ping Scan at 07:03
Scanning 10.10.2.144 [2 ports]
Completed Ping Scan at 07:03, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:03
Completed Parallel DNS resolution of 1 host. at 07:03, 0.03s elapsed
Initiating Connect Scan at 07:03
Scanning 10.10.2.144 [1000 ports]
Discovered open port 21/tcp on 10.10.2.144
Discovered open port 53/tcp on 10.10.2.144
Discovered open port 80/tcp on 10.10.2.144
Discovered open port 3389/tcp on 10.10.2.144
Discovered open port 135/tcp on 10.10.2.144
Completed Connect Scan at 07:04, 11.39s elapsed (1000 total ports)
Nmap scan report for 10.10.2.144
Host is up (0.19s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
3389/tcp  open  ms-wbt-server

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.74 seconds
```

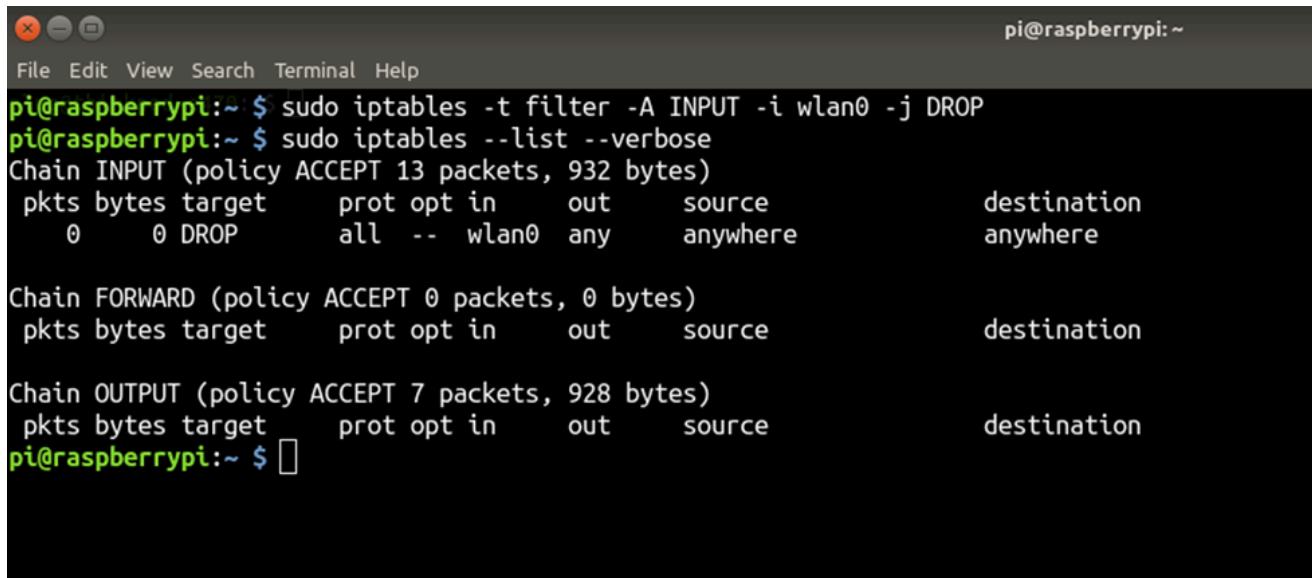
Un comando típico para realizar un escaneo de puertos rápidos es:

```
nmap -T4 -F <ip_address>
```

Este comando escanea rápidamente los puertos más comunes en el host especificado por <ip_address>. NMap también permite escaneos más profundos, incluyendo detección de versiones de software y servicios, lo cual es crucial para identificar vulnerabilidades en una red.

5. **iptables:**

iptables es una herramienta de administración de firewall en sistemas Linux. Se utiliza para configurar reglas de filtrado de paquetes que determinan qué tráfico está permitido o bloqueado. Es extremadamente flexible y se puede utilizar para establecer políticas complejas de seguridad.



The screenshot shows a terminal window titled 'Terminal' with the command line interface 'pi@raspberrypi:~\$'. The user has run the command 'sudo iptables -t filter -A INPUT -i wlan0 -j DROP' to add a rule that drops all incoming traffic on the wlan0 interface. Then, they ran 'sudo iptables --list --verbose' to view the current iptables rules. The output shows three chains: INPUT (policy ACCEPT), FORWARD (policy ACCEPT), and OUTPUT (policy ACCEPT). The INPUT chain contains one rule: 'DROP' on wlan0. The FORWARD and OUTPUT chains have no rules listed.

```
File Edit View Search Terminal Help
pi@raspberrypi:~$ sudo iptables -t filter -A INPUT -i wlan0 -j DROP
pi@raspberrypi:~ $ sudo iptables --list --verbose
Chain INPUT (policy ACCEPT 13 packets, 932 bytes)
  pkts bytes target     prot opt in     out     source               destination
      0    0  DROP        all   --  wlan0   any    anywhere
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 7 packets, 928 bytes)
  pkts bytes target     prot opt in     out     source               destination
pi@raspberrypi:~ $
```

Un ejemplo de regla para permitir tráfico solo desde una dirección IP específica es:

```
iptables -A INPUT -s <trusted_ip> -j ACCEPT
iptables -A INPUT -j DROP
```

Aquí, <trusted_ip> es la dirección IP permitida. La primera regla acepta tráfico desde esa IP, mientras que la segunda descarta todo el tráfico restante. Esto asegura que solo los dispositivos autorizados puedan comunicarse con el servidor, fortaleciendo así la seguridad de la red.

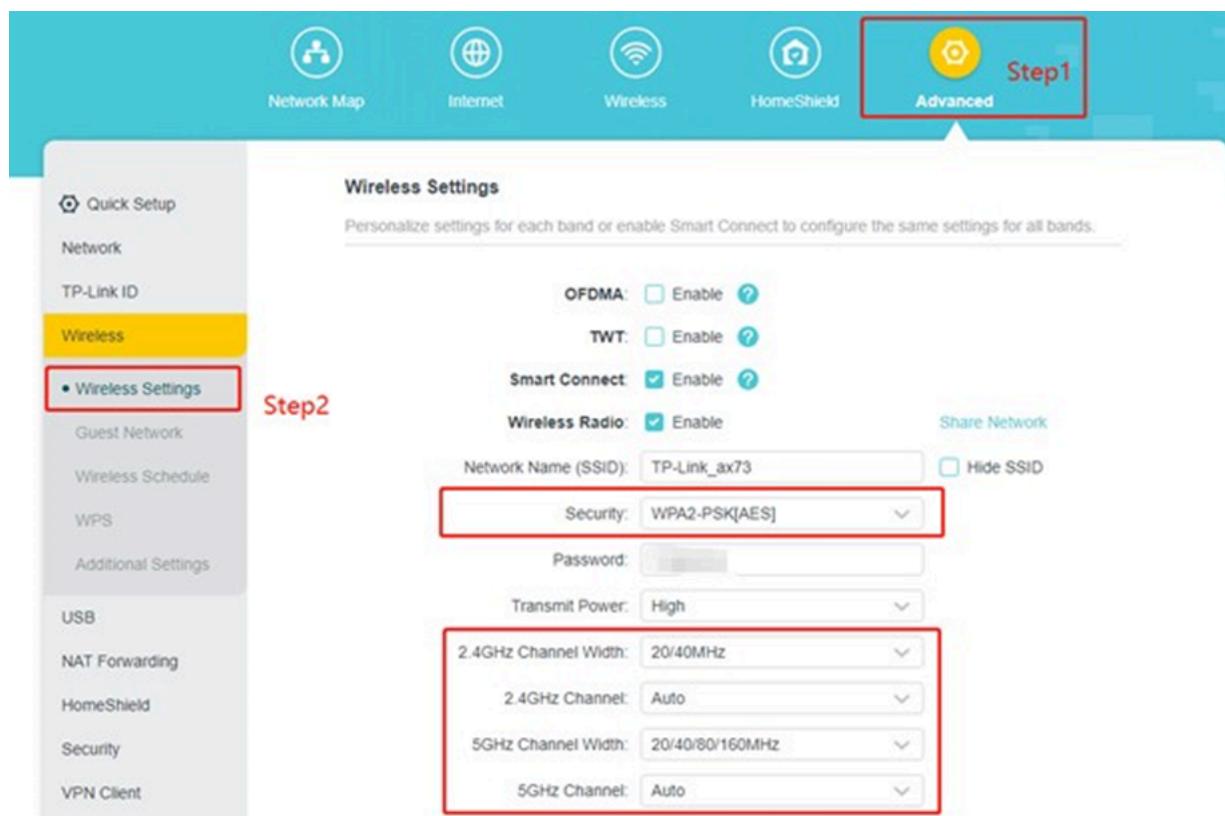
4.6. Medidas Preventivas en Enrutadores

La seguridad de los enrutadores es fundamental para proteger las redes WiFi contra intrusiones y asegurar la integridad de los datos transmitidos. Implementar medidas preventivas adecuadas no solo fortalece la defensa contra posibles ataques, sino que también minimiza las vulnerabilidades. A continuación, se exploran algunas de las medidas más efectivas:

- *Actualización Regular del Firmware:* Mantener el firmware del enrutador actualizado es crucial para eliminar vulnerabilidades conocidas y mejorar la estabilidad y seguridad general del dispositivo. Los fabricantes suelen lanzar actualizaciones que corrigen problemas de seguridad, por lo que es recomendable configurar el enrutador para que se actualice automáticamente o verificar manualmente las actualizaciones disponibles.
- *Cambio de Contraseñas Predeterminadas:* Las contraseñas predeterminadas de fábrica son conocidas por los hackers y representan un riesgo significativo. Cambiar tanto la contraseña de administración del enrutador como la del SSID de la red WiFi a contraseñas fuertes y únicas es una práctica básica pero efectiva para prevenir accesos no autorizados.

autorizados.

- *Desactivación de Funcionalidades No Utilizadas*: Muchos enrutadores vienen con funciones habilitadas por defecto que no son esenciales para el funcionamiento diario, como UPnP (Plug and Play) o el control remoto a través de la web. Desactivar estas funciones reduce la superficie de ataque y mejora la seguridad general del enrutador.
- *Filtrado de Direcciones MAC*: Configurar el enrutador para filtrar direcciones MAC permite limitar el acceso solo a dispositivos específicos cuyas direcciones MAC estén en una lista blanca. Esto dificulta el acceso a la red a dispositivos no autorizados que intenten conectarse utilizando direcciones MAC falsificadas.
- *Configuración de Firewall*: Utilizar las capacidades de firewall integradas en el enrutador para establecer reglas que filtren el tráfico entrante y saliente según criterios específicos. Por ejemplo, se pueden bloquear rangos de direcciones IP conocidos por ser maliciosos o limitar los servicios accesibles desde el exterior.



