UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

APLICACIÓN DEL PROCESO THREAT HUNTING PARA LA DETECCIÓN DE VULNERABILIDADES Y CONTRAMEDIDAS EN LA INFRAESTRUCTURA DE RED DEL CUERPO DE BOMBEROS DE AMBATO.

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Tecnologías de la Información.

ÁREA: Seguridad informática.
LÍNEA DE INVESTIGACIÓN: Tecnologías de la información
AUTOR: Bryan Jardiel Avilés Vasco
TUTOR: Ing. Andrea Patricia Sánchez Zumba, Mg.

Ambato - Ecuador
agosto – 2023

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: APLICACIÓN DEL PROCESO THREAT HUNTING PARA LA DETECCIÓN DE VULNERABILIDADES Y CONTRAMEDIDAS EN LA INFRAESTRUCTURA DE RED DEL CUERPO DE BOMBEROS DE AMBATO, desarrollado bajo la modalidad Proyecto de Investigación por el señor Bryan Jardiel Avilés Vasco, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, agosto 2023.

Ing. Andrea Patricia Sánchez Zumba, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación titulado: APLICACIÓN DEL PROCESO THREAT HUNTING PARA LA DETECCIÓN DE VULNERABILIDADES Y CONTRAMEDIDAS EN LA INFRAESTRUCTURA DE RED DEL CUERPO DE BOMBEROS DE AMBATO es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, agosto 2023.

Bryan Jardiel Avilés Vasco

C.C. 0503518219

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, agosto 2023.

Bryan Jardiel Avilés Vasco

C.C. 0503518219

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Bryan Jardiel Avilés Vasco estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado APLICACIÓN DEL PROCESO THREAT HUNTING PARA LA DETECCIÓN DE VULNERABILIDADES Y CONTRAMEDIDAS EN LA INFRAESTRUCTURA DE RED DEL CUERPO DE BOMBEROS DE AMBATO, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, agosto 2023.

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
FELIX OSCAR FERNANDEZ PENA

PhD. Félix Oscar Fernández Peña
PROFESOR CALIFICADOR

Firmado electrónicamente por:
DENNIS VINICIO CHICAIZA CASTILLO

Ing. Dennis Vinicio Chicaiza Castillo
PROFESOR CALIFICADOR

DEDICATORIA

El presente trabajo de titulación siendo uno de los mayores logros en mi vida, se lo dedico, primeramente, a mis padres Edgar Avilés y Sandra Vasco quiénes siempre confiaron en mí, me inculcaron valores, me enseñaron a nunca rendirme, y con su apoyo y cariño logré cumplir todas mis metas. A mi amada novia Johanna Cañizares quien estuvo a mi lado en muchos momentos difíciles durante gran parte de mi experiencia universitaria, que desde el primer instante supo brindarme su apoyo incondicional, confianza y amor siendo parte importe en la obtención de este logro.

A mi hermana Doménica Avilés que nunca dudo de mis aptitudes y me motivo para siempre seguir adelante. A mis tías Jenny Avilés, Martha Avilés, Mayra Vasco y familia en general quienes fueron parte de mi crecimiento personal y siempre estuvieron presentes cuando más las necesitaba. A Luis Correa, Marco Castellano y Oscar Chacón, que desde la infancia nunca me dejaron solo y fueron como hermanos para mí.

A todos mis amigos que me acompañaron durante este proceso de aprendizaje, Joel, Damián, Ariel y Pablo, por enseñarme y ofrecerme una amistad sincera.

Y finalmente quiero dedicar este proyecto a la ingeniera Andrea Sánchez quien supo ser una excelente tutora, y guiarme a lo largo de todo el proceso.

AGRADECIMIENTO

Agradezco primeramente a Dios por brindarme salud, no abandonarme en ningún aspecto de mi vida y por ayudarme a sobrepasar cada obstáculo que la vida me presentaba.

A mis padres y familia por enseñarme a no darme por vencido, a ser una mejor persona y por procurar que nunca me falte nada sobre todo amor y apoyo.

A mi novia Johanna Cañizares por todo el amor, apoyo y cariño que siempre me brindó que me ayudar superar muchas adversidades en gran parte este camino.

A mis queridos amigos por toda las experiencias y aventuras vividas a lo largo de toda la vida universitaria.

A mi tutora Andrea Sánchez por ayudarme aportándome su conocimiento y experiencia como profesional.

