

Implementación de un Sistema de Aislamiento de Dispositivos mediante la Integración de Tecnologías de Monitoreo y Respuesta a Incidentes

María Lucía Orozco Guerra

Documento presentado como requisito parcial para optar al título de Ingeniera de Telecomunicaciones

Modalidad de Práctica

Semestre de Industria

Asesor:

Sergio Armando Gutiérrez Betancur,Ph.D.

Universidad de Antioquia

Facultad de Ingeniería

Ingeniería de Telecomunicaciones

Medellín

2025

Cita	(Orozco & Gutiérrez, 2025)
Referencia **Estilo APA 7 (2020)**	Orozco,M & Gutiérrez,S. (2025). *Implementación de un Sistema de Aislamiento de Dispositivos mediante la Integración de Tecnologías de Monitoreo y Respuesta a Incidente* [Semestre de Industria]. Universidad de Antioquia, Medellín.

creative commons CC BY NC SA

UNIVERSIDAD DE ANTIOQUIA
Vicerrectoría de Docencia

Sistema de Bibliotecas

Centro de Documentación Ingeniería (CENDOI)

Repositorio Institucional: http://bibliotecadigital.udea.edu.co

Universidad de Antioquia - www.udea.edu.co

El contenido de esta obra corresponde al derecho de expresión de los autores y no compromete el pensamiento institucional de la Universidad de Antioquia ni desata su responsabilidad frente a terceros. Los autores asumen la responsabilidad por los derechos de autor y conexos.

Dedicatoria

Dedico este proyecto a mi familia, en especial a mis padres, cuya presencia ha sido parte de mi camino y de mi crecimiento personal. A mi novio, quien ha sido mi mayor apoyo, brindándome su compañía, paciencia y confianza en cada desafío. Gracias por estar siempre a mi lado, impulsándome a seguir adelante.Y, sobre todo, a mí misma, por la dedicación, el esfuerzo y la determinación que me han permitido llegar hasta aquí. Por no rendirme ante las dificultades demostrarme que soy capaz de alcanzar mis metas.

Agradecimientos

Agradezco a mi familia por haber formado parte de este proceso y a mis padres por estar presentes en este camino. A mi novio, por su paciencia, apoyo constante y por acompañarme en cada desafío con motivación y confianza en mis capacidades.

A mis amigos, por su compañía y palabras de aliento. A mis profesores y mentores, por compartir su conocimiento y contribuir a mi crecimiento profesional. A Aligo Defensores Informáticos, por brindarme la oportunidad de realizar mis prácticas y permitirme aplicar lo aprendido en un entorno real.

Tabla de contenido

Resumen..... 7
Abstract.....9
1. Introducción.....9
2. Objetivos.....11
    2.1 Objetivo general.....11
    2.2 Objetivos específicos..... 11
3. Marco teórico.....11
4. Metodología.....15
5. Análisis de resultados..... 15
    Escaneo de vulnerabilidades:.....17
6. Conclusiones y recomendaciones.....29
Referencias..... 29

Lista de figuras

Figura 1 . Flujo general del proyecto 13
Figura 2. Packetfence Aligo 15
Figura 3. Arquitectura de red Aligo 15
Figura 4. Distribución de dispositivos por tipo de conexión 16
Figura 5. Escaneo en Nessus de Switch 192.168.4.20 17
Figura 6. Escaneo en Nessus de Switch 192.168.4.22 18
Figura 7. Escaneo en Nessus de Switch 192.168.4.26 20
Figura 8. Escaneo en Nessus de Switch 192.168.4.27 22
Figura 9. Regla Suricata 24
Figura 10. Regla Suricata guardada 24
Figura 11. Regla YARA 25
Figura 12. Regla YARA ransomware YMIR 26
Figura 13. Creación regla de aislamiento en Packetfence 27
Figura 14. Aislamiento en Packetfence 27

Resumen

Este proyecto presenta el desarrollo e implementación de un sistema automatizado de detección y respuesta a incidentes de seguridad cibernética, con un enfoque en la creación de reglas personalizadas para la identificación de amenazas. La solución integra un Sistema de Detección de Intrusiones (IDS) y un sistema de Control de Acceso a la Red (NAC), permitiendo la detección proactiva de patrones maliciosos en el tráfico de red y en archivos analizados dentro del entorno de la organización.

Con el objetivo de detectar y mitigar amenazas de seguridad, se diseñaron y configuraron reglas de detección específicas que permiten identificar comportamientos anómalos asociados a ciberataques, tales como la descarga de archivos maliciosos o la ejecución de comandos sospechosos. Con base en los eventos detectados mediante estas reglas, se establecieron mecanismos de respuesta automática, incluyendo el aislamiento de dispositivos comprometidos a través del NAC, con el fin de mitigar riesgos y evitar la propagación de amenazas en la red. La evaluación del sistema demostró la eficacia de estas reglas personalizadas en la detección temprana de incidentes, reduciendo significativamente el tiempo de respuesta y mejorando la seguridad de un entorno empresarial. Como resultado, se concluye que la integración de reglas de detección avanzadas con sistemas IDS y NAC proporciona una solución eficiente, escalable y replicable para fortalecer la seguridad de redes empresariales, mejorando la capacidad de respuesta y optimizando la detección, análisis y mitigación de incidentes, minimizando así el impacto de ataques cibernéticos..

Palabras clave: Ciberseguridad, Sistema de Detección de Intrusos (IDS), Control de Acceso a la Red (NAC), Detección de amenazas, Respuesta a incidentes

Abstract

This project presents the development and implementation of an automated system for detecting and responding to cybersecurity incidents, with a focus on creating custom rules for threat identification. The solution integrates an Intrusion Detection System (IDS) and a Network Access Control (NAC) system, enabling proactive detection of malicious patterns in network traffic and files analyzed within the organization's environment.

To detect and mitigate security threats, specific detection rules were designed and configured to identify anomalous behaviors associated with cyberattacks, such as the download of malicious files or the execution of suspicious commands. Based on the events detected through these rules, automatic response mechanisms were established, including the isolation of compromised devices through NAC, in order to mitigate risks and prevent the spread of threats across the network.

The system evaluation demonstrated the effectiveness of these custom rules in the early detection of incidents, significantly reducing response time and enhancing the security of an enterprise environment. As a result, we conclude that the integration of advanced detection rules with IDS and NAC systems provides an efficient, scalable, and replicable solution to strengthen enterprise network security, improving response capabilities and optimizing the detection, analysis, and mitigation of incidents, thereby minimizing the impact of cyberattacks.

Keywords: Cybersecurity, Intrusion Detection System (IDS), Network Access Control (NAC), Threat detection, Incident response

1. Introducción

En el contexto actual de amenazas cibernéticas cada vez más sofisticadas (Symantec, 2024), la protección de las redes empresariales se ha convertido en una prioridad. Las organizaciones necesitan soluciones integradas que no sólo identifiquen intrusiones, sino que también respondan rápidamente a estas (Muhammad, Munir, Munir & Zafar, 2022). La implementación de tecnologías de monitoreo y respuesta ante incidentes es crucial para minimizar riesgos y garantizar la seguridad de los sistemas críticos (Lindemulder & Kosinski, 2024).

Este proyecto tiene como objetivo desarrollar un sistema para la detección y respuesta eficiente ante amenazas, mediante la identificación de patrones maliciosos en el tráfico de red, archivos y procesos a nivel de sistema operativo. La solución propuesta integra mecanismos automatizados que no solo generan alertas sobre actividades sospechosas, sino que también habilitan una respuesta inmediata mediante el aislamiento de dispositivos comprometidos, optimizando así la capacidad de detección y respuesta ante amenazas, y reduciendo el impacto de posibles incidentes..