4.7. Maquina Virtual SEC Pretorian

La Máquina Virtual de SEC Pretorian, basada en el sistema operativo Kali Linux, se desarrolla con el propósito de detectar y responder a intrusiones en redes WiFi de manera eficiente y efectiva.

Esta herramienta especializada aprovecha las capacidades avanzadas de Kali Linux para ofrecer funcionalidades específicas de detección y defensa:

Detección de Intrusiones en Tiempo Real: Pretorian utiliza técnicas avanzadas de análisis de paquetes para monitorear y detectar actividades sospechosas en la red WiFi. Esto incluye la captura y análisis de tráfico para identificar patrones de comportamiento típicos de intrusos.

Interfaz Gráfica de Usuario (GUI) Intuitiva: La GUI de Pretorian facilita la visualización y comprensión de datos de seguridad en tiempo real. Permite a los administradores de red identificar rápidamente dispositivos no autorizados y tomar acciones correctivas de manera inmediata.

Herramientas Integradas de Análisis: Incorpora herramientas como Wireshark y Aircrack-ng, que permiten la captura y análisis exhaustivo de paquetes, así como la simulación de ataques para evaluar la resistencia de la red frente a posibles intrusiones.

Capacidades de Respuesta Automatizada: Pretorian está diseñado para actuar rápidamente ante amenazas detectadas, incluyendo la capacidad de desconectar dispositivos no autorizados y aplicar políticas de seguridad en tiempo real, minimizando así el impacto de los ataques.

La Máquina Virtual de SEC Pretorian representa una solución integral para la seguridad en redes WiFi, ofreciendo detección avanzada de amenazas y herramientas robustas para la respuesta proactiva y la mitigación de riesgos.



4.8. Network Security Monitoring (NSM)

El Network Security Monitoring (NSM) es una práctica fundamental en la gestión de la seguridad de redes, centrada en la detección temprana y respuesta ante actividades anómalas que podrían indicar un compromiso de seguridad. Este enfoque estratégico incluye varios componentes esenciales:

NSM se basa en la recopilación continua de datos de tráfico de red, logs de sistemas y otros eventos relevantes. Este proceso genera un flujo constante de información que luego se analiza en busca de comportamientos sospechosos o maliciosos.

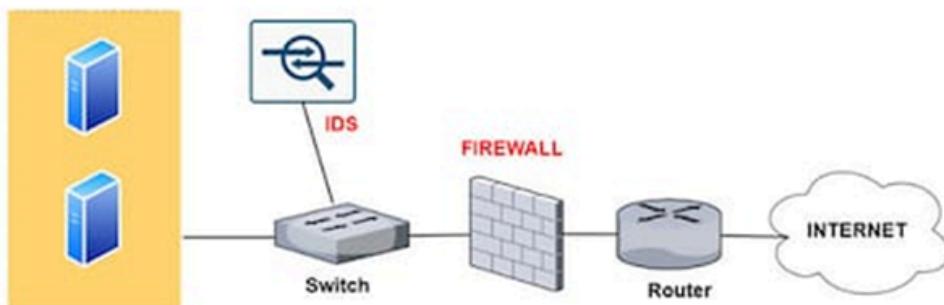
Utilizando herramientas especializadas, una NSM examina detalladamente los datos recopilados para identificar patrones de tráfico anómalos que podrían indicar actividades no autorizadas. Por ejemplo, la correlación de eventos puede revelar intentos de exploración de red o tráfico malicioso.

Cuando NSM detecta una actividad sospechosa, genera alertas inmediatas que notifican a los administradores de seguridad. Estas alertas incluyen información detallada sobre la naturaleza del incidente y recomendaciones para la respuesta adecuada.

No solo se centra en la detección en tiempo real, sino que también facilita la respuesta forense ante incidentes de seguridad. Permite la reconstrucción de eventos pasados y el análisis de la cadena de ataque, proporcionando insights cruciales para la mitigación de riesgos y la prevención de futuros incidentes.

4.9. Intrusion Detection System (IDS)

Un Sistema de Detección de Intrusiones (IDS) es una herramienta esencial en la seguridad de redes, diseñada para monitorear activamente el tráfico de red en busca de actividades anómalas que puedan indicar intentos de intrusión. Funciona de manera pasiva, analizando continuamente los patrones de tráfico y comparándolos con firmas conocidas de ataques o comportamientos maliciosos.



Hay dos tipos principales de IDS:

El IDS Basado en Red examina el tráfico de red para identificar patrones sospechosos utilizando técnicas como la inspección de paquetes y el análisis de protocolos. Detecta actividades como escaneos de puertos, intentos de penetración y tráfico inusual que podrían indicar amenazas en la red.

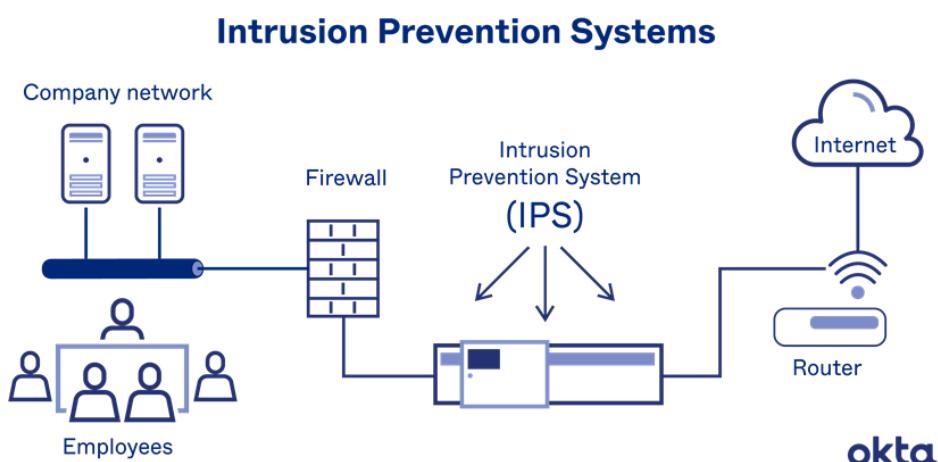
Por otro lado, el IDS Basado en Host se enfoca en detectar actividades sospechosas en hosts individuales. Monitoriza los registros de eventos y las actividades del sistema operativo para identificar comportamientos inusuales como intentos de acceso no autorizado o modificaciones no autorizadas de archivos de sistema.

4.10. Intrusion Prevention System (IPS)

Un Sistema de Prevención de Intrusiones (IPS) va más allá de las capacidades de un IDS al no solo detectar actividades anómalas, sino también tomar medidas activas para bloquear o prevenir ataques en tiempo real. Utiliza técnicas avanzadas como la inspección profunda de paquetes y la aplicación de reglas de seguridad para responder automáticamente a las amenazas identificadas. Los IPS pueden operar de dos formas principales:

En modo de prevención en línea (inline), donde los paquetes sospechosos se bloquean en tiempo real antes de que lleguen al destino final, protegiendo así la red y los sistemas contra ataques conocidos y desconocidos.

En modo de prevención fuera de línea (out-of-band), donde se registran las amenazas identificadas y se toman medidas correctivas para evitar futuros incidentes similares.



La implementación efectiva de un IPS mejora la capacidad de respuesta ante amenazas y reduce la carga operativa al automatizar la detección y mitigación de riesgos de seguridad en entornos de red complejos y dinámicos.

4.11. Modus operandi de intrusos

El modus operandi de los intrusos se refiere a los métodos y técnicas utilizadas por los hackers y ciberdelincuentes para infiltrarse en sistemas y redes con el fin de obtener acceso no autorizado o causar daño. Comprender estos patrones de comportamiento es crucial para desarrollar estrategias efectivas de defensa y mitigación de riesgos.

Ingeniería Social: Los intrusos pueden utilizar tácticas de manipulación psicológica para engañar a usuarios y obtener acceso a información confidencial, como contraseñas o datos de acceso.

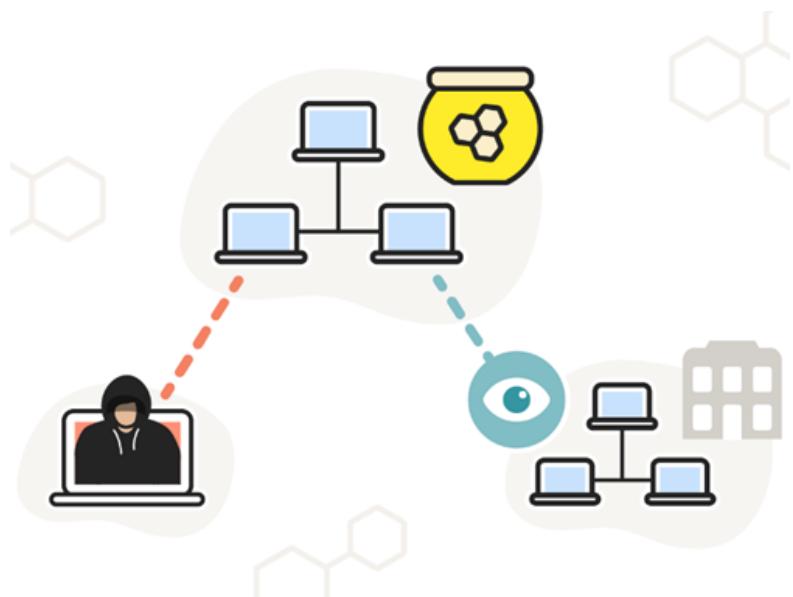
- ❖ **Ataques de Fuerza Bruta:** Intentos repetidos y automáticos para adivinar contraseñas mediante la prueba sistemática de diferentes combinaciones.
- ❖ **Explotación de Vulnerabilidades Conocidas:** Aprovechar fallos de seguridad en software, sistemas operativos o configuraciones mal protegidas para obtener acceso no autorizado.
- ❖ **Phishing y Spear Phishing:** Envío de correos electrónicos o mensajes falsos que parecen legítimos para engañar a los usuarios y hacer que revelen información confidencial o descarguen malware.
- ❖ **Inyección de Código Malicioso:** Insertar código malicioso, como malware o scripts, en sistemas y aplicaciones vulnerables para tomar control del sistema o robar información.
- ❖ **Uso de Herramientas Especializadas:** Utilización de herramientas como exploits, troyanos y rootkits para facilitar el acceso y el control remoto de sistemas comprometidos.

4.12. Honeypots

Los Honeypots son dispositivos o sistemas diseñados específicamente para atraer a los intrusos y desviar su atención lejos de los sistemas y datos reales de una red. Actúan como señuelos que imitan sistemas vulnerables o servicios de red auténticos, pero están configurados para registrar y analizar las actividades de los atacantes. La principal finalidad de un Honeypot es recopilar información detallada sobre las tácticas, técnicas y procedimientos utilizados por los atacantes, permitiendo a los equipos de seguridad entender mejor las amenazas y mejorar sus estrategias defensivas.