Bryan Jardiel Avilés Vasco

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICO

RESUMEN EJECUTIVO

La seguridad de la infraestructura de red del Cuerpo de Bomberos de Ambato adquiere un papel de vital importancia, dado que alberga datos sensibles y estratégicos para el funcionamiento de sus operaciones. Frente al constante incremento de los ciberataques y la continua evolución de las tácticas empleadas por actores maliciosos, se hace esencial contar con una estrategia efectiva que permita identificar y mitigar las amenazas en tiempo real. En este contexto, este trabajo propone la elaboración de un manual exhaustivo para implementar el proceso de Threat Hunting en la red del Cuerpo de Bomberos de Ambato. Utilizando una variedad de herramientas especializadas en ciberseguridad como Wireshark, Nessus y Advance IP scanner. Además, se realizó un análisis manual de los archivos log, profundizando en el entendimiento de su manejo y en su relevancia en el ámbito de la ciberseguridad. Como complemento, se desarrolló un código en Python para ampliar el análisis, con el propósito de identificar y abordar vulnerabilidades que puedan poner en peligro la solidez de la infraestructura de la red. Este enfoque no solo permitió detectar debilidades en la seguridad, sino que también dio paso a la planificación de diversas contramedidas destinadas a fortalecer los puntos susceptibles hallados en la red. Finalmente, el proceso fue documentado para asegurar la trazabilidad y replicabilidad de las acciones emprendidas.

Palabras clave: Ciberseguridad, monitoreo, Archivos log, Threat hunting, vulnerabilidad, amenaza, mitigación.

ABSTRACT

The security of the network infrastructure of Ambato Fire Department takes on a vital role, as it houses sensitive and strategic data for the functioning of its operations. Given the constant increase in cyberattacks and the ongoing evolution of tactics employed by malicious actors, it is essential to have an effective strategy that enables the identification and mitigation of threats in real time. In this context, this work proposes the development of a comprehensive manual to implement the Threat Hunting process in the network of Ambato Fire Department. Utilizing a variety of specialized cybersecurity tools such as Wireshark, Nessus, and Advanced IP Scanner. Additionally, a manual analysis of log files was conducted, delving into the understanding of their handling and their relevance in the realm of cybersecurity. As a complement, a Python code was developed to enhance the analysis, with the purpose of identifying and addressing vulnerabilities that could jeopardize the solidity of the network infrastructure. This approach not only allowed for the detection of security weaknesses but also paved the way for the planning of various countermeasures aimed at strengthening the identified susceptible points in the network. Finally, the process was documented to ensure the traceability and replicability of the undertaken actions.

Keywords: Cybersecurity, monitoring, Log files, Threat hunting, vulnerability, threat, mitigation.

CAPÍTULO I.- MARCO TEÓRICO

1.1. Tema de investigación

APLICACIÓN DEL PROCESO THREAT HUNTING PARA LA DETECCIÓN DE VULNERABILIDADES Y CONTRAMEDIDAS EN LA INFRAESTRUCTURA DE RED DEL CUERPO DE BOMBEROS DE AMBATO.

1.1.1. Planteamiento del problema

En los últimos años, a nivel mundial ha existido un crecimiento considerable en los ataques informáticos [1]. Debido al uso de internet y al desarrollo de nuevas tecnologías, tanto las empresas como los usuarios convencionales han generado una dependencia a dichos sistemas, volviendo vulnerable su entorno de trabajo, ya que estas tecnologías están expuestas a cualquier tipo de ataque con el fin de obtener datos de la empresa con diferentes fines, en su mayoría maliciosos [2].

La pérdida de información y daños causados a la infraestructura de Tecnologías de la Información (TI) son varias de las consecuencias que pueden causar estos llamados ataques informáticos. En consecuencia, se ha registrado un aumento considerable de estos ataques en las empresas y en las entidades que dependen de la tecnología para realizar sus procesos industriales [3]. En enero de 2021, se realizó un reporte de la actividad de los ataques informáticos, en especial el denominado phishing que ataca principalmente a las entidades financieras con un 24.9% de los ataques, seguido del medio social con 23.6% y los demás sectores son SAAS/Webmail, Payment, Otros, Comercio electrónico, logistics/Shipping, y criptomonedas con el 19.6%, 8.5%, 8.0%,7.6%, 5.8%, y 2.0% respectivamente [4].

El problema creció notablemente tras la pandemia del SARS-CoV-2, que sufrió la humanidad, obligando a los diferentes usuarios a aplicar diferentes técnicas para prevenir posibles ataques. La principal causa que ha generado la vulnerabilidad de la información de los sistemas es la actual dependencia de la tecnología junto con la fácil accesibilidad que se tiene [5].