En el marco de este proyecto, la implementación de estos mecanismos automatizados se lleva a cabo en Aligo Defensores Informáticos S.A.S., una empresa dedicada a la ciberseguridad y a la protección de infraestructuras tecnológicas críticas. La adopción de un sistema de aislamiento de dispositivos no solo fortalecerá su capacidad de respuesta ante incidentes, sino que también servirá como modelo replicable para otras organizaciones que enfrentan desafíos similares en la protección de sus redes

El problema central que aborda este proyecto radica en la falta de una respuesta automatizada ante dispositivos comprometidos, lo que puede generar una propagación de amenazas dentro de la red (Rios,2020). Se busca responder a la pregunta: ¿cómo mejorar la detección y respuesta ante incidentes de seguridad mediante la integración de tecnologías de monitoreo y aislamiento de dispositivos?

Para ello, se plantea el diseño de una solución siguiendo una metodología basada en el análisis de vulnerabilidades, el diseño de reglas de detección de amenazas y la integración de tecnologías de seguridad como Suricata, YARA y PacketFence dentro de la infraestructura de Security Onion.
Se espera que los resultados obtenidos permitan validar la efectividad del sistema y su capacidad para mejorar la seguridad de la red en entornos empresariales.

2. Objetivos

2.1 Objetivo general

Desarrollar reglas de detección de amenazas para identificar incidentes de seguridad, para lograr el aislamiento de dispositivos comprometidos de manera automática, con el fin de fortalecer las medidas de protección de la red.

2.2 Objetivos específicos

- Analizar las vulnerabilidades existentes en el entorno de una empresa, enfocado en identificar patrones de amenazas relevantes.
- Diseñar un conjunto de reglas y estrategias de automatización para detectar patrones asociados a las amenazas relevantes previamente identificadas, y plantear una estrategia para el aislamiento de dispositivos comprometidos en dichas amenazas.
- Configurar y desplegar reglas de detección y mecanismos de respuesta automatizada en la infraestructura de monitoreo de seguridad de la red de la empresa.
- Evaluar el funcionamiento del sistema de detección y respuesta ante amenazas, validando su capacidad para identificar y alertar sobre incidentes de seguridad.

3. Marco teórico

La seguridad de la red es una de las principales preocupaciones para las organizaciones en la actualidad debido a la creciente sofisticación de las amenazas cibernéticas. Estas amenazas incluyen ataques de *ransomware*, explotación de vulnerabilidades, descarga de archivos maliciosos, ataques de denegación de servicio (DDoS) y técnicas avanzadas de persistencia utilizadas por atacantes para comprometer infraestructuras críticas (Soares, 2023).

Para mitigar estos riesgos, las organizaciones implementan estrategias de protección basadas en soluciones de Control de Acceso a la Red (Network Access Control - NAC). El NAC es un enfoque de seguridad que permite gestionar el acceso a la red con base en políticas específicas, asegurándose de que sólo los dispositivos autorizados y en cumplimiento con los estándares establecidos puedan conectarse. Este tipo de solución actúa como un punto de control que verifica la identidad y el estado de los dispositivos antes de permitirles acceso a los recursos de la red.

Además del NAC, otras tecnologías como los Sistemas de Detección de Intrusos (IDS) y los motores de reglas desempeñan un papel clave en la protección de la red. Los IDS permiten identificar patrones maliciosos en el tráfico de la red en tiempo real, mientras que los motores de reglas, como Suricata y YARA, posibilitan la detección avanzada de amenazas mediante la aplicación de criterios específicos de análisis. La combinación de estas soluciones fortalece la postura de seguridad de una organización al proporcionar capacidades tanto de prevención como de respuesta ante incidentes de ciberseguridad.

Dentro de las soluciones NAC disponibles se encuentra PacketFence, una plataforma de código abierto que permite a las organizaciones gestionar el acceso de dispositivos y usuarios a la red mediante la aplicación de políticas de seguridad basadas en diferentes criterios, tales como direcciones IP, direcciones MAC o los resultados de autenticación de usuarios. Una de las características más destacadas de PacketFence es su capacidad para realizar el aislamiento automático de dispositivos comprometidos, restringiendo su acceso a la red hasta que se resuelvan los problemas detectados. Esto lo convierte en un componente esencial en entornos donde la respuesta rápida es crítica (Ngua, 2023). A pesar de que existen diversas soluciones NAC en el mercado, como Cisco Identity Services Engine (ISE) o ForeScout CounterACT (Omar & Abdelaziz, 2020), la elección de PacketFence en la empresa responde a su naturaleza de código abierto, su facilidad de integración con otras herramientas de seguridad y la posibilidad de personalizar sus funciones sin depender de proveedores comerciales.

Otra herramienta clave en el ámbito de la ciberseguridad es Suricata, un motor de detección de intrusos (IDS) y prevención de intrusos (IPS) diseñado para analizar el tráfico de red en busca de patrones maliciosos (Bhatia & Almukhaini, 2024). Suricata permite detectar anomalías en tiempo

real mediante reglas específicas que describen comportamientos sospechosos. Su capacidad para inspeccionar el tráfico de red a nivel de paquetes y flujos lo convierte en una herramienta poderosa para la detección de ataques en tiempo real. Suricata utiliza reglas de detección basadas en firmas, las cuales consisten en identificadores específicos de amenazas conocidas, como secuencias de bytes o patrones en el tráfico de red. Además, este IDS puede emplear análisis de comportamiento y técnicas heurísticas para detectar amenazas emergentes que no han sido catalogadas previamente. Esta funcionalidad es clave para la detección de ataques *zero-day* y técnicas de explotación avanzadas.

Además de Suricata, herramientas como YARA complementan la detección de amenazas al enfocarse en el análisis de archivos y procesos a nivel del sistema operativo. YARA utiliza patrones definidos mediante reglas para identificar características comunes en *malware* conocido, ayudando a detectar amenazas en la etapa de análisis de archivos específicos (Mahdi & Trabelsi, 2024).

YARA permite crear reglas personalizadas basadas en firmas de *malware*, lo que facilita la identificación de variantes de código malicioso. Su implementación en conjunto con Suricata proporciona una cobertura de seguridad integral, permitiendo detectar amenazas tanto en tráfico de red como en archivos almacenados o ejecutados en los sistemas de la organización.

La integración de estas tecnologías se realiza en plataformas como Security Onion, que actúa como un sistema integral para el monitoreo y análisis de seguridad en redes empresariales (Tymoshchuk, Vorona, Dolinskyi & Shymanska, 2024). Security Onion proporciona un entorno centralizado donde se pueden gestionar alertas generadas por herramientas como Suricata y YARA, ofreciendo una visión consolidada de los eventos de seguridad.

A pesar de la existencia de otras soluciones disponibles, como Splunk y AlienVault USM (Alkasassbeh & Baddar, 2023), Security Onion es utilizada en la empresa debido a su política de código abierto, lo que permite una mayor personalización y control sin depender de licencias costosas.

El sistema de detección y respuesta ante incidentes planteado en este proyecto busca aprovechar la integración de PacketFence, Suricata, YARA y Security Onion para crear un entorno de seguridad robusto y automatizado.