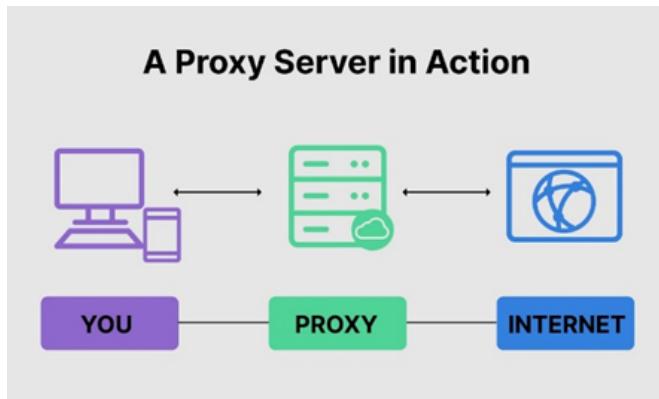
Funcionamiento de los Honeypots

1. Los Honeypots se configuran para parecer sistemas reales con vulnerabilidades específicas que los atacantes buscarían explotar. Esto puede incluir servicios comunes, configuraciones de software conocidas por ser vulnerables y datos señuelo que parecen valiosos.
2. Una vez que un atacante interactúa con el Honeypot, todas sus acciones son registradas. Esto incluye intentos de acceso, comandos ejecutados, y cualquier técnica utilizada para comprometer el sistema.
3. La información recopilada se analiza para identificar patrones y técnicas de ataque. Esto permite a las organizaciones ajustar sus medidas de seguridad, parchear vulnerabilidades y desarrollar respuestas más efectivas ante amenazas similares en sus sistemas reales.



4.13. Proxy Server

Un Proxy Server actúa como intermediario entre los usuarios y los recursos en Internet, proporcionando una variedad de funcionalidades que mejoran la seguridad, la privacidad y el rendimiento de la red. Al interceptar y reenviar las solicitudes de los clientes, un Proxy Server oculta la dirección IP real del cliente y permite el filtrado y control del tráfico, lo que protege a los usuarios de posibles amenazas y mejora la gestión de recursos.



Filtran contenido malicioso y bloquear el acceso a sitios web peligrosos, protegiendo a los usuarios contra malware y otras amenazas cibernéticas. Además, pueden implementar políticas de acceso basadas en direcciones IP, horarios, o tipos de contenido, asegurando que solo usuarios autorizados accedan a ciertos recursos.

Al ocultar la dirección IP del cliente, los Proxy Servers ayudan a mantener la privacidad del usuario, evitando que terceros rastreen sus actividades en línea. Esto es especialmente útil para proteger la identidad de los usuarios y evitar la recopilación de datos no autorizada.

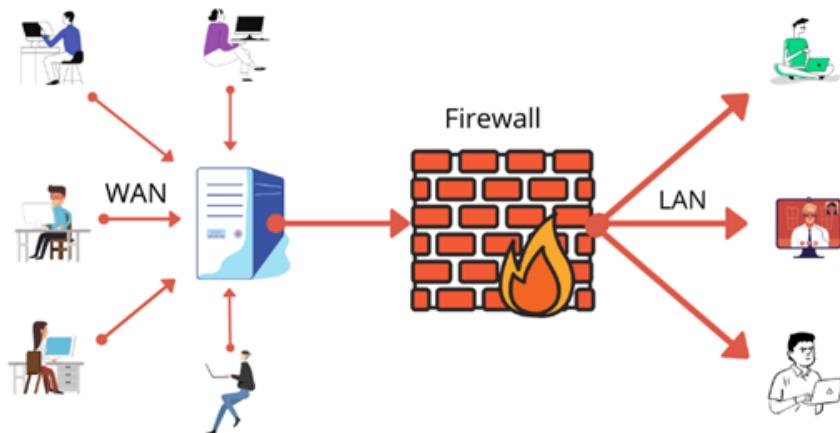
Pueden cachear contenido, lo que reduce el tiempo de carga para los usuarios y disminuye el uso del ancho de banda. Al almacenar copias de recursos solicitados frecuentemente, un proxy puede responder a futuras solicitudes más rápidamente sin tener que volver a contactar el servidor original.

Tipos de Proxy Servers

1. **Proxy HTTP/HTTPS:** Manejan el tráfico web (HTTP y HTTPS). Los proxies HTTPS proporcionan una capa adicional de seguridad al manejar tráfico cifrado, protegiendo la integridad y confidencialidad de los datos.
2. **Proxy Reverso:** Actúa como intermediario para los servidores, manejando las solicitudes entrantes y distribuyéndolas entre varios servidores backend. Esto optimiza el rendimiento mediante el balanceo de carga y la caché.

4.14. Firewalls físicos y firewalls con inteligencia artificial

Un firewall es un sistema de seguridad diseñado para controlar el tráfico de red entre dos o más redes, aplicando políticas de seguridad que determinan qué tráfico puede pasar y cuál debe ser bloqueado. Funciona inspeccionando y filtrando los paquetes de datos que entran y salen de la red según reglas configuradas por los administradores.



¿Dónde puede ejecutarse un firewall?

- **A nivel de red:** Implementado en el perímetro de la red para proteger la infraestructura completa.
- **A nivel de host:** Instalado en servidores individuales o dispositivos finales para protegerlos de amenazas específicas.

Firewall físico

Un Firewall físico es un dispositivo hardware dedicado diseñado para controlar el tráfico de red y aplicar políticas de seguridad para proteger los sistemas y datos contra accesos no autorizados y ataques maliciosos. Funciona inspeccionando paquetes de datos que entran y salen de la red, aplicando reglas configuradas para permitir o bloquear el tráfico según criterios específicos.

Ventajas del Firewall físico:

- Rendimiento dedicado: No comparte recursos con otros servicios.
- Seguridad robusta: Difícil de manipular sin acceso físico al dispositivo.
- Gestión centralizada: Fácil de administrar múltiples políticas de seguridad.



Firewalls basados en Inteligencia Artificial

Los Firewalls basados en Inteligencia Artificial (AI) utilizan algoritmos avanzados de aprendizaje automático y análisis de comportamiento para detectar y responder a amenazas en tiempo real. A diferencia de los Firewalls tradicionales, que dependen de reglas estáticas, los Firewalls basados en AI pueden adaptarse dinámicamente a patrones de tráfico cambiantes y identificar anomalías que podrían indicar actividades maliciosas.

Características del Firewall basado en AI:

- *Aprendizaje Automático*: Mejora continuamente su capacidad para detectar amenazas a medida que analiza más datos.
- *Detección de Anomalías*: Identifica comportamientos inusuales que pueden indicar ataques.
- *Respuesta en Tiempo Real*: Puede actuar inmediatamente ante amenazas detectadas, minimizando el impacto potencial.
- *Adaptabilidad*: Ajusta sus políticas y reglas automáticamente en función de nuevas amenazas y patrones de tráfico.

4.15. Desvinculación de IP de administración

La desvinculación de la IP de administración es una medida para proteger los dispositivos de red, como enruteadores y switches, contra accesos no autorizados desde la red pública o Internet. Consiste en configurar estos dispositivos para que la interfaz de administración solo sea accesible desde direcciones IP específicas o segmentos de red internos, restringiendo así el acceso desde ubicaciones externas no confiables.

4.16. Modificación de SSID y contraseñas

El SSID es el nombre de la red visible para los usuarios y, aunque puede parecer una medida menor, cambiarlo regularmente puede disuadir a los atacantes de focalizarse en una red específica. La contraseña, por otro lado, es la clave de acceso que asegura la comunicación cifrada entre los dispositivos y el punto de acceso Wi-Fi.

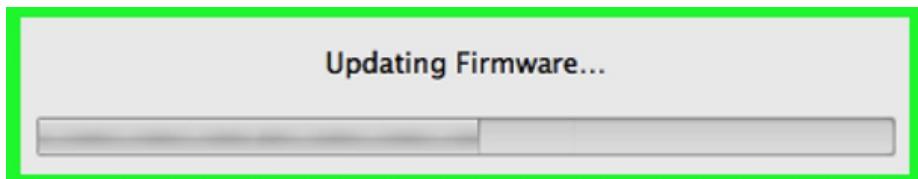
Utilizar contraseñas fuertes y únicas, y cambiarlas periódicamente, reduce significativamente el riesgo de que sean adivinadas o comprometidas mediante ataques de fuerza bruta, de diccionario o ingeniería social.

4.17. Actualización del Firmware del enrutador

La actualización regular del firmware del enrutador es crucial para mantener la seguridad y el rendimiento óptimo del dispositivo. Las actualizaciones de firmware incluyen parches de

seguridad que corrigen vulnerabilidades descubiertas en versiones anteriores. Ignorar estas actualizaciones puede dejar el dispositivo expuesto a exploits conocidos y ataques dirigidos.

Los fabricantes lanzan actualizaciones de firmware para resolver problemas de seguridad, mejorar la estabilidad y añadir nuevas funcionalidades.



4.18. Análisis de tráfico en tiempo real

El análisis de tráfico en tiempo real es una práctica fundamental en la seguridad de redes que permite monitorear y detectar actividades anómalas o maliciosas en la red mientras ocurren. Esta técnica proporciona visibilidad instantánea sobre el tráfico de datos, permitiendo la identificación de patrones sospechosos, ataques de denegación de servicio (DoS) o intentos de intrusión que podrían comprometer la seguridad de la red. Al analizar el tráfico en tiempo real, los administradores pueden reaccionar rápidamente ante amenazas emergentes, minimizar el impacto de los ataques y ajustar las políticas de seguridad en consecuencia.

Ejemplo de herramientas para análisis de tráfico en tiempo real:

1. **Wireshark:** Captura y analiza paquetes de red en tiempo real, permitiendo a los administradores identificar comportamientos sospechosos o tráfico malicioso con una interfaz gráfica detallada.
2. **tcpdump:** Herramienta de línea de comandos que captura y muestra paquetes en tiempo real, proporcionando una opción poderosa y flexible para el monitoreo detallado del tráfico de red en entornos Unix/Linux.

4.19. Formación y capacitación en ciberseguridad

La formación y capacitación son esenciales para educar a los empleados sobre las mejores prácticas de seguridad cibernética, políticas de uso aceptable y procedimientos para proteger activos críticos de la organización. Esto incluye la sensibilización sobre amenazas comunes, técnicas de mitigación y respuesta a incidentes para fortalecer la postura de seguridad de la red.

La formación continua en seguridad de redes asegura que el personal esté preparado para enfrentar y mitigar los constantes desafíos de seguridad cibernética en un entorno empresarial cada vez más digitalizado y conectado.

Algunos de las prácticas más importantes a nivel empresa de formación y capacitación de los empleados pueden ser:

- **Políticas de seguridad:** Implementación de políticas robustas de contraseñas, acceso y auditoría de seguridad.
- **Respuesta a incidentes:** Procedimientos para manejar y mitigar ataques de seguridad, incluyendo notificación y recuperación.