En todo el mundo, el riesgo de sufrir un robo de información por los ataques informáticos es alto, por lo que las empresas pequeñas y grandes han tomado la decisión de contrarrestarlos a través de los departamentos de TIC'S, dando prioridad al cuidado de la información [6].

El Ecuador ha experimentado un aumento significativo en los ataques cibernéticos en los últimos años, lo que ha llevado al país a ocupar el cuarto lugar en Sudamérica en términos de número de ataques recibidos. Según estadísticas recientes, el país ha recibido alrededor del 3.16% del total de los ataques en la región. Estos ataques incluyen incidentes como el robo de información personal de millones de ecuatorianos y la exposición de información confidencial de empresas de telecomunicaciones. Además, se han producido numerosos ataques como HackTool.Win32.NetScan.gen con un 17.48%, Troyanos con un 7.96% de ataques que se han efectuado en el último mes, lo que demuestra la importancia de que las empresas y los usuarios adopten medidas de seguridad adecuadas para proteger sus sistemas y datos personales [4].

En la provincia de Tungurahua existen microempresas, entidades y empresas que gracias a la facilidad de acceso a la tecnología han crecido de una manera impresionante, incluyendo la infraestructura de red que las instituciones manejan para cubrir la demanda y necesidades empresariales.

La información crítica manejada por el cuerpo de bomberos de Ambato se encuentra en riesgo debido a la falta de un proceso concreto para protegerla, lo que la hace susceptible a diversos tipos de ataques cibernéticos. Entre ellos, se destacan la suplantación de identidad, el ataque Man-in-the-Middle (MiTM), el ataque de denegación de servicio (DoS), el ataque de denegación de servicio distribuido (DDoS) y el phishing, así como otros tipos de ataques como la inyección de SQL y el ransomware. La falta de conocimiento sobre seguridad cibernética por parte de los miembros de la entidad también agrava la situación, ya que pueden convertirse en víctimas de ingeniería social o de otros métodos de ataque. Es esencial que la entidad implemente medidas de seguridad adecuadas, como la encriptación de datos, la gestión adecuada de contraseñas, el control de acceso y la autenticación de usuarios, así como la revisión regular de los procesos y procedimientos de seguridad. Además, la formación del personal sobre ciberseguridad es fundamental para garantizar la protección adecuada de la

información almacenada. La entidad también debe realizar pruebas de penetración regulares para identificar posibles vulnerabilidades y tomar medidas preventivas y correctivas

1.2.Antecedentes investigativos

Después de una recopilación y análisis de distintas fuentes bibliográficas realizadas por investigadores en distintas Universidades del País hasta el momento se han tomado de referencias los siguientes proyectos.

Según Julio Javier [7], indican formas para reducir las vulnerabilidades en la infraestructura de los sistemas. Concluyeron que la búsqueda semiautomática a través de la implementación de bots, mejora la velocidad de detección de potenciales ataques y vulnerabilidades que pueden ser fácilmente detectadas y aprovechadas por los atacantes.

Según, Mendoza de los Santos [8] menciona que para poder mejorar las prácticas de seguridad propone la implementación de nuevas políticas, que sean capaces de mejorar y aumentar la seguridad de los sistemas mediante la correcta aplicación de dichas normas.

En el artículo de Jadidi y Lu [9], concluyeron que el proceso Threat Hunting mejora la seguridad en entornos críticos aplicando diferentes técnicas dependiendo de la necesidad de la organización y su aplicación ayuda a comprender las actividades de una red. Adicionalmente, con la ayuda del proceso Proactivo Threat Hunting se puede reconocer características de las amenazas e identificar el comportamiento de éstas. La gran variedad de opciones y acciones que se pueden realizar en los diferentes escenarios a los que se enfrente este proceso beneficia en gran medida la capacidad de respuesta.

En el paper de M. R. Fatemi, A. A. Ghorbani, y J. J. McNally [10]. Se concluye que los registros en host son una fuente importante de información, que se puede usar para analizar el comportamiento de las diferentes anomalías y amenazas que se encuentren en la infraestructura de red y que el uso de herramientas para el monitorio de la red es muy útil para poder registrar todos los datos y así definir los patrones y características que se necesiten para la posterior identificación de una posible amenaza. Cuando ya se tienen claras las características de las diferentes anomalías, es posible el diseñar e implementar un motor de detección

de anomalías con ayuda de la información recopilada del registro de los *Sysmon* generado por Windows y con conjuntos de datos que contengan las características que podrán ser reconocidas por el motor de detección de anomalías.