Se plantea el siguiente flujo:

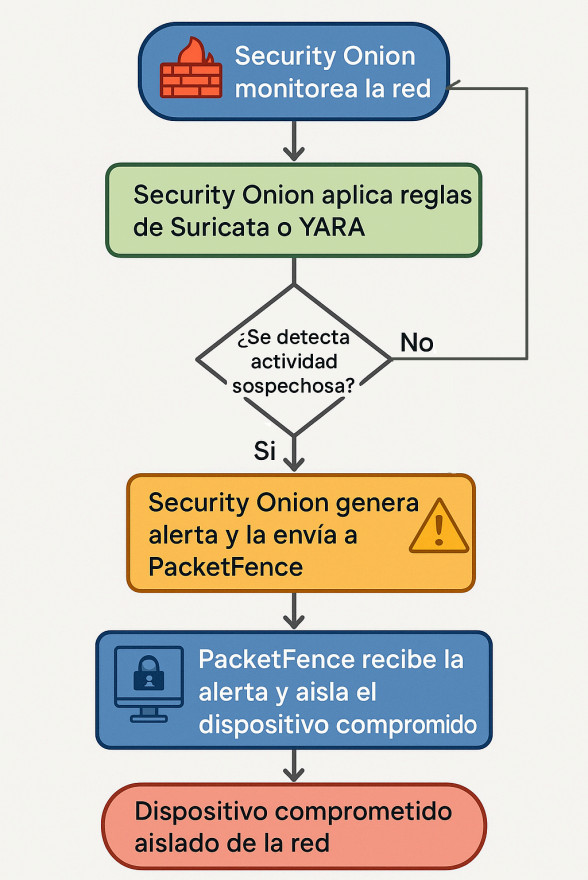


Figura 1 . Flujo general del proyecto

La combinación de estas tecnologías permite:

- Detección temprana de amenazas mediante análisis de tráfico de red y archivos sospechosos.
- Respuesta automatizada a incidentes a través del aislamiento inmediato de dispositivos comprometidos.
- Centralización de eventos de seguridad mejorando la visibilidad y la toma de decisiones en la gestión de incidentes.
- Reducción del impacto de ataques cibernéticos al contener la propagación de amenazas dentro de la red corporativa.

Este enfoque no solo fortalece la seguridad de la red de la empresa, sino que también ofrece un modelo replicable que puede ser adoptado por otras organizaciones que buscan optimizar sus estrategias de defensa ante un panorama de amenazas en constante evolución.

4. Metodología

- Llevar a cabo un escaneo de vulnerabilidades para identificar posibles puntos débiles y amenazas específicas en la infraestructura de red.
- Investigar y recopilar información sobre comportamientos maliciosos comunes, como técnicas de ataque conocidas, patrones de tráfico de red y características de malware, para redactar reglas en formatos compatibles con Suricata y YARA. Estas reglas estarán orientadas a detectar las amenazas identificadas en el entorno de la empresa.
- Validar la comunicación existente entre las instancias Security Onion y PacketFence desplegadas en la empresa, realizando pruebas de generación de alertas mediante las reglas diseñadas en formatos compatibles con Suricata y YARA, implementadas en Security Onion, y que estas alertas se envíen de manera efectiva a PacketFence para su gestión.
- Monitorear la generación de alertas a partir de las reglas diseñadas en formatos compatibles con Suricata y YARA, implementadas en Security Onion. Se verificará que, al generarse una alerta, ésta sea enviada correctamente a PacketFence y que el sistema aísle automáticamente el dispositivo comprometido, registrando los resultados para su análisis.

5. Análisis de resultados

En la empresa se utiliza la solución de control de acceso a la red de código abierto PacketFence, una tecnología clave para reforzar la seguridad y la administración de la infraestructura de red. PacketFence actúa como una capa de seguridad entre los usuarios y los recursos de la red, garantizando que solo los dispositivos y usuarios autorizados puedan acceder a los recursos adecuados. Además, permite la aplicación de medidas correctivas en caso de incumplimiento de las políticas de seguridad establecidas, contribuyendo así a una administración más efectiva y a la mitigación de posibles riesgos.

Al acceder a la plataforma de PacketFence dentro del entorno de la empresa, se obtiene una visión detallada y en tiempo real de la topología de la red. Esta visualización permite identificar

la estructura y organización de los dispositivos conectados, tanto aquellos que están registrados y cumplen con los requisitos de seguridad, como aquellos no registrados que podrían representar un riesgo.

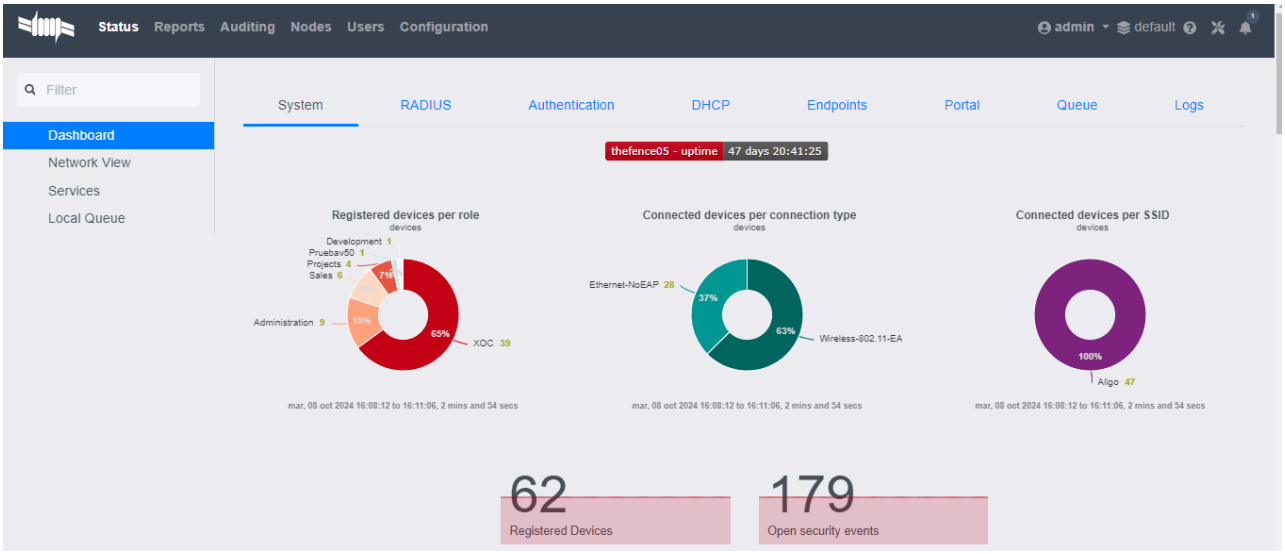


Figura 2. Packetfence Aligo

La arquitectura de red dentro de Aligo está diseñada con PacketFence como el eje central de la organización. Desde este núcleo de administración y seguridad se desprenden cinco switches, cada uno de los cuales está destinado a diferentes roles dentro de la empresa. Esta segmentación garantiza que los distintos departamentos y niveles de acceso cuenten con una configuración específica según sus necesidades y privilegios, reforzando el control y reduciendo la exposición a amenazas.