- **Herramientas de seguridad:** Uso adecuado de herramientas como firewalls, IDS/IPS y sistemas de detección de malware.



5. Metodología de Trabajo

5.1. Planificación del proyecto y metodología utilizada

La planificación del proyecto se llevó a cabo utilizando JIRA para gestionar y documentar las tareas y el progreso. Se realizaron sprints semanales de una semana cada uno, permitiendo una gestión ágil y flexible del proyecto. El enfoque metodológico adoptado fue mixto, combinando tanto técnicas cualitativas como cuantitativas para abordar de manera integral la seguridad de las redes WiFi. Este enfoque permitió una comprensión profunda y exhaustiva del problema de investigación.

Detalles del plan de trabajo

El plan de trabajo se estructuró en actividades específicas, cada una asignada a un miembro del equipo, cubriendo tanto la parte práctica como la redacción del paper:

1. Investigación y recopilación de información:

- **Objetivo:** Identificar técnicas de seguridad y analizar herramientas especializadas..
- **Actividades:**
 - Revisión de literatura y fuentes relevantes.
 - Evaluación de técnicas y herramientas utilizadas para detectar intrusiones en redes WiFi.

2. Implementación de medidas preventivas:

- **Objetivo:** Configurar enrutadores y aplicar prácticas de seguridad.
- **Actividades:**
 - Configuración de parámetros de seguridad en enrutadores.
 - Implementación de medidas preventivas en redes.

3. Desarrollo de la máquina virtual "PRETORIAN":

- **Objetivo:** Programar y probar la solución de detección en tiempo real.
- **Actividades:**
 - Desarrollo de la máquina virtual.
 - Pruebas y ajustes de la solución de detección de intrusiones.

4. Evaluación y análisis:

- **Objetivo:** Probar la efectividad y ajustar estrategias.
- **Actividades:**
 - Ejecución de pruebas de penetración.
 - Análisis de datos y ajuste de medidas de seguridad.

5. Redacción y revisión del paper:

- **Objetivo:** Documentar los hallazgos y resultados de la investigación.
- **Actividades:**
 - Escritura de secciones del paper.
 - Revisión y edición del documento final.

El cronograma se organizó en sprints semanales, con objetivos claros y revisiones al final de cada sprint para evaluar el progreso y ajustar el plan si era necesario. Cada sprint incluyó actividades específicas para la parte práctica y la redacción del paper, asegurando un avance equilibrado en ambas áreas.

Registro de reuniones y decisiones clave

Se mantuvo un registro detallado de todas las reuniones de equipo, incluyendo temas discutidos y decisiones tomadas. Las reuniones se documentaron en JIRA, lo que permitió un seguimiento claro de los avances y cambios en el proyecto. Cualquier ajuste en el plan de trabajo o enfoque metodológico se registró y justificó adecuadamente.

5.2. Mapeo de la Bibliografía y su Relevancia

La organización y análisis de la bibliografía consultada se realizó de manera sistemática. Se identificaron las fuentes más relevantes, clasificándolas según su relevancia para el tema de investigación. Cada fuente fue evaluada por su contribución a la comprensión del problema de seguridad en redes WiFi y su relación con las soluciones propuestas en el proyecto.

Identificación de las fuentes más relevantes

Las fuentes más relevantes fueron aquellas que proporcionaron información detallada sobre las técnicas de intrusión, las herramientas utilizadas por los intrusos, y las estrategias de defensa efectivas. Estas fuentes se utilizaron para fundamentar las decisiones del proyecto y para desarrollar la máquina virtual "PRETORIAN". El análisis bibliográfico permitió asegurar que el proyecto se basara en conocimientos actualizados y pertinentes en el campo de la ciberseguridad.

Al mantener una planificación detallada y una documentación exhaustiva, se garantizó que el proyecto avanzara de manera organizada y efectiva, integrando tanto el desarrollo práctico como la redacción académica del paper.

6. Descripción del Proceso de Documentación

6.1. Introducción

En el contexto del desarrollo de nuestro paper sobre la seguridad en redes Wi-Fi presentado en el WICC 2024, hemos decidido documentar minuciosamente cada paso del proceso para futuras referencias y posibles publicaciones. Para ello, hemos adoptado un enfoque ágil utilizando Scrum y JIRA para gestionar nuestras tareas y sprints de una semana.

6.2. Metodología

El proceso de documentación ha sido dividido en varios sprints, cada uno con una duración de una semana. Esto nos ha permitido mantener un ritmo constante y asegurar que cada parte del proyecto sea abordada de manera sistemática. A continuación, se detalla la metodología Scrum que hemos utilizado:

1. Weekly Stand-up (Reunión Semanal): Durante este proceso llevamos a cabo reuniones semanales (stand-ups) para hacer un seguimiento del progreso y resolver cualquier impedimento. Estas reuniones son breves y permiten mantener la comunicación fluida entre los miembros del equipo.
2. Sprint Execution (Ejecución del Sprint): Durante la semana, cada miembro del equipo trabaja en sus respectivas tareas. JIRA nos permite hacer seguimiento del progreso y colaborar de manera eficiente.
3. Sprint Review (Revisión del Sprint): Al final de cada semana, realizamos una reunión de revisión del sprint para evaluar el progreso y demostrar el trabajo completado. Las tareas completadas son revisadas y se proporciona retroalimentación.
4. Sprint Retrospective (Retrospectiva del Sprint): Tras la revisión del sprint, llevamos a cabo una retrospectiva para reflexionar sobre el sprint que acaba de finalizar. Identificamos lo que funcionó bien, lo que no funcionó y cómo podemos mejorar en el siguiente sprint.

6.2.1. Descripción Semanal del Proceso

The screenshot shows a Jira software interface for a project titled 'Investigación Seguridad en Redes WiFi'. The left sidebar includes options like 'Planning', 'Timeline', 'Backlog', 'Board', 'Calendar', 'List', 'Goals', 'Issues', 'Code', 'Project pages', 'Add shortcut', and 'Project settings'. The main area is titled 'Backlog' and shows a list of tasks under 'Sprint 1' (19 May - 2 Jun) with 12 issues. The tasks are:

- SRW-7: Verificar Contenido a Documento
- SRW-8: Generar estructura documentación
- SRW-9: Realizar Introducción [Abstract]
- SRW-10: Realizar Introducción [Motivación y objetivos]
- SRW-11: Realizar Introducción [Grupo y Roles]
- SRW-12: Dividir el trabajo - Introducción
- SRW-13: Realizar Estado del Arte - | Definir Estrategia de Búsqueda
- SRW-14: Realizar Estado del Arte - | Sintetizar la Información
- SRW-15: Realizar Estado del Arte - | Revisión Bibliográfica
- SRW-16: Realizar Estado del Arte - | Identificar Fuentes de Información
- SRW-18: Revisar y Corregir posibles errores

On the right, there is a timeline from 10:00 to 10:00 with several tasks assigned to team members (VY, MT, etc.) with different status indicators (green, orange, blue).

Sprint 1: Generación de la Estructura de Investigación y Redacción de la Introducción

- Objetivo: Definir la estructura general del documento y redactar la introducción.
- Tareas:
 - Crear la estructura de la investigación.
 - Dividir el trabajo entre los miembros del equipo.
 - Redactar la introducción del documento.

Imagen de JIRA:

The screenshot shows the JIRA interface for a project titled "Investigacion Seguridad en Redes WiFi". The main view is a Kanban board for "SOF Sprint 1".

Left Sidebar (PLANNING):

- Investigacion Seguridad ... Software project
- Timeline
- Backlog
- Board** (selected)
- Calendar NEW
- List
- Goals
- Issues
- + Add view

Left Sidebar (DEVELOPMENT):

- Code
- Project pages
- Add shortcut
- Project settings

Top Bar:

- Your work
- Projects
- Filters
- Dashboards
- Teams
- Plans
- Apps
- Create

Header:

Projects / Investigacion Seguridad en Redes WiFi
SOF Sprint 1
Tenerlo terminado para la Primer Entrega de Ingenieria de Software

Search Bar:

Search JP VT

Board View:

Column	Issue	Assignee
TO DO 5	Generar estructura documentacion	VT
	Dividir el trabajo - Introduccion	JP
	Realizar Introduccion [Abstract]	JP
	Realizar Introduccion [Motivacion y objetivos]	VT
	Realizar Introduccion [Grupo y Roles]	VT
+ Create issue		
IN PROGRESS	SRW-7	JP
	SRW-8	JP
	SRW-9	JP
	SRW-10	VT
	SRW-11	VT
DONE	SRW-7	JP
	SRW-8	JP
	SRW-9	JP
	SRW-10	VT
	SRW-11	VT

SOF Sprint 1
Tenerlo terminado para la Primer Entrega de Ingeniería de Software

TO DO	IN PROGRESS 3	DONE 2
+ Create issue	Realizar Introducción [Abstract] SRW-9 Realizar Introducción [Motivación y objetivos] SRW-10 Realizar Introducción [Grupo y Roles] SRW-11	Generar estructura documentación SRW-7 Dividir el trabajo - Introducción SRW-8
	+ Create issue	

SOF Sprint 1
Tenerlo terminado para la Primer Entrega de Ingeniería de Software

TO DO	IN PROGRESS	DONE 5
+ Create issue		Generar estructura documentación SRW-7 Dividir el trabajo - Introducción SRW-8 Realizar Introducción [Grupo y Roles] SRW-11 Realizar Introducción [Motivación y objetivos] SRW-10 Realizar Introducción [Abstract] SRW-9

Sprint 2: Desarrollo del Estado del Arte y Corrección de Errores

- Objetivo: Desarrollar la sección del estado del arte y realizar correcciones en el documento.
- Tareas:
 - Dividir el trabajo para la sección de estado del arte.
 - Investigar y redactar sobre la historia del arte en la seguridad en redes Wi-Fi.
 - Volcar la información en el documento.
 - Corregir errores encontrados en el documento.

Imagen de JIRA:

The screenshot shows a JIRA project board for 'SOF Sprint 2'. The left sidebar includes options like 'Timeline', 'Backlog', 'Board' (which is selected), 'Calendar', 'List', 'Goals', 'Issues', 'Add view', 'Code', 'Project pages', 'Add shortcut', and 'Project settings'. The main area displays a board with three columns: 'TO DO', 'IN PROGRESS', and 'DONE'. The 'TO DO' column contains tasks: 'Dividir Trabajo - Historia de Arte' (SRW-12), 'Realizar Estado del Arte - [Definir Estrategia de Busqueda]' (SRW-13), 'Realizar Estado del Arte - [Identificar Fuentes de Informacion]' (SRW-14), 'Realizar Estado del Arte - [Revision Bibliografica]' (SRW-15), 'Volcar Contenido a Documento' (SRW-17), 'Revisar y Corregir posibles errores' (SRW-18), 'Realizar Estado del Arte - [Sintetizar la Informacion]' (SRW-16), and 'Dividir Tareas' (SRW-20). The 'IN PROGRESS' and 'DONE' columns are currently empty.