1.3. Fundamentación Teórica

1.3.1. Método de mitigación Threat Hunter:

Es un proceso de búsqueda proactivo e iterativo que identifica la actividadanormal en servidores y redes que pueden reconocerse como una amenaza parar los sistemas [9]. La seguridad y la integridad de la información es su principal objetivo. El proceso Threat Hunting se realiza utilizando diferentes medidas de seguridad y diversas herramientas según requiera la estructura de red [11].

El método de mitigación Threat Hunter, se basa en los principios de la ciberseguridad y la detección temprana de amenazas [10]. En particular, se enfoca en la detección proactiva, en lugar de esperar a que un ataque ocurra para entonces tomar medidas. Además, se centra en la identificación de indicadores de compromiso y comportamientos anómalos, para poder identificar y mitigar amenazas antes de que causen daño [11].

1.3.2. Métodos de protección:

Son técnicas para la protección de los sistemas informáticos y la infraestructura de TI. Para mantener la información a salvo de los delincuentes que buscan penetrar en los sistemas con fines principalmente de lucro [2].

Para proteger los sistemas informáticos, existen diversos métodos y herramientas que pueden ser utilizados. Uno de los métodos más importantes es la implementación de políticas y procedimientos de seguridad de la información. Estas políticas y procedimientos establecen las normas y prácticas para el manejo de la información y la protección de los sistemas informáticos. También pueden incluir medidas de control de acceso, monitoreo de actividades y prevención de intrusiones [13].

1.3.3. Arquitectura de TI

La arquitectura de TI se refiere a la estructura, diseño y organización de los sistemas informáticos y de la red de una organización. Esto incluye los

componentes de hardware, software, redes y servicios que se utilizan para gestionar, almacenar y procesar los datos de la organización [12].

La arquitectura de TI es esencial para garantizar que los sistemas informáticos y de red estén optimizados para satisfacer las necesidades de la organización, y para asegurar que la información se almacene y se proteja de manera adecuada. La arquitectura de TI también es importante para garantizar que los sistemas sean escalables y puedan adaptarse a medida que las necesidades de la organización cambian [14].

Existen diferentes enfoques de arquitectura de TI, como la arquitectura orientada a servicios (SOA), la arquitectura de microservicios, la arquitectura de nube, entre otras. Cada enfoque tiene sus propias ventajas y desventajas y se debe seleccionar en función de las necesidades y objetivos de la organización [12].

Según J. M. Hernández-Suárez [14], la arquitectura de TI es fundamental para el éxito de cualquier organización que dependa de la tecnología de la información para el logro de sus objetivos. La arquitectura de TI permite la integración de tecnologías y sistemas, lo que mejora la eficiencia y la productividad, y permite a la organización tomar decisiones informadas basadas en la información disponible.[12]

1.3.4. Análisis de vulnerabilidades

Búsqueda intensiva de los puntos frágiles en las redes, servidores, en pocas palabras todos los elementos involucrados en la arquitectura de TI. Con el propósito de fortalecer dichos puntos débiles para mantener integra la red y la información que este almacenada en dicha red [10].

1.3.5. Robo de información

El robo de información es una actividad ilegal perpetrada contra individuos, empresas o entidades con el propósito de secuestrar datos y utilizarlos con fines lucrativos [1]. Este tipo de ataque se lleva a cabo con el objetivo de obtener acceso no autorizado a información confidencial y, posteriormente, utilizarla para obtener beneficios económicos mediante diversas prácticas delictivas.[11]

1.3.6. Efectividad de los métodos de ciberseguridad

Porcentaje de cumplimiento exitoso o de fallo aplicando una metodología enfocada a la seguridad de la información de una institución o entidad [1].

1.3.7. Integridad de la información

Se refiere a la exactitud y fiabilidad de los datos asegurando que dicha información no podrá ser alterada a conveniencia, ni perdida, ni destruida sea esta de forma intencionada o accidental. También dicha información no debe ser usada por terceros con fines ilegales [6].

1.3.8. Detección y mitigación de ataques informáticos

Identificación y control de ataques de tipo informáticos dentro de una institución con el fin de salvaguardar la información que allí se encuentre y de proteger la estructura de TI para que este ataque no cause daños en dicha infraestructura [12].