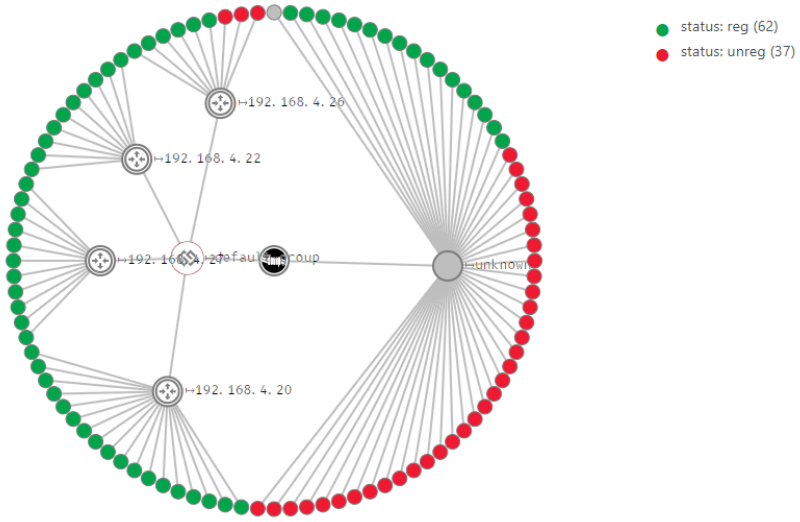


Figura 3. Arquitectura de red Aligo

Además, se cuenta con un apartado específico para los tipos de conexión, en el que se detalla si la red es cableada o inalámbrica. Esta clasificación permite gestionar de manera más eficiente la infraestructura de red, asegurando un mejor control sobre la organización. Al contar con un registro claro y estructurado, se optimiza la administración de los recursos y se facilita la identificación de posibles mejoras o necesidades en la conectividad.

connection_type	connections	percent
Wireless-802.11-EAP	28	60.9
Ethernet-NoEAP	18	39.1

Figura 4. Distribución de dispositivos por tipo de conexión

Escaneo de vulnerabilidades:

Se realizó un escaneo de seguridad en los cuatro switches de la red utilizando la herramienta Nessus, una plataforma especializada en la detección de vulnerabilidades. Este análisis permitió identificar posibles fallos de seguridad, configuraciones incorrectas y puertos expuestos, con el objetivo de fortalecer la protección de la infraestructura de red.

192.168.4.20



Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5	4.2	0.0876	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
LOW	2.1*	2.2	0.8939	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	185519	SNMP Server Detection
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported

Figura 5. Escaneo en Nessus de Switch 192.168.4.20

192.168.4.22



Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5	4.2	0.0876	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
LOW	2.1*	2.2	0.8939	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	185519	SNMP Server Detection
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported

Figura 6. Escaneo en Nessus de Switch 192.168.4.22

Tras realizar un escaneo de seguridad con la herramienta Nessus en los switches con dirección IP 192.168.4.20 y 192.168.4.22, se identificaron un total de 28 vulnerabilidades para cada uno, clasificadas en distintos niveles de severidad: 1 crítica, 2 altas, 2 medias, 1 baja y 22 informativas. Estas vulnerabilidades pueden comprometer la seguridad del dispositivo y, por ende, la integridad de la red si no se gestionan adecuadamente.

Uno de los hallazgos más relevantes es la presencia de un certificado SSL autofirmado, el cual no ha sido emitido por una autoridad certificadora confiable. Como resultado, Nessus generó las alertas "SSL Certificate Cannot Be Trusted" y "SSL Self-Signed Certificate", ambas clasificadas con una severidad media. Este tipo de certificados puede exponer las comunicaciones cifradas a ataques de intermediario (MITM), ya que los clientes no pueden verificar su autenticidad. Además, se detectó que el certificado utiliza un algoritmo de hash débil, lo que representa un riesgo adicional para la seguridad de las conexiones.

Otra vulnerabilidad identificada es la exposición del timestamp ICMP, la cual permite a un atacante remoto conocer la hora del sistema del dispositivo. Esta información puede ser utilizada para realizar ataques de sincronización de tiempos o facilitar otras técnicas de reconocimiento dentro de la red.

Para el switch con ip 192.168.4.26, se obtuvo lo siguiente desde Nessus:

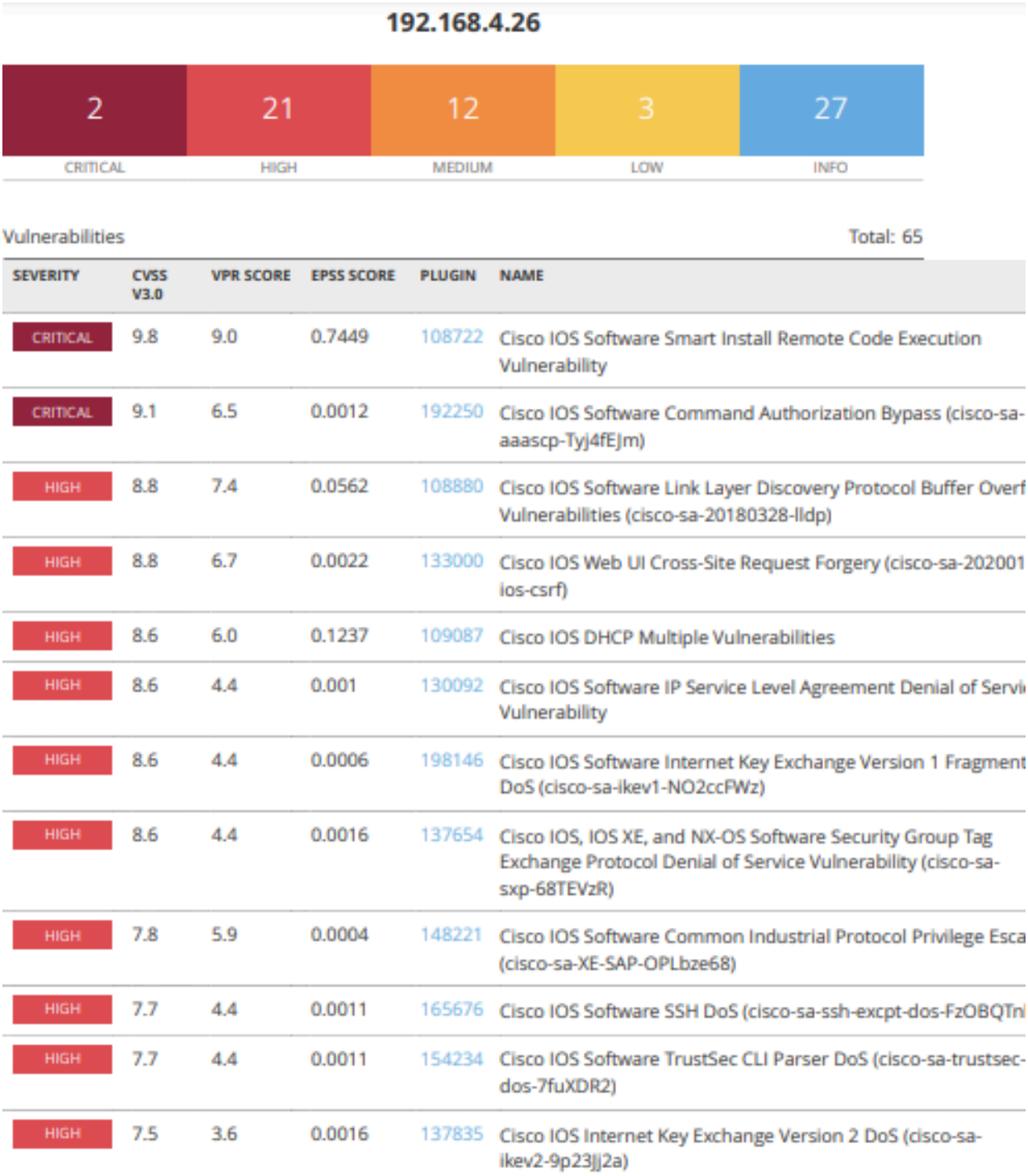


Figura 7. Escaneo en Nessus de Switch 192.168.4.26

Se revelaron un total de 65 vulnerabilidades, clasificadas en 2 críticas, 21 altas, 12 medias, 3 bajas y 27 informativas. Las vulnerabilidades críticas incluyen fallas graves como la ejecución remota de código en Cisco Smart Install (CVE-2018-0171), con un puntaje CVSS de 9.8, lo que

permite que un atacante pueda tomar el control del switch sin autenticación. Otra vulnerabilidad crítica detectada es un bypass de autorización de comandos en Cisco IOS, con un puntaje de 9.1, que permite a usuarios no autorizados ejecutar comandos con privilegios elevados, comprometiendo la seguridad del dispositivo.