The screenshot shows a Jira project board for 'SOF Sprint 2'. The left sidebar contains navigation links for 'Your work', 'Projects', 'Filters', 'Dashboards', 'Teams', 'Plans', 'Apps', and 'Create'. The main area displays a board with three columns: 'TO DO', 'IN PROGRESS 6', and 'DONE 1'. The 'TO DO' column has one task: 'Dividir Tareas' (SRW-20). The 'IN PROGRESS' column has six tasks: 'Realizar Estado del Arte - [Definir Estrategia de Búsqueda]' (SRW-13), 'Realizar Estado del Arte - [Identificar Fuentes de Información]' (SRW-14), 'Realizar Estado del Arte - [Revisión Bibliográfica]' (SRW-15), 'Realizar Estado del Arte - [Sintetizar la Información]' (SRW-16), 'Volcar Contenido a Documento' (SRW-17), and 'Revisar y Corregir posibles errores' (SRW-18). The 'DONE' column has one task: 'Dividir Trabajo - Historia de Arte' (SRW-12). A search bar and user icons (JP, VT, others) are at the top of the board.

The screenshot shows a Jira board for the project 'Investigacion Seguridad ... Software project'. The board is titled 'SOF Sprint 2'. It has three columns: 'TO DO 1', 'IN PROGRESS', and 'DONE 7'. A search bar and filter buttons (JP, VT) are at the top. The 'Board' view is selected on the left sidebar.

Column	Task Description	Status	Assignee
TO DO 1	Dividir Tareas	New	SRW-20
IN PROGRESS	Realizar Estado del Arte - [Definir Estrategia de Busqueda]	In Progress	SRW-12
	Realizar Estado del Arte - [Identificar Fuentes de Informacion]	In Progress	SRW-13
	Revisar y Corregir posibles errores	In Progress	SRW-14
	Volcar Contenido a Documento	In Progress	SRW-15
	Realizar Estado del Arte - [Revision Bibliografica]	In Progress	SRW-16
	Realizar Estado del Arte - [Sintetizar la Informacion]	In Progress	SRW-17
	Dividir Trabajo - Historia de Arte	Completed	SRW-18
	Realizar Estado del Arte - [Definir Estrategia de Busqueda]	Completed	SRW-19
DONE 7			

The screenshot shows the Jira software interface for a project titled "Investigación Seguridad en Redes WiFi". The left sidebar includes links for Planning, Backlog, Board, Calendar, List, Goals, Issues, Project pages, Add shortcut, and Project settings. The main area displays a "Backlog" view with a search bar and filter options (Sprint, Type, Status, Epic). A list of tasks is shown under "SOF Sprint 1: 19 May - 2 Jun (12 issues)", each with a green checkmark icon and a brief description. To the right, a "Burndown chart" shows progress over time, with a "Create sprint" button at the bottom. At the bottom of the backlog list, there is a section titled "What needs to be done?" containing three items.

Sprint 3: Contexto Académico del Proyecto

- **Objetivo:** Desarrollar la sección del contexto académico y su relación con el programa académico.
- **Tareas:**
 - Dividir el trabajo para la sección de contexto académico.
 - Investigar y redactar sobre el contexto académico del proyecto.
 - Relacionar el proyecto con el programa académico o institución.
 - Redactar sobre los antecedentes del problema de investigación.
 - Describir la supervisión de la investigación y el equipo de trabajo.
 - Referenciar al CAETI.
 - Volcar y corregir la información en el documento.

The screenshot shows a Jira project interface for a sprint titled 'Sprint 3' from June 17 to June 24. The backlog contains the following tasks:

- SRW-01: Redactar Contenido académico
- SRW-02: Análisis de los temas investigados
- SRW-03: Redactar Equipo de trabajo y referencia CAETI
- SRW-04: Área de investigación
- SRW-05: Desglose sección por sección
- SRW-06: Organizar Próxima Entrega
- SRW-07: Identificación de los principales puntos tratados
- SRW-08: Metodología de Trabajo
- SRW-09: Detalles del plan de trabajo
- SRW-10: Mapeo de la bibliografía y su relevancia
- SRW-11: Planificación del proyecto
- SRW-12: Detalles del plan de trabajo

The tasks are categorized by status: In Progress (4), To Do (4), and Done (4). A 'Create Sprint' button is visible at the bottom right.

The screenshot shows a Jira project board for 'Investigacion Seguridad en Redes WiFi'. The board is titled 'SOF Sprint 3'. It has three columns: 'TO DO 11', 'IN PROGRESS 1', and 'DONE'. The 'TO DO' column contains 11 tasks, the 'IN PROGRESS' column contains 1 task, and the 'DONE' column contains 0 tasks.

Column	Tasks
TO DO 11	Redactar Contexto académico (SRW-20), Redactar Equipo de trabajo y referencia CAETI (SRW-22), Área de Investigación (SRW-23), Análisis de los temas investigados (SRW-24), Desglose sección por sección (SRW-25), Identificación de los principales puntos tratados (SRW-26), Metodología de Trabajo (SRW-27), Detalles del plan de trabajo (SRW-28), Mapeo de la bibliografía y su relevancia (SRW-29), Planificación del proyecto (SRW-30), Detalles del plan de trabajo, (SRW-31)
IN PROGRESS 1	Organizar Proxima Entrega (SRW-19)
DONE	0

The sidebar on the left includes sections for PLANNING (Timeline, Backlog), DEVELOPMENT (Code), and other project management tools like Project pages, Add shortcut, and Project settings. A message at the bottom states 'You're in a team-managed project'.

The screenshot shows a Jira project board for 'Investigación Seguridad en Redes WiFi'. The board is divided into three columns: 'TO DO', 'IN PROGRESS', and 'DONE'. The 'TO DO' column contains six items: 'Identificación de los principales puntos tratados' (SRW-26), 'Metodología de Trabajo' (SRW-27), 'Detalles del plan de trabajo' (SRW-28), 'Mapeo de la bibliografía y su relevancia' (SRW-29), 'Planificación del proyecto' (SRW-30), and 'Detalles del plan de trabajo, ...' (SRW-31). The 'IN PROGRESS' column contains four items: 'Redactar Contexto académico' (SRW-20), 'Análisis de los temas investigados' (SRW-24), 'Redactar Equipo de trabajo y referencia CAETI' (SRW-22), and 'Área de Investigación' (SRW-23). The 'DONE' column contains one item: 'Organizar Próxima Entrega' (SRW-19). A search bar at the top right shows 'JP VT'. The left sidebar includes sections for PLANNING (Timeline, Backlog, Board, Calendar, List, Goals, Issues, Add view), DEVELOPMENT (Code, Project pages, Add shortcut, Project settings), and a general section for Project pages, Add shortcut, and Project settings.

Sprint 4: Resumen y Metodología de Trabajo

- Objetivo: Resumir cada sección del trabajo de investigación y documentar la metodología utilizada.
- Tareas:
 - Dividir el trabajo para la sección de resumen y metodología.
 - Identificar y resumir los principales puntos de cada sección.
 - Describir el enfoque metodológico (cuantitativo, cualitativo, mixto).
 - Detallar el plan de trabajo y cronograma.
 - Registrar cambios en el plan de trabajo.
 - Mapear y analizar la bibliografía relevante.
 - Volcar y corregir la información en el documento.

The screenshot shows the Jira software interface for a project titled "Investigacion Seguridad en Redes WiFi". The main view is a Kanban board for "SOF Sprint 4".

Left Sidebar:

- Projects: Investigacion Seguridad en Redes WiFi (Software project)
- PLANNING:
 - Timeline
 - Backlog
 - Board** (selected)
 - Calendar (NEW)
 - List
 - Goals
 - Issues
 - + Add view
- DEVELOPMENT:
 - Code
- Project pages
- Add shortcut
- Project settings

Top Bar:

- Jira
- Your work
- Projects
- Filters
- Dashboards
- Teams
- Plans
- Apps
- Create

Board View:

The board has three columns: TO DO, IN PROGRESS, and DONE.

- TO DO:** Contains one item: "Redaccion en Conjunto" (SRW-32).
- IN PROGRESS:** Contains six items:
 - "Identificación de los principales puntos tratados" (SRW-26) assigned to VT.
 - "Metodología de Trabajo" (SRW-27) assigned to JP.
 - "Detalles del plan de trabajo" (SRW-28) assigned to VT.
 - "Detalles del plan de trabajo," (SRW-31) assigned to JP.
 - "Mapeo de la bibliografía y su relevancia" (SRW-29) assigned to JP.
 - "Planificación del proyecto" (SRW-30) assigned to VT.
- DONE:** Contains one item: "+ Create issue".

The screenshot shows a Jira project board for 'Investigacion Seguridad en Redes WiFi'. The board is titled 'SOF Sprint 4'. It has three main columns: 'TO DO', 'IN PROGRESS 1', and 'DONE 6'. The 'TO DO' column contains a '+ Create issue' button. The 'IN PROGRESS 1' column contains a task titled 'Redaccion en Conjunto' with a sub-task 'SRW-32'. The 'DONE 6' column lists several completed tasks: 'Detalles del plan de trabajo', 'Planificación del proyecto', 'Mapeo de la bibliografía y su relevancia', 'Identificación de los principales puntos tratados', 'Detalles del plan de trabajo', and 'Metodología de Trabajo'. Each task is associated with a user icon (JP or VT) and a green checkmark.

Sprint 5: Áreas de Investigación

- Objetivo: Resumir cada sección del trabajo de investigación y documentar la metodología utilizada.
- Tareas:
 - Prevención y Detección de intrusos.
 - Realizar maquina PRETORIAN
 - Análisis de tráfico
 - Honeyports, Proxy Server y Firewalls
 - Tipo de Intrusiones
 - Firmware y SSID
 - Redacción Final

Imagen de JIRA:

The screenshot shows the JIRA interface for a project titled "Investigacion Seguridad en Redes WiFi" under "SOF Sprint 5". The left sidebar includes options like Planning, Backlog, Board (which is selected), Calendar, List, Goals, Issues, Add view, Development, Code, Project pages, Add shortcut, and Project settings. The main board view has three columns: TO DO, IN PROGRESS 6, and DONE. The IN PROGRESS 6 column lists six issues with their respective assignees (JP, VT, and others) and descriptions.