1.3.9. La prevención de intrusiones

La prevención de intrusiones (IPS, por sus siglas en inglés) es una técnica de seguridad de la información que se utiliza para detectar y prevenir intrusiones en redes y sistemas informáticos. El IPS utiliza una variedad de técnicas para detectar y bloquear el tráfico malicioso, como la inspección profunda de paquetes (DPI), la detección de anomalías y la correlación de eventos. El objetivo principal de la IPS es proteger los sistemas informáticos de posibles amenazas y prevenir la pérdida de datos críticos [14].

Según M. Al-Shammari [14], el IPS se basa en la identificación y el bloqueo proactivos de los ataques mediante el análisis del tráfico de red en busca de patrones maliciosos. El IPS puede implementarse como un sistema de hardware o software, y se puede configurar para que se integre con otros sistemas de seguridad, como los sistemas de prevención de intrusiones en host (HIPS) y los sistemas de detección de intrusiones (IDS).

1.3.10. Herramientas de detección

Las herramientas de detección son soluciones tecnológicas que se utilizan para identificar posibles amenazas y ataques en la red y los sistemas informáticos. Estas herramientas funcionan mediante la monitorización continua del tráfico de red, el análisis de patrones de comportamiento y la detección de anomalías en el tráfico de red y en los sistemas. Estas herramientas se enfocan en una tarea específica y puede ser implementada de forma independiente o en conjunto con otras herramientas de seguridad [15].

De acuerdo con O. Salazar-García [15], la utilización de herramientas de detección es fundamental en cualquier estrategia de seguridad de la información, ya que permite identificar posibles amenazas y ataques antes de que puedan causar daño a la organización. Además, estas herramientas pueden ser configuradas para enviar alertas en tiempo real, lo que permite a los administradores de seguridad responder de manera inmediata y efectiva a las amenazas detectadas.

1.3.11. Tipos de herramientas de detección

Existen varios tipos de herramientas de detección que se utilizan en seguridad informática [16]. Entre las cuales se pueden destacar:

- **Sistemas de detección de intrusiones (IDS, por sus siglas en inglés):** son herramientas que monitorean la red en busca de patrones de tráfico y comportamientos anómalos que puedan indicar un intento de intrusión o ataque [16].
- **Sistemas de prevención de intrusiones (IPS, por sus siglas en inglés):** son herramientas que no solo detectan, sino que también previenen los intentos de intrusión mediante la adopción de medidas de seguridad proactivas, como bloquear el tráfico de red malicioso [16].
- **Herramientas de análisis de vulnerabilidades:** son herramientas que identifican y evalúan las vulnerabilidades en los sistemas informáticos, aplicaciones y redes [16].
- **Herramientas de escaneo de puertos**: son herramientas que escanean los puertos de la red para detectar servicios y aplicaciones que podrían ser

vulnerables a ataques [16].

- **Herramientas de análisis de tráfico**: son herramientas que analizan el tráfico de red para identificar patrones y anomalías que puedan indicar actividades maliciosas [16].
- **Herramientas de análisis de registros (logs):** son herramientas que analizan los registros de eventos de los sistemas informáticos y las aplicaciones para detectar patrones y anomalías que puedan indicar actividad maliciosa [16].
- **Herramientas de detección de malware:** son herramientas que detectan la presencia de software malicioso en los sistemas informáticos y las redes [16].

1.4.Objetivos

1.4.1. Objetivo general

Generar un manual de aplicación del proceso Threat Hunting para la detección de vulnerabilidades y contramedidas en la infraestructura de red del Cuerpo de Bomberos de Ambato.

1.4.2. Objetivos específicos

- Recolectar información relevante en los sistemas de seguridad sobre las posibles amenazas que se puedan encontrar.
- Identificar patrones en las amenazas y anomalías que se hayan encontrado en la infraestructura de red.
- Planificar y ejecutar una contramedida con el uso de diferentes técnicas aplicando la metodología del proceso Threat Hunting dependiendo de las necesidades de la infraestructura de red.
- Documentar el proceso que se realice en la contramedida aplicada y los resultados que se obtengan

CAPÍTULO II.- METODOLOGÍA

2.1. Materiales

Para el desarrollo del presente proyecto de investigación se manejaron dos encuestas, las cuales se realizaron tomando en cuenta el rol del personal en la institución.

2.1.1. Encuesta dirigida al personal de TI del CBA.

¿Cómo calificaría el nivel de seguridad dentro de la organización?

- □ Excelente
- □ Bueno
- □ Regular
- □ Malo
- □ Pésimo

¿Ha sido víctima de ataques informáticos dentro de la organización?

- □ Si
- □ No

¿Qué tan frecuente considera que los ataques cibernéticos son una amenaza constante dentro de la organización?