Dentro de las vulnerabilidades altas, se encuentran múltiples fallas en protocolos y servicios utilizados en Cisco IOS. Se detectó un desbordamiento de búfer en el Protocolo de Descubrimiento de Capa de Enlace (LLDP), que puede ser explotado para ejecutar código arbitrario o causar una denegación de servicio. También se identificó una vulnerabilidad en la interfaz web de Cisco IOS, expuesta a ataques de Cross-Site Request Forgery (CSRF), lo que permite a un atacante realizar cambios en la configuración del dispositivo sin autorización. Adicionalmente, existen problemas en la implementación del protocolo DHCP, que pueden derivar en ataques de denegación de servicio, así como fallas en Internet Key Exchange (IKE) v1 y v2, utilizadas en ataques DoS.

En cuanto a las vulnerabilidades de nivel medio, se identificaron configuraciones débiles en SNMP, donde el uso de comunidades predeterminadas como "public" facilita ataques de recopilación de información sobre la infraestructura de red. Además, se detectaron problemas en los certificados SSL/TLS, como el uso de hashes inseguros y cifrados obsoletos, entre ellos RC4 y SWEET32, lo que podría exponer el tráfico de red a ataques de interceptación.

Las vulnerabilidades bajas e informativas incluyen configuraciones inseguras en SSL/TLS, revelación de información a través de ICMP timestamp, y exposición de datos del sistema mediante consultas SNMP. Aunque estas no representan un riesgo inmediato, pueden ser aprovechadas por atacantes para recopilar información sobre la red y planear ataques más avanzados.

En conjunto, estas vulnerabilidades reflejan debilidades propias de Cisco IOS que pueden comprometer seriamente la seguridad del switch. La presencia de múltiples fallas de ejecución remota de código, acceso no autorizado y ataques de denegación de servicio resalta la necesidad de aplicar medidas de mitigación específicas para dispositivos Cisco, incluyendo la actualización del sistema operativo y la configuración segura de los servicios expuestos.

Y para el switch con la dirección IP 192.168.4.27, se obtuvieron los siguientes resultados a partir del análisis realizado con Nessus:



Vulnerabilities Total: 56

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.1	6.5	0.0012	192250	Cisco IOS Software Command Authorization Bypass (cisco-sa-aaascp-Tyj4fEJm)
HIGH	8.6	4.4	0.0006	198146	Cisco IOS Software Internet Key Exchange Version 1 Fragment DoS (cisco-sa-ikev1-NO2ccFWz)
HIGH	8.6	4.4	0.0004	193269	Cisco IOS Software Locator ID Separation Protocol DoS (cisco-lisp-3gYXs3qP)
HIGH	7.5	4.2	0.0876	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.4	4.4	0.0004	216409	Cisco IOS Software Intermediate System to Intermediate Syste DoS (cisco-sa-isis-sGjyOUHX)
HIGH	7.5*	5.2	0.4545	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.6	7.4	0.0096	183215	Cisco IOS Software Group Encrypted Transport VPN Out of Bo Write (cisco-sa-getvpn-rce-g8qR68sx)
MEDIUM	6.5	3.6	0.0005	207787	Cisco IOS Software Web UI XSRF (cisco-sa-ios-webui-HfwnRgk)
MEDIUM	6.5	3.6	0.0018	91854	Cisco IOS Zone-Based Firewall Feature Security Bypass (CSCun94946)
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.0*	3.6	0.0575	76474	SNMP 'GETBULK' Reflection DDoS

Figura 8. Escaneo en Nessus de Switch 192.168.4.27

El escaneo de seguridad realizado en el switch con dirección IP 192.168.4.27 reveló un total de 56 vulnerabilidades, clasificadas en una crítica, cinco altas, ocho medias, seis bajas y 36 informativas. Este análisis permitió identificar una serie de debilidades en la configuración del dispositivo, muchas de las cuales pueden ser explotadas por atacantes para comprometer la infraestructura de red.

Dentro de las vulnerabilidades críticas, se encontró una relacionada con la autorización de comandos en Cisco IOS, la cual permite la ejecución de instrucciones sin los permisos adecuados. Esta falla representa un riesgo significativo, ya que un atacante podría modificar configuraciones sensibles o deshabilitar controles de seguridad sin autenticación previa.

Entre las vulnerabilidades de nivel alto, destaca un problema con el protocolo SNMP, donde se detectó el uso de comunidades predeterminadas como "public", lo que facilita el acceso no autorizado a información del dispositivo. Además, se identificaron fallos en la implementación del protocolo IKEv1, lo que podría ser explotado en ataques de denegación de servicio. También se encontraron debilidades en la gestión de paquetes en el protocolo IS-IS, lo que podría derivar en interrupciones en la comunicación entre dispositivos de la red.

Las vulnerabilidades de severidad media incluyen problemas en la configuración de SSL/TLS, tales como el uso de certificados autofirmados y cifrados obsoletos, lo que expone las comunicaciones a ataques de intermediario (MITM). Asimismo, se hallaron fallos en la configuración del firewall basado en zonas en Cisco IOS, lo que podría permitir la evasión de políticas de seguridad establecidas.

En cuanto a las vulnerabilidades bajas, se identificaron configuraciones inseguras en SSH, específicamente el uso de algoritmos débiles para el intercambio de claves. También se detectó la exposición del timestamp ICMP, lo que permite a atacantes externos obtener la hora del sistema del dispositivo, información que podría ser utilizada para coordinar ataques basados en sincronización de tiempo.

Las vulnerabilidades informativas revelaron detalles del dispositivo, como la versión del sistema operativo, los servicios activos y la estructura de la red. Aunque estos hallazgos no representan un riesgo inmediato, pueden ser aprovechados por atacantes para planificar ataques más avanzados.

Para mitigar las vulnerabilidades detectadas en los switches analizados, se aprovechó Security Onion, una plataforma de detección y respuesta ante amenazas utilizada en la empresa. Esta herramienta permitió fortalecer la seguridad de la infraestructura de red mediante la monitorización en tiempo real, la detección de eventos sospechosos y la correlación de alertas generadas por los dispositivos.

El primer paso en la mitigación fue la configuración de reglas en Suricata, un sistema de detección y prevención de intrusiones integrado en Security Onion. Se diseñaron reglas específicas para identificar intentos de explotación de vulnerabilidades críticas, como ejecución remota de código y bypass de autenticación en Cisco IOS. Estas reglas permitieron generar

alertas ante cualquier actividad maliciosa dirigida a los switches, facilitando la detección temprana de ataques.