Column	Issue Key	Description	Assignee
TO DO		+ Create issue	
IN PROGRESS 6	SRW-32	Redaccion en Conjunto	JP
IN PROGRESS 6	SRW-37	Analisis de Trafico y Modificacion de SSID	JP
IN PROGRESS 6	SRW-35	Pretorian	VT
IN PROGRESS 6	SRW-34	Intrusion detection/prevention	JP
IN PROGRESS 6	SRW-33	Refinar area de investigacion	VT
IN PROGRESS 6	SRW-36	Honeypots / Proxy / Firewalls	VT
DONE			

The screenshot shows a Jira project titled "Investigacion Seguridad en Redes WiFi" under the "SOF Sprint 5" iteration. The left sidebar contains navigation links for planning, backlog, calendar, lists, goals, issues, and project pages. The main board has three columns: "TO DO", "IN PROGRESS", and "DONE". The "DONE" column is highlighted with a green border and contains the following tasks:

- Redaccion en Conjunto (SRW-32)
- Pretorian (SRW-35)
- Honeypots / Proxy / Firewalls (SRW-36)
- Refinar area de investigacion (SRW-33)
- Intrusion detection/prevention (SRW-34)
- Analisis de Trafico y Modificacion de SSID (SRW-37)

Each task row includes a green checkmark and initials (JP, VT) next to the issue number.

6.3. Conclusion

El uso de Scrum y JIRA nos ha permitido llevar un control detallado y eficiente del proceso de documentación. Hasta ahora, hemos completado cinco sprints que nos han permitido establecer una sólida estructura inicial, desarrollar la sección del estado del arte, contexto, área de investigación y metodología de trabajo. Semana a semana, avanzamos de manera organizada, asegurando que cada aspecto del documento sea abordado de manera correcta. Adicionalmente, la documentación detallada de nuestro trabajo no solo sirve como respaldo de nuestro proceso, sino también como un recurso valioso para futuros proyectos y publicaciones.

7. Sección Práctica

7.1. Montaje Gladiator

Gladiator fue concebido como un sistema operativo enfocado en la defensa y monitoreo de redes. Con este fin, hemos utilizado una distribución de Kali Linux y, sobre ella, hemos integrado herramientas importantes y destacadas para auditar y monitorear las redes a las que el sistema operativo esté conectado. El propósito de Gladiator es proporcionar una plataforma robusta y eficiente para la gestión de la seguridad de la red, permitiendo a los administradores de sistemas detectar, analizar y mitigar amenazas de manera efectiva.

7.1.1. Instalacion y Configuracion

Preparación del Entorno Para comenzar, descargamos la imagen de Kali Linux y la instalamos en una máquina virtual utilizando Oracle Virtual Box. La elección de Kali Linux se debió a su reputación y capacidades como una distribución especializada en seguridad, equipada con numerosas herramientas preinstaladas para pruebas de penetración y análisis de seguridad.

Configuración de la Máquina Virtual Configuramos la máquina virtual con las siguientes especificaciones:

- Procesador: 6 núcleos
- Memoria RAM: 8 GB
- Disco Duro: 50 GB
- Red: Modo puente para permitir el acceso directo a la red local

Instalación de Kali Linux Procedimos a la instalación de Kali Linux en la máquina virtual, siguiendo los pasos estándar proporcionados por el instalador.

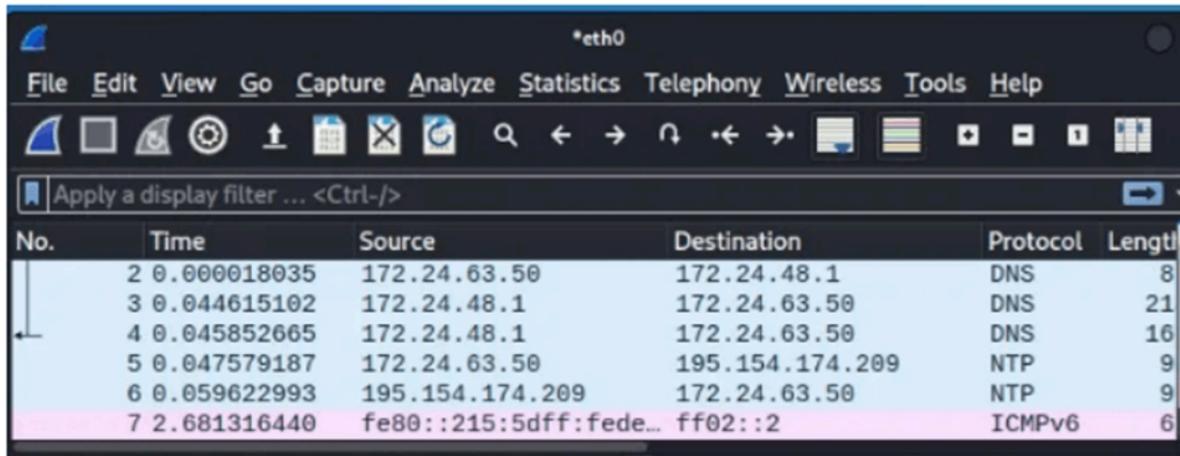
7.1.2. Integración de Herramientas

Después de la instalación de Kali Linux, pasamos a integrar herramientas adicionales y configurar las que ya estaban incluidas para personalizar Gladiator según nuestras necesidades de seguridad y monitoreo de red. A continuación, se detalla la integración de cada herramienta:

Wireshark

Wireshark es una herramienta de análisis de paquetes de red que permite capturar y analizar el tráfico de red en tiempo real. Es una de las herramientas más utilizadas por los profesionales de seguridad para la inspección profunda de paquetes y la detección de anomalías.

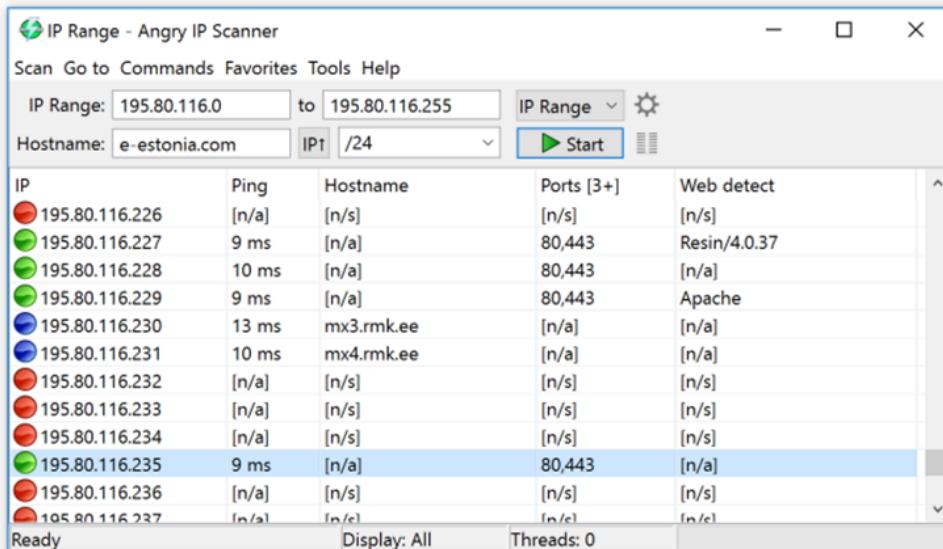
Utilización: Wireshark fue empleado para capturar y analizar el tráfico de red, identificar patrones anómalos y detectar posibles ataques de sniffing y spoofing. La capacidad de Wireshark para desglosar los paquetes de datos y proporcionar información detallada sobre el tráfico de red fue fundamental.



Angry IP Scanner

Angry IP Scanner es una herramienta de código abierto que permite escanear direcciones IP y puertos en una red de manera rápida y sencilla. Es útil para descubrir dispositivos activos y puertos abiertos, proporcionando una visión general del estado de la red.

Utilización: Utilizamos Angry IP Scanner para identificar dispositivos conectados a la red y verificar la configuración de puertos. Esta herramienta nos ayudó a detectar dispositivos no autorizados y posibles puntos de vulnerabilidad.



Netdiscover

Netdiscover es una herramienta de descubrimiento de red que permite identificar dispositivos conectados en una red local. Es particularmente útil en entornos donde no se dispone de un servidor DHCP y se requiere un escaneo pasivo.

Utilización: Netdiscover fue empleado para mapear la topología de la red y encontrar dispositivos activos mediante el análisis de paquetes ARP. Esta herramienta complementó nuestros esfuerzos de mapeo de red y detección de intrusiones.

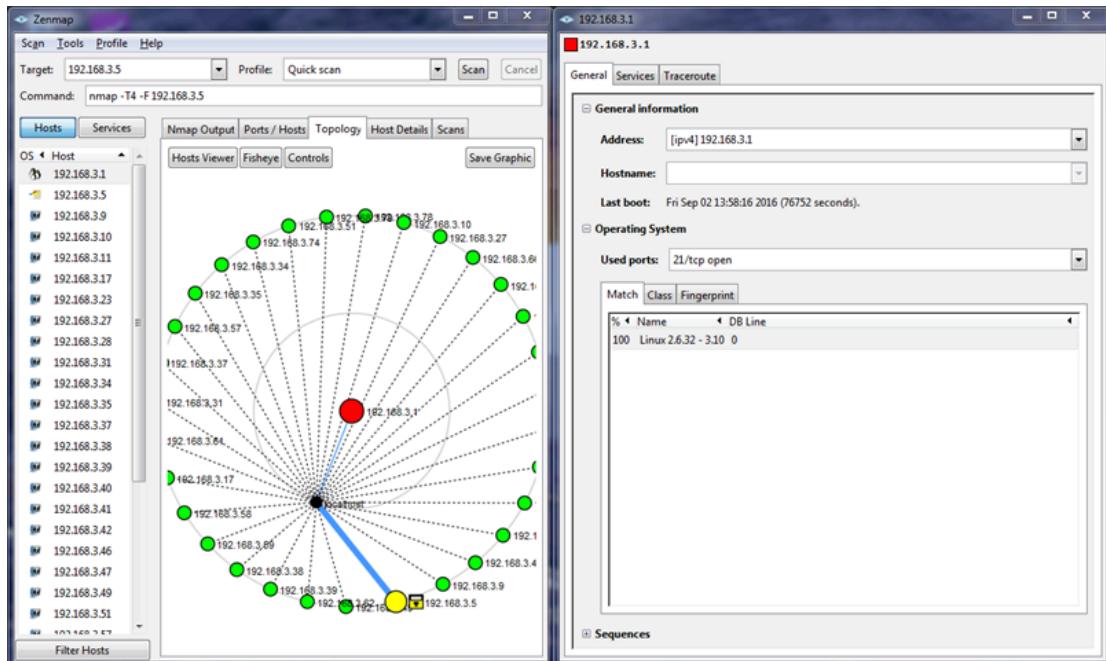
```
File Edit View Search Terminal Help
Currently scanning: Finished! | Screen View: Unique Hosts
folders.sh
19 Captured ARP Req/Rep packets, from 16 hosts. Total size: 1140

IP          At MAC Address      Count    Len   MAC Vendor / Hostname
-----+-----+-----+-----+-----+-----+-----+
10.128.128.128 88:15:44:aa:4b:18 1        60   Meraki, Inc.