- □ Todo el tiempo
- □ Frecuentemente
- □ Regularmente
- □ Casi nunca
- □ Nunca

¿Considera que la institución tiene sistemas de seguridad adecuados para detectar y prevenir amenazas de seguridad?

- □ Muy adecuados
- □ Adecuados
- □ Neutro
- □ Inadecuados

Muy inadecuados

¿Cree necesaria la implementación de un nuevo proceso de seguridad de la formación dentro de la organización?

□ Muy necesaria

□ Necesaria

□ Neutral

□ Poco necesaria

□ Innecesaria

¿Qué herramientas o sistemas de seguridad utiliza actualmente para detectar y prevenir amenazas de seguridad en su organización?

□ Avanzados

□ Básicos

□ No sabe

□ Ninguno

¿Está de acuerdo con la implementación del proceso Threat Hunting dentro de la institución?

□ Totalmente de acuerdo

□ De acuerdo

□ Neutral

□ En desacuerdo

□ Totalmente en desacuerdo

¿Conoces el proceso proactivo de detección de amenazas (Threat Hunting) y su importancia para la seguridad de la información?

□ Soy experto en el tema

□ Conozco bastante sobre su importancia

□ Conozco algo sobre su importancia

□ Escuchado algo, pero no estoy seguro de su importancia específica

□ Nunca había escuchado del tema

¿En qué medida cree que la implementación del proceso Threat Hunting es compatible con la estrategia general de seguridad de la organización?

□ Totalmente compatible

□ Compatible

□ Neutral

□ Incompatible

□ Totalmente incompatible

¿Cómo cree que afectaría la implementación del proceso Threat Hunting a los procesos actuales de seguridad de la organización?

□ Positivamente a gran escala

□ Positivamente

□ No afectaría

□ Negativamente

□ Negativamente a gran escala

2.1.2 Encuesta dirigida al resto de funcionarios del CBA.

¿Cree que la seguridad de la información es importante para la organización?

□ Totalmente de acuerdo

□ De acuerdo

□ Ni de acuerdo ni en desacuerdo

□ En desacuerdo

□ Totalmente en desacuerdo

¿Conoce los riesgos a los que está expuesta la empresa en cuanto a seguridad de la información?

□ Soy experto en seguridad de la información

□ Conozco muchos riesgos

□ Conozco algunos riesgos

□ Escuchado algo, pero no estoy seguro de los riesgos específicos

□ Nunca había escuchado del tema

¿Cree que la empresa debería implementar medidas de seguridad proactivas para prevenir ataques cibernéticos?

□ Totalmente de acuerdo

□ De acuerdo

□ Ni de acuerdo ni en desacuerdo

□ En desacuerdo

□ Totalmente en desacuerdo

¿Considera que los empleados de la empresa están capacitados para reconocer amenazas de seguridad en línea?

□ No estoy seguro

□ No, no están capacitados

□ Algunos están capacitados

□ La mayoría está capacitada

□ Todos están capacitados

¿Qué tan seguido recibe información o capacitación acerca de seguridad de la información?

□ Nunca

□ Casi nunca

□ A veces

□ Frecuentemente

□ Siempre

¿Cree que las medidas de seguridad de la información en la empresa son adecuadas?

□ Totalmente inadecuadas

□ Inadecuadas

□ Ni adecuadas ni inadecuadas

□ Adecuadas

□ Totalmente adecuadas

¿Cómo calificaría la importancia de la seguridad de la información en su trabajo diario?

□ Muy poco importante

□ Poco importante

□ Neutral

□ Importante

□ Muy importante

¿Cree que la empresa debería invertir más recursos en seguridad de la información?

□ Totalmente de acuerdo

□ De acuerdo

□ Ni de acuerdo ni en desacuerdo

□ En desacuerdo

□ Totalmente en desacuerdo

¿Conoce el proceso proactivo de detección de amenazas (Threat Hunting) y su importancia para la seguridad de la información?

□ Soy experto en el tema

□ Conozco bastante sobre su importancia

□ Conozco algo sobre su importancia

□ Escuchado algo, pero no estoy seguro de su importancia específica

□ Nunca había escuchado del tema

¿Cree que los procesos de seguridad de la información afectan negativamente la productividad en la empresa?

□ Totalmente en desacuerdo
□ En desacuerdo
□ Ni de acuerdo ni en desacuerdo
□ De acuerdo
□ Totalmente de acuerdo

2.2. Métodos

2.2.1. Modalidad de la Investigación

La presente investigación se contextualizó en la modalidad de investigación de campo y bibliográfica-documental.