Figura 9. Regla Suricata

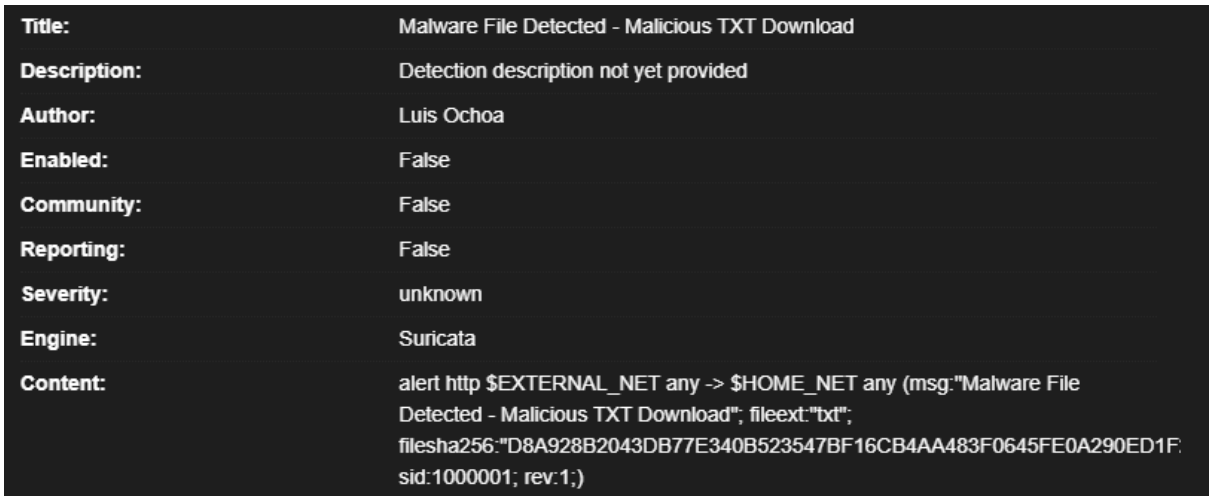


Figura 10. Regla Suricata guardada

Además, se implementaron reglas YARA para analizar los registros de tráfico de red en busca de patrones maliciosos. Estas reglas fueron clave para detectar intentos de explotación relacionados con el uso de protocolos inseguros y configuraciones vulnerables en los dispositivos. Mientras que las reglas de Suricata se centraron en identificar patrones anómalos en el tráfico de red, como intentos de escaneo y conexiones con servidores sospechosos, las reglas de YARA permitieron reconocer archivos y procesos asociados con malware conocido.

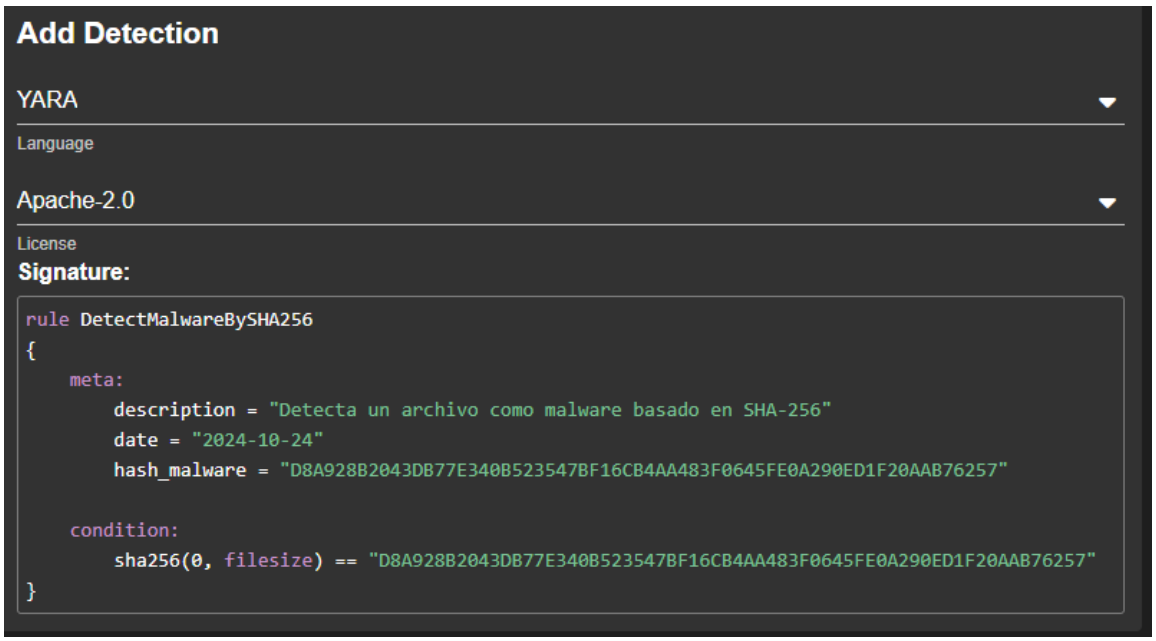


Figura 11. Regla YARA

La creación de estas reglas se llevó a cabo mediante un enfoque combinado que incluyó tanto el desarrollo manual como la adaptación de reglas provenientes de fuentes en línea. Las reglas personalizadas fueron diseñadas a partir de un análisis detallado de las vulnerabilidades detectadas, asegurando una cobertura específica para los riesgos identificados en la infraestructura de la empresa. Por otro lado, las reglas obtenidas externamente fueron seleccionadas con base en su relevancia y efectividad dentro del entorno evaluado.

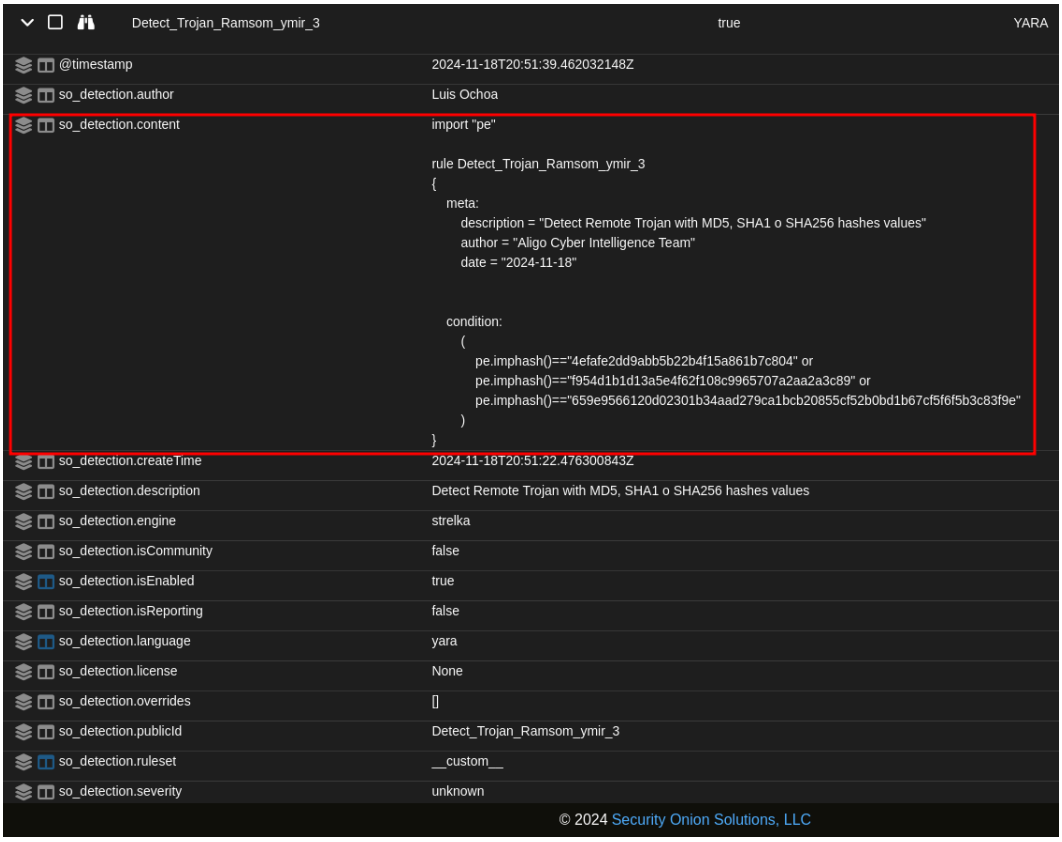


Figura 12. Regla YARA ransomware YMIR

Para complementar la estrategia de detección y respuesta ante amenazas en la infraestructura de red, se implementó la integración de Security Onion con PacketFence, una solución de Network Access Control (NAC) que permite aislar dispositivos comprometidos en caso de detectar actividad maliciosa. Esta integración facilitó una respuesta automatizada y efectiva ante incidentes de seguridad, minimizando el impacto de posibles ataques en la red.