192.168.33.3   3c:15:c2:dc:02:b4 3        180  Apple, Inc.
192.168.33.1   e0:55:3d:77:04:b5 2        120  Cisco Meraki
192.168.33.2   88:15:44:e3:a1:00 1        60   Meraki, Inc.
192.168.33.4   88:15:44:aa:4b:18 1        60   Meraki, Inc.
192.168.33.21  8c:7c:92:3b:83:63 1        60   Apple, Inc.
192.168.33.14  e4:c7:22:9a:a2:b4 1        60   Cisco Systems, Inc
192.168.33.20  e0:55:3d:83:0a:23 1        60   Cisco Meraki
192.168.33.16  00:11:d9:40:c7:36 1        60   TiVo
192.168.33.17  00:11:d9:3d:c6:c1 1        60   TiVo
192.168.33.24  e0:55:3d:84:a6:84 1        60   Cisco Meraki
192.168.33.12  f0:d1:a9:20:74:c7 1        60   Apple, Inc.
192.168.33.123 b8:27:eb:6a:35:5f 1        60   Raspberry Pi Foundation
192.168.33.210 00:80:77:d5:f6:ea 1        60   Brother industries, LTD.
192.168.33.7   cc:20:e8:10:cd:55 1        60   Apple, Inc.
192.168.33.18  cc:29:f5:49:e1:87 1        60   Apple, Inc.
```

Zenmap

Zenmap es la interfaz gráfica de usuario (GUI) para Nmap, una de las herramientas de escaneo de red más potentes y versátiles disponibles. Zenmap facilita la realización de escaneos complejos y la visualización de los resultados.

Utilización: Utilizamos Zenmap para realizar escaneos de puertos, detección de servicios y sistemas operativos. Los resultados obtenidos con Zenmap fueron cruciales para evaluar la seguridad de la red y descubrir posibles vectores de ataque.



7.2. Demostraciones Prácticas

Escenario 1: Detección de Dispositivos no Autorizados con Angry IP Scanner

- **Objetivo:** Identificar dispositivos no autorizados en la red.
- **Proceso:** Ejecutamos Angry IP Scanner para escanear el rango de IPs de la red local.
- **Resultados:** Los resultados mostraron varios dispositivos activos, identificando aquellos que no deberían estar presentes.

Escenario 2: Análisis de Tráfico con Wireshark

- **Objetivo:** Capturar y analizar el tráfico de red en tiempo real.
- **Proceso:** Configuramos Wireshark para capturar todo el tráfico en la red local, aplicando filtros como dns para enfocarnos en tráfico sospechoso.
- **Resultados:** Detectamos patrones de tráfico inusual que indicaban posibles intentos de sniffing y spoofing.

Escenario 3: Escaneo y Detección de Servicios con Zenmap

- **Objetivo:** Realizar un escaneo de red para detectar servicios y sistemas operativos activos.
- **Proceso:** Utilizamos Zenmap para ejecutar escaneos detallados en la red local.
- **Resultados:** Los resultados proporcionaron una lista completa de puertos abiertos, servicios activos y sistemas operativos detectados.

Escenario 4: Mapeo de la Red con Netdiscover

- **Objetivo:** Mapear la topología de la red y descubrir dispositivos activos.
- **Proceso:** Ejecutamos Netdiscover en modo pasivo para detectar dispositivos mediante el análisis de paquetes ARP.
- **Resultados:** Netdiscover proporcionó un mapa detallado de la red, mostrando todos los dispositivos conectados y sus direcciones MAC.

7.3. Objetivos de Gladiator

La integración de estas herramientas en Gladiator nos permitió crear un entorno de monitoreo y defensa de red altamente efectivo. Los beneficios principales incluyen:

- ❖ Visibilidad Completa de la Red: La combinación de herramientas como Wireshark y Netdiscover proporcionó una visión integral de todos los dispositivos y tráfico en la red.
- ❖ Detección Temprana de Amenazas: Herramientas como Zenmap y Angry IP Scanner ayudaron a identificar y responder a posibles amenazas antes de que pudieran causar daños significativos.
- ❖ Evaluación Continua de Seguridad: AirCrack-ng y otras herramientas permitieron realizar auditorías de seguridad regulares, asegurando que las redes WiFi mantuvieran configuraciones de seguridad robustas.
- ❖ Flexibilidad y Personalización: La naturaleza abierta y flexible de Kali Linux permite personalizar Gladiator para satisfacer necesidades específicas de seguridad y monitoreo.

7.4. Conclusion

El montaje y configuración de Gladiator demostraron ser una solución efectiva para la defensa y monitoreo de redes. La combinación de herramientas potentes y la flexibilidad de Kali Linux proporcionaron una plataforma sólida para la gestión de la seguridad de la red. A través de nuestras demostraciones prácticas, pudimos identificar y mitigar varias vulnerabilidades, mejorando significativamente la seguridad de las redes auditadas.

Las experiencias y resultados obtenidos subrayan la importancia de utilizar una combinación de herramientas y técnicas para proteger las redes de manera integral. Gladiator, como sistema operativo enfocado en la seguridad, ofrece una solución eficiente y adaptable para enfrentar los desafíos de seguridad en redes modernas.

8. Resultados

8.1. Presentación de Hallazgos

A lo largo de nuestra investigación, hemos identificado una serie de resultados significativos que subrayan tanto las vulnerabilidades como las posibles medidas de defensa en el ámbito de la seguridad de redes. Nuestra exploración abarcó diversas áreas, desde la seguridad en redes WiFi y la identificación de intrusiones hasta el uso de herramientas de análisis de red y la implementación de medidas preventivas en routers.

8.2. Seguridad de Redes Wifi

Uno de los primeros hallazgos relevantes es la identificación de las principales amenazas a la seguridad en redes wireless. Se constató que, a pesar de los avances en tecnologías de cifrado, las redes WiFi siguen siendo vulnerables a diversos tipos de ataques, incluyendo la interceptación de datos y el acceso no autorizado. Las redes que utilizan cifrados antiguos como WEP son particularmente vulnerables, ya que pueden ser comprometidas en cuestión de minutos mediante técnicas de fuerza bruta y ataques de diccionario.

Se observó que el uso de contraseñas débiles o predecibles sigue siendo un problema común, facilitando los ataques de fuerza bruta. La implementación de contraseñas complejas y el uso de métodos de autenticación más robustos, como WPA3, han demostrado ser efectivos en mitigar estas vulnerabilidades. Sin embargo, el despliegue de WPA3 aún no es generalizado, lo que deja a muchas redes expuestas.

8.3. Tipos de Intrusiones

Nuestro análisis reveló que los ataques de spoofing y sniffing son dos de los métodos más comunes empleados por los atacantes para comprometer redes. El spoofing permite a los atacantes hacerse pasar por un dispositivo legítimo dentro de la red, mientras que el sniffing implica la interceptación de tráfico de red para recopilar información sensible.



Estos ataques pueden llevarse a cabo mediante el uso de herramientas especializadas y son particularmente efectivos en redes que no utilizan cifrado o que emplean cifrado débil. La detección y mitigación de estos ataques requieren la implementación de sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) que monitorean continuamente el tráfico de red en busca de patrones sospechosos.

8.4. Señales de Ingreso no Deseados

Se identificaron varios indicadores clave de ingreso no deseado en una red, como aumentos repentinos en el tráfico de red, conexiones a direcciones IP desconocidas, y la presencia de dispositivos no autorizados. Estos indicadores son esenciales para la detección temprana de intrusiones y la respuesta rápida a incidentes de seguridad.

La implementación de soluciones de monitoreo de red y la capacitación del personal para reconocer estos signos son fundamentales para mejorar la seguridad de la red.

8.5. Implementación y Funcionamiento de los Honeypots

La implementación de honeypots proporcionó información valiosa sobre las tácticas y objetivos de los atacantes. Los honeypots de alta interacción, que simulan sistemas reales con múltiples servicios vulnerables, permitieron capturar datos detallados sobre los métodos de ataque utilizados. Esto incluye la identificación de técnicas de explotación de vulnerabilidades.



8.6. Herramientas de Análisis de Red

El uso de herramientas de análisis de red como Wireshark, Netcut, AirCrack, NMap, e iptables ha demostrado ser fundamental para la identificación y mitigación de vulnerabilidades en la red. Cada una de estas herramientas proporciona capacidades únicas para la inspección y el análisis de tráfico de red.

- **Wireshark:** Esta herramienta permite la captura y el análisis detallado de paquetes de datos, lo que facilita la identificación de tráfico anómalo y la resolución de problemas de red.
- **Netcut:** Utilizada principalmente para controlar y gestionar dispositivos conectados a una red, Netcut puede identificar dispositivos no autorizados y ayudar en la prevención de intrusiones.
- **AirCrack:** Especializada en la auditoría de seguridad de redes WiFi, AirCrack puede descifrar claves WEP y WPA, destacando la importancia de utilizar cifrados más robustos.
- **NMap:** Esta herramienta de escaneo de red es fundamental para mapear redes, identificar dispositivos y descubrir puertos abiertos, lo que es crucial para la evaluación de la seguridad de la red.
- **iptables:** Utilizado para configurar reglas de firewall en sistemas Linux, iptables permite a los administradores de red controlar el tráfico entrante y saliente, protegiendo la red contra accesos no autorizados.

Wireless Summary View				
Group by:	Access Point	IP Address	Type	SSIDs
Location	OMSEAAP102	10.199.17.89	Thin	6, 44
[Unknown] (1)	OMSEAAP502	10.199.17.88	Thin	6, 44
Cairo (6)	zT363 - 06C4011	10.199.17.90	Thin	1, 132
Indianapolis, IN (12)	zT363 - 06C4011	10.199.17.91	Thin	10, 132
L30 (1)				
Seattle - 201 5th (14)				
Sydney (8)				
Texas (8)				
Tokyo (11)				
	Client Name	SSID	IP Address	MAC Address
	vprice	lab	10.199.17.184	C4017C057620
	mprice	lab	10.199.17.19	001B207F5216
	zT363 - 06C4011	10.199.17.92	Thin	6, 161
	zT363 - 06C4011	10.199.17.93	Thin	4, 48
	zT363 - 06C4011	10.199.17.94	Thin	3, 56
	zT363 - 06C4011	10.199.17.95	Thin	9, 44
	zT363 - 06C4011	10.199.17.96	Thin	2, 104
	zT363 - 06C4011	10.199.17.97	Thin	4, 153
	zT363 - 06C410E	10.199.17.98	Thin	11, 64
	zT363 - 06C410E	10.199.17.99	Thin	4, 56
	zT363 - 06C410E	10.199.17.100	Thin	3, 44
	zT363 - 06C410E	10.199.17.101	Thin lab	44

8.7. Medidas Preventivas en Enrutadores

Las medidas preventivas implementadas en enrutadores son cruciales para la protección de redes domésticas y empresariales. Nuestra investigación destacó varias prácticas recomendadas para mejorar la seguridad de los enrutadores:

- **Desvinculación de IP de Administración:** Cambiar la IP de administración predeterminada del enrutador para dificultar su acceso por parte de atacantes.