Investigación de Campo: Se considera esta modalidad ya que el investigador acudirá a la entidad en cuestión para recopilar información por medio de

entrevistas, encuestas y la ejecución de los procesos con respecto al análisis del problema en conjunto con el personal involucrado en el tema.

Investigación bibliográfica – documental: debido a que la información recopilada en revistas, tesis del área informática, artículos y leyes existentes servirán como apoyo para el fundamento teórico y posterior ejecución del proceso Threat Hunting.

2.2.2. Población y muestra

La población se dividirá en dos sectores los cuales son: Administradores de TI, funcionarios miembros de la organización que posean una computadora y forman parte de la red.

Administradores de TI

Tabla 1: Población de Estudio

Población	**Número**	**Porcentaje**
Gerente de TI	1	33.33%
Gerente de Telecomunicaciones	1	33.33%
Asistente de TI	1	33.33%
Total	**3**	**100%**

Elaborado por: Investigador

Funcionarios Públicos

Tabla 2: Población de los funcionarios públicos

Población	**Número**	**Porcentaje**
Funcionarios públicos miembros de la organización	53	100%
Total	**53**	**100%**

Elaborado por: Investigador

2.2.3. Recolección de la Información

Para aplicar el formulario al personal de la institución, se utilizó Google forms, debido a que el alcance y tabulación son facilitadas mediante la misma plataforma.

Pregunta Nro.1: ¿Cómo calificaría el nivel de seguridad dentro de la organización?

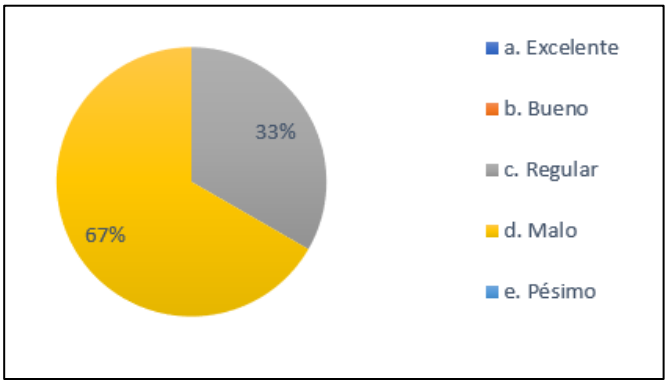


Gráfico 1: Encuesta al personal de TI, pregunta 1

Elaborado por: Investigador

Análisis e interpretación de los resultados

Después de recopilar los datos de la encuesta, se observa en el ***Gráfico 1*** que el 67% de las personas encuestadas considera que el nivel de seguridad de la institución es "malo", mientras que el 33% lo califica como "regular". Estos resultados indican que la mayoría de los encuestados perciben la seguridad en la institución como deficiente. Esta interpretación sugiere que existe una preocupación generalizada acerca de la condición actual de la seguridad en la institución.

Pregunta Nro.2: ¿Como calificaría el nivel de seguridad dentro de la organización?

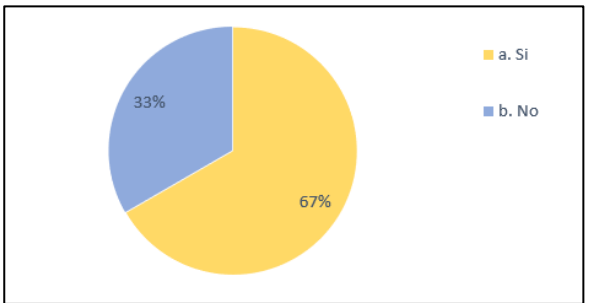


Gráfico 2:Encuesta al personal de TI, pregunta 2

Elaborado por: Investigador

Después de realizar la encuesta y analizar los resultados representados en el ***Gráfico 2,*** se observa que el 67% de los encuestados si ha sido víctima de los ataques dentro de la institución, mientras que el 33% no ha sido víctima de los ataques dentro de la institución. Esta proporción sugiere que hay una alta tasa de vulnerabilidad y exposición a los ataques en la institución, destacando también que los sistemas de seguridad actuales son insuficientes para proteger a los usuarios y clientes de la institución

Pregunta Nro.3: ¿Qué tan frecuente considera que los ataques cibernéticos son una amenaza constante dentro de la organización?