El proceso de integración se basó en la transmisión de alertas generadas en Security Onion hacia PacketFence, permitiendo que los dispositivos identificados como potencialmente comprometidos fueran aislados de forma automática. Para lograr esto, se estableció un mecanismo en el que, cuando Suricata o YARA detectaban eventos críticos, como intentos de explotación de vulnerabilidades, tráfico malicioso o actividad sospechosa en un dispositivo, Security Onion generaba una alerta que era enviada a PacketFence.

PacketFence, al recibir la alerta, aplicaba una política de contención al dispositivo afectado, restringiendo su acceso a la red o redirigiéndolo a una zona de cuarentena con permisos limitados. Esta acción evitaba que un posible atacante pudiera propagar malware, realizar movimientos laterales dentro de la red o exfiltrar información sensible.

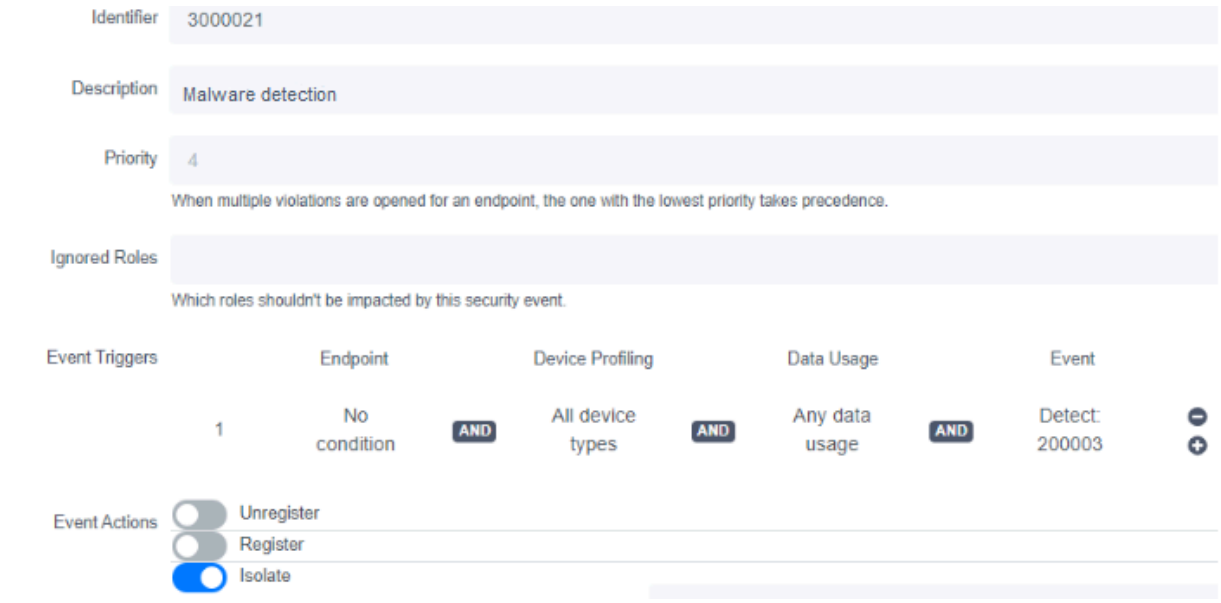


Figura 13. Creación regla de aislamiento en Packetfence

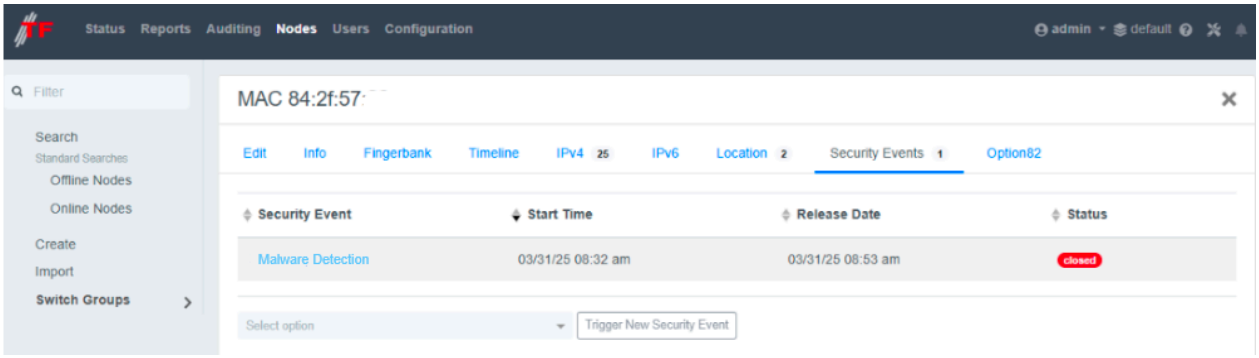


Figura 14. Aislamiento en Packetfence

Para garantizar una integración eficiente, se desarrollaron reglas específicas que permitieron a Security Onion identificar los dispositivos en riesgo con precisión, asegurando que solo aquellos con actividad sospechosa fueran aislados. Asimismo, se configuraron mecanismos de registro y monitoreo en ambos sistemas para validar que los dispositivos afectados por un aislamiento pudieran ser restaurados tras una revisión manual, evitando interrupciones innecesarias en la operación de la empresa.

Esta integración fortaleció significativamente la capacidad de respuesta ante incidentes, permitiendo no solo la detección temprana de amenazas, sino también la aplicación de medidas correctivas en tiempo real. Al combinar detección avanzada (Security Onion) con control de acceso y contención (PacketFence), se logró mejorar la seguridad de la red, reduciendo los riesgos asociados a la propagación de ataques y garantizando la estabilidad de la infraestructura tecnológica.

6. Conclusiones y recomendaciones

El desarrollo de este proyecto permitió validar la efectividad de la integración de tecnologías para la detección y respuesta ante incidentes de seguridad en entornos empresariales. La implementación de reglas específicas para la identificación de patrones maliciosos en el tráfico de red y archivos sospechosos demostró ser una estrategia eficiente para la detección temprana de amenazas.

Se logró establecer un mecanismo automatizado de respuesta que, a través de PacketFence, permite el aislamiento de dispositivos comprometidos, minimizando el impacto de posibles ataques y evitando la propagación de amenazas dentro de la red corporativa.

El análisis de vulnerabilidades realizado permitió identificar y mitigar riesgos en la infraestructura de la empresa, reforzando la importancia de un monitoreo continuo y una actualización constante de reglas y configuraciones de seguridad. Además, la validación de la comunicación entre Security Onion y PacketFence confirmó la viabilidad de un sistema de respuesta automatizada basado en eventos generados por Suricata y YARA.

Referencias

Rios, C. A. (2020). Arquitectura para automatizar respuesta a incidentes de seguridad de la información relacionados con ataques internos mediante la ejecución de técnicas spoofing. Recuperado de: http://hdl.handle.net/20.500.12622/4456.