- **Modificación de SSID y Contraseñas:** Cambiar el nombre de la red (SSID) y las contraseñas predeterminadas para evitar accesos no autorizados.
- **Encriptación y Cifrado WiFi:** Utilizar cifrados robustos como WPA3 para proteger la comunicación inalámbrica.
- **Actualización de Firmware del Enrutador:** Mantener el firmware del enrutador actualizado para protegerse contra vulnerabilidades conocidas.
- **Randomización de Canal de Transmisión:** Cambiar periódicamente el canal de transmisión para evitar interferencias y mejorar la seguridad.
- **Habilitación de Multibanda:** Utilizar bandas de frecuencia múltiples para mejorar el rendimiento y la seguridad de la red.
- **Filtrado por Dirección MAC:** Restringir el acceso a la red mediante el filtrado de direcciones MAC, permitiendo solo dispositivos autorizados.
- **Reducción de Rangos de Direcciones IP Permitidas:** Limitar el rango de direcciones IP asignadas por el enrutador para reducir la superficie de ataque.
- **Desactivación de Administración Remota y PnP:** Desactivar características innecesarias como la administración remota y Plug and Play (PnP) para reducir los vectores de ataque.



8.8. Network Security Monitoring (NSM)

El monitoreo de la seguridad de la red (NSM) es una estrategia esencial para la detección y respuesta a incidentes de seguridad. NSM implica la recopilación, análisis y correlación de datos de red para identificar patrones de comportamiento anómalos y actividades sospechosas.

Nuestra investigación destacó la importancia de implementar soluciones NSM que proporcionen visibilidad completa del tráfico de red, permitiendo la detección temprana de intrusiones. Herramientas como Zeek (anteriormente conocido como Bro) y Security Onion han demostrado ser eficaces en la implementación de NSM, proporcionando capacidades avanzadas de análisis y monitoreo.

El uso de NSM permite a los administradores de red identificar rápidamente las amenazas, correlacionar eventos de seguridad y tomar medidas preventivas antes de que los ataques puedan causar daños significativos. La integración de NSM con otras herramientas de seguridad, como IDS/IPS y firewalls, crea un entorno de seguridad más efectivo.

8.9. Proxy Servers y sus tipos

La investigación también abarcó la evaluación de los servidores proxy y sus diferentes tipos, cada uno con sus propias aplicaciones y ventajas:

- **Proxy HTTP**
- **Proxy Transparente**
- **Proxy Inverso**
- **Proxy SOCKS**: Permite una mayor flexibilidad al manejar diferentes tipos de tráfico, no solo HTTP, y es útil para aplicaciones que requieren acceso a diferentes tipos de servicios de red.

8.10. Firewalls

El análisis de los firewalls físicos y los basados en inteligencia artificial destacó sus respectivas ventajas y aplicaciones en la protección de redes:

- **Firewalls Físicos**
- **Firewalls Basados en Inteligencia Artificial**

La combinación de medidas preventivas, el uso de herramientas avanzadas de análisis y monitoreo, y la implementación de soluciones de seguridad basadas en inteligencia artificial, proporciona una defensa integral contra las amenazas a la seguridad de redes y WiFi.

9. Conclusiones

9.1. Reflexion

Al concluir esta investigación, es importante reflexionar sobre el proceso y los resultados obtenidos, así como sobre las lecciones aprendidas y las implicaciones de nuestros hallazgos. Este estudio ha sido una experiencia enriquecedora que nos ha permitido profundizar en el campo de la seguridad de redes, y ha subrayado la importancia de la continua evolución y adaptación en este ámbito.

Desde el inicio, nuestra meta fue identificar las vulnerabilidades más críticas en las redes WiFi y explorar las herramientas y técnicas más efectivas para mitigarlas. La recopilación y análisis de datos, la implementación de pruebas de seguridad, y la evaluación de diversas herramientas de análisis de red, nos han proporcionado una comprensión más profunda de los desafíos que enfrentan tanto los usuarios domésticos como las empresas en la protección de sus redes.

El proceso de investigación no estuvo exento de desafíos. La rápida evolución de las tecnologías de ataque y defensa requiere una constante actualización de conocimientos y habilidades. Nos encontramos con que muchos de los ataques que considerábamos sofisticados hace apenas unos años, ahora pueden ser ejecutados con relativa facilidad debido a la disponibilidad de herramientas avanzadas y tutoriales en línea. Esto subraya la necesidad de una educación continua y una adaptación constante a nuevas amenazas.

Trabajar en este proyecto también nos ha enseñado la importancia de la colaboración y la comunicación efectiva. La coordinación entre los miembros del equipo y la integración de diferentes perspectivas y habilidades fueron cruciales para el éxito del proyecto. Cada miembro aportó su experiencia en áreas específicas, desde la configuración y análisis de redes hasta la

implementación de medidas de seguridad y la interpretación de datos. Esta sinergia nos permitió abordar el problema desde múltiples ángulos y desarrollar soluciones más robustas y completas.

El desarrollo final, si bien complejo para nuestra experiencia y conocimientos, es apenas la punta del iceberg para encontrar una resolución a uno de los problemas más complicados y difíciles de la ciberseguridad actual: la protección y monitoreo de redes.

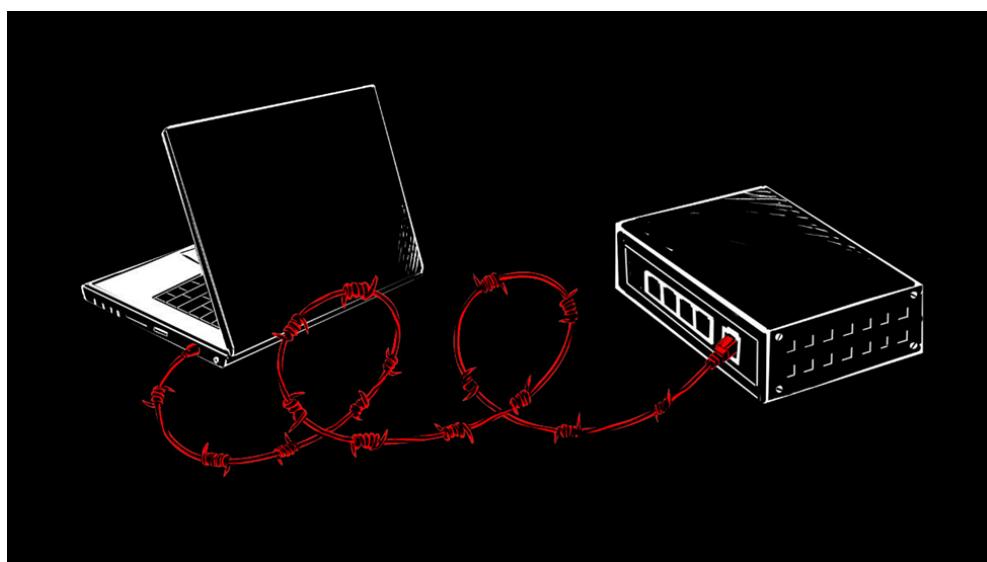
9.2. Recomendaciones para Futuras Investigaciones

Basándonos en los hallazgos de nuestra investigación, presentamos las siguientes recomendaciones para futuras investigaciones y aplicaciones prácticas en el campo:

1. **Investigación Continua en Nuevas Amenazas:** La rápida evolución de las tecnologías de ataque requiere una investigación continua para identificar nuevas amenazas y desarrollar contramedidas efectivas.
2. **Desarrollo de Herramientas de Seguridad Avanzadas:** Es crucial continuar desarrollando y mejorando herramientas de seguridad que puedan detectar y mitigar amenazas de manera más efectiva.
3. **Capacitación y Educación Continua:** La capacitación constante de los profesionales de TI y la educación de los usuarios finales sobre las mejores prácticas de seguridad son esenciales para mantener la seguridad de las redes.
4. **Promoción del Uso de Cifrados Modernos:** Fomentar el uso de cifrados modernos como WPA3 en lugar de cifrados obsoletos como WEP. Las campañas de concienciación y los incentivos pueden ayudar a acelerar la adopción de estas tecnologías más seguras.
5. **Desarrollo de Normativas y Estándares de Seguridad:** La creación y promoción de normativas y estándares de seguridad específicos para redes WiFi pueden ayudar a garantizar un nivel básico de protección en todas las implementaciones, por ejemplo a través de las normas ISO.
6. **Investigación sobre el Impacto de IoT en la Seguridad de Redes:** Con el aumento de dispositivos IoT conectados a redes WiFi, es esencial investigar y desarrollar soluciones específicas para proteger estos dispositivos y prevenir que se conviertan en puntos de entrada para atacantes.
7. **Fomento de la Colaboración entre Industria y Academia:** La colaboración entre la industria y la academia puede acelerar el desarrollo de nuevas tecnologías y soluciones de seguridad. Proyectos conjuntos y la compartición de información pueden conducir a avances significativos en la protección de redes.

8. **Desarrollo de Estrategias de Respuesta a Incidentes:** La creación de planes y equipos de respuesta a incidentes es crucial para minimizar el impacto de los ataques cuando ocurren.
9. **Fomento del Uso de Redes Segmentadas:** La segmentación de redes puede limitar la propagación de ataques y contener posibles brechas. La implementación de redes segmentadas y el uso de VLANs pueden mejorar la seguridad al aislar diferentes partes de la red.
10. **Integración de Soluciones de Seguridad en el Proceso de Desarrollo:** La seguridad debe integrarse en el proceso de desarrollo de software y hardware desde el principio. El uso de DevSecOps y la implementación de revisiones de seguridad en todas las etapas del desarrollo es fundamental.
11. **Evaluación del Impacto de la Inteligencia Artificial en la Seguridad de Redes:** La inteligencia artificial tiene el potencial de revolucionar la seguridad de redes, pero también puede ser utilizada por atacantes para desarrollar nuevos tipos de ataques. Es esencial evaluar el impacto de la inteligencia artificial y desarrollar estrategias para mitigar sus riesgos.

En conclusión, la seguridad de redes y WiFi es un campo dinámico y en constante evolución que requiere una combinación de medidas preventivas, herramientas avanzadas de análisis y monitoreo, y una continua adaptación a nuevas amenazas. Las recomendaciones presentadas proporcionan una guía para futuras investigaciones y aplicaciones prácticas que pueden ayudar a mejorar la seguridad de las redes y proteger contra una amplia gama de amenazas. La colaboración, la educación y el desarrollo continuo de tecnologías de seguridad son esenciales para enfrentar los desafíos de seguridad actuales y futuros.



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-intuitive-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 Católica.
- [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.