Symantec. (2024).The 2024 Ransomware Threat Landscape. Recuperado de https://www.symantec.broadcom.com/hubfs/Symantec_Ransomware_Threat_Landscape_2024.pdf

Muhammad, T., Munir, M. T., Munir, M. Z., & Zafar, M. W. (2022). Integrative cybersecurity: merging zero trust, layered defense, and global standards for a resilient digital future. International Journal of Computer Science and Technology, 6(4), 99-135. Recuperado de https://www.researchgate.net/profile/Tayyab-Muhammad-2/publication/376046489_Integrative_Cybersecurity_Merging_Zero_Trust_Layered_Defense_and_Global_Standards_for_a_Resilient_

Digital_Future/links/65683aa1ce88b870311fcc5a/Integrative-Cybersecurity-Merging-Zero-Trust-Layered-Defense-and-Global-Standards-for-a-Resilient-Digital-Future.pdf

Lindemulder, G., & Kosinski, M. (2024). Cybersecurity. *IBM*. Recuperado de https://www.ibm.com/es-es/topics/cybersecurity

Soares, Luis. (2023). The evolution of cyber threats and its future landscape. Recuperado de https://www.researchgate.net/publication/369010694_The_evolution_of_cyber_threats_and_its_future_landscape

Ngua Nsee, R. B. N. (2023). Implementación y creación de escenarios de pruebas con el NAC PacketFence. Recuperado de http://hdl.handle.net/10045/135259

Rami Radwan Omar and M. Abdelaziz. 2020. A Comparative Study of Network Access Control and Software-Defined Perimeter. In Proceedings of the 6th International Conference on Engineering & MIS 2020 (ICEMIS'20). Association for Computing Machinery, New York, NY, USA, Article 22, 1–5. https://doi.org/10.1145/3410352.3410754

G. Bhatia and G. Almukhaini, "Enhancing Cyber Attack Detection: An Analysis of Security Onion for Small and Midsize Enterprise," 2024 1st International Conference on Innovative Engineering Sciences and Technological Research (ICIESTR), Muscat, Oman, 2024, pp. 1-6. Recuperado de https://www.researchgate.net/publication/336332064_Intrusion_Detection_System_Based_on_Network_Traffic_Using_Deep_Neural_Networks

R. H. Mahdi and H. Trabelsi, "Detection of Malware by Using YARA Rules,"2024 21st International Multi-Conference on Systems, Signals & Devices (SSD), Erbil, Iraq, 2024, pp. 1-8. Recuperado de: https://ieeexplore.ieee.org/document/10549308

Tymoshchuk, V., Vorona, M., Dolinskyi, A., & Shymanska, V. (2024, 13 de diciembre). Security Onion platform as a tool for detecting and analysing cyber threats. Logos Science. Recuperado de https://archive.logos-science.com/index.php/conference-proceedings/article/view/2538/2575

Alkasassbeh, M., & Al-Haj Baddar, S. (2023). Intrusion detection systems: A state-of-the-art taxonomy and survey. Arabian Journal for Science and Engineering, 48(8), 10021–10064. https://doi.org/10.1007/s13369-022-07412-1

Departamento de Ingeniería Electrónica y de Telecomunicaciones

Implementación de un Sistema de Aislamiento de Dispositivos mediante la Integración de Tecnologías de Monitoreo y Respuesta a Incidentes

UNIVERSIDAD DE ANTIOQUIA
Facultad de Ingeniería

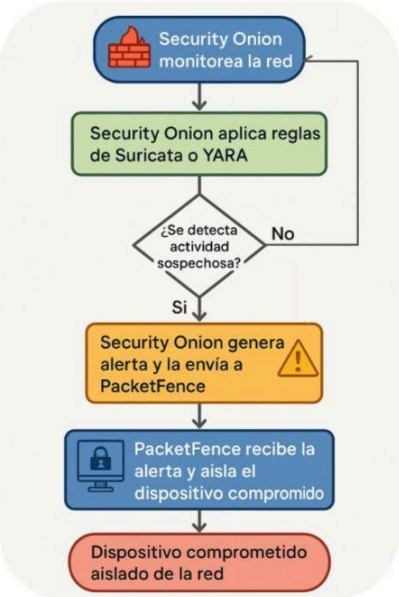
PRACTICANTE: María Lucía Orozco Guerra
ASESORES: Sergio Armando Gutiérrez Betancur

PROGRAMA: Ingeniería de Telecomunicaciones
Semestre de la práctica: 2024-2

Introducción

La seguridad de la red es una preocupación creciente para las organizaciones debido al aumento en la complejidad y frecuencia de las amenazas cibernéticas. Ante este panorama, es fundamental contar con soluciones que no solo detecten actividades sospechosas, sino que también permitan una respuesta rápida y eficiente.

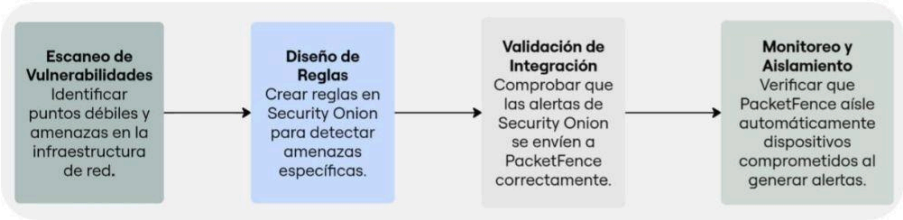
Actualmente, existen diversas herramientas que ofrecen funciones de monitoreo, detección y control de acceso a la red. Entre ellas se destacan los sistemas de detección de intrusos (IDS), los motores de reglas para análisis de tráfico y archivos, y las soluciones de Control de Acceso a la Red (NAC). La integración de estas tecnologías permite mejorar la visibilidad, reducir los tiempos de respuesta y contener las amenazas antes de que se propaguen por toda la red.



Objetivos

- Analizar las vulnerabilidades existentes en el entorno de una empresa, enfocado en identificar patrones de amenazas relevantes.
- Diseñar un conjunto de reglas y estrategias de automatización para detectar patrones asociados a las amenazas relevantes previamente identificadas, y plantear una estrategia para el aislamiento de dispositivos comprometidos en dichas amenazas.
- Configurar y desplegar reglas de detección y mecanismos de respuesta automatizada en la infraestructura de monitoreo de seguridad de la red de la empresa.
- Evaluar el funcionamiento del sistema de detección y respuesta ante amenazas, validando su capacidad para identificar y alertar sobre incidentes de seguridad.

Metodología



Resultados

- Se identificaron 23 vulnerabilidades en switches de la red, de las cuales 11 fueron clasificadas como críticas, permitiendo ajustar las reglas de detección.
- Se crearon 7 reglas tipo Suricata enfocadas en tráfico malicioso como descargas de malware, y 5 reglas YARA orientadas a archivos sospechosos.
- La integración con PacketFence permitió automatizar el aislamiento de dispositivos comprometidos tras la validación de alertas generadas en Security Onion, en entornos de pruebas.

Conclusiones

- Se validó la efectividad de integrar tecnologías como Security Onion y PacketFence para la detección y respuesta a incidentes.
- Las reglas específicas permitieron una detección temprana de amenazas en tráfico de red y archivos.
- Se implementó con éxito un mecanismo automatizado de aislamiento de dispositivos comprometidos.
- El análisis de vulnerabilidades y la validación de comunicaciones fortalecieron la seguridad del entorno empresarial.

DATOS DE CONTACTO DEL AUTOR:
+57 3015679702
marial.orozco@udea.edu.co