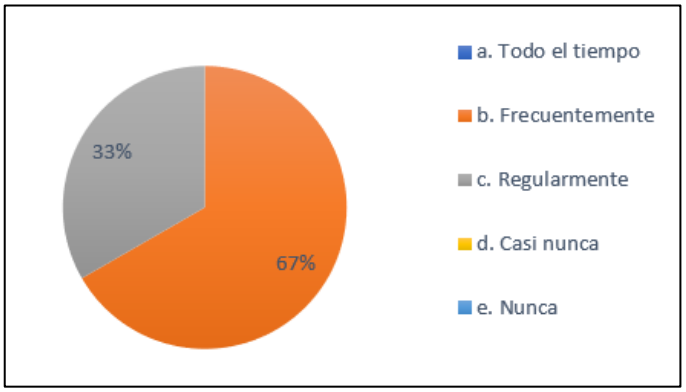


Gráfico 3: Encuesta al personal de TI, pregunta 3

Elaborado por: Investigador

De acuerdo los resultados que están representados en el ***Gráfico 3***, Se puede notar que el 67% de las personas que fueron encuestadas consideran que los ataques cibernéticos son una amenaza frecuente para la institución, por otro lado, el 37% lo consideran una amenaza regular. Concluyendo así que las amenazas cibernéticas si son un riesgo para la institución.

Pregunta Nro.4: ¿Considera que la institución tiene sistemas de seguridad adecuados para detectar y prevenir amenazas de seguridad?

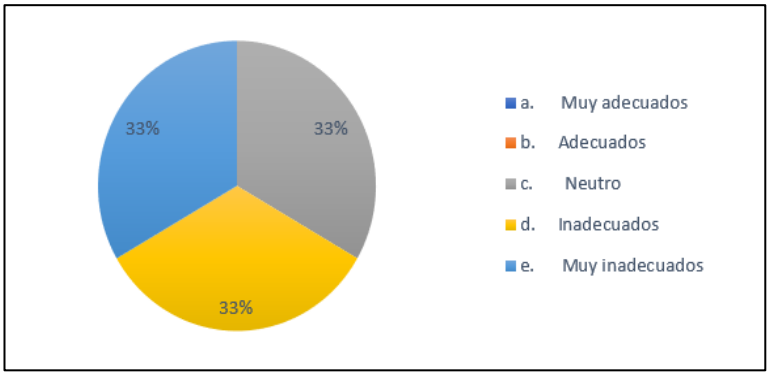


Gráfico 4: Encuesta al personal de TI, pregunta 4

Elaborado por: Investigador

Basándonos en los resultados representados en el ***Gráfico 4***, se destaca una preocupante percepción por parte de las personas encuestadas en relación con los sistemas de seguridad. Según los datos recopilados, el 33% de los encuestados considera que estos sistemas son neutrales, otro 33% los califica como inadecuados y, alarmantemente, el restante 33% los percibe como muy inadecuados. Estas cifras sugieren que existe una brecha significativa en la efectividad de las medidas de seguridad para detectar y prevenir amenazas potenciales. Es fundamental abordar esta problemática y mejorar la infraestructura de seguridad para garantizar una protección sólida frente a los riesgos de seguridad.

Pregunta Nro.5: ¿Cree necesaria la implementación de un nuevo proceso de seguridad de la formación dentro de la organización?

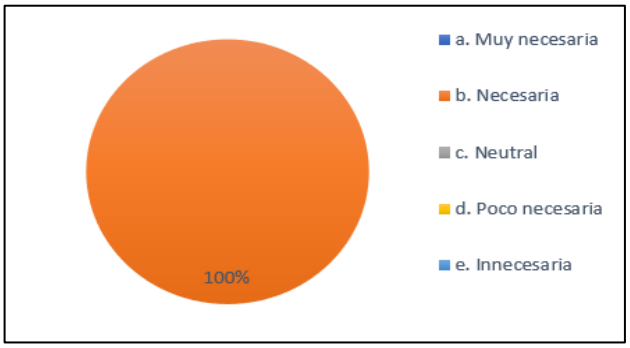


Gráfico 5: Encuesta al personal de TI, pregunta 5

Elaborado por: Investigador

De acuerdo con el ***Gráfico 5*** en el cual están representados los resultados obtenidos de la encuesta**,** se denota que el 100% del personal piensa que es necesaria la implementación de nuevas medidas de seguridad. Con esto se llega a la conclusión de que el personal de TI necesita de nuevas tecnologías y herramientas para salvaguardar la integridad de la red.

Pregunta Nro.6: ¿Qué herramientas o sistemas de seguridad utiliza actualmente para detectar y prevenir amenazas de seguridad en su organización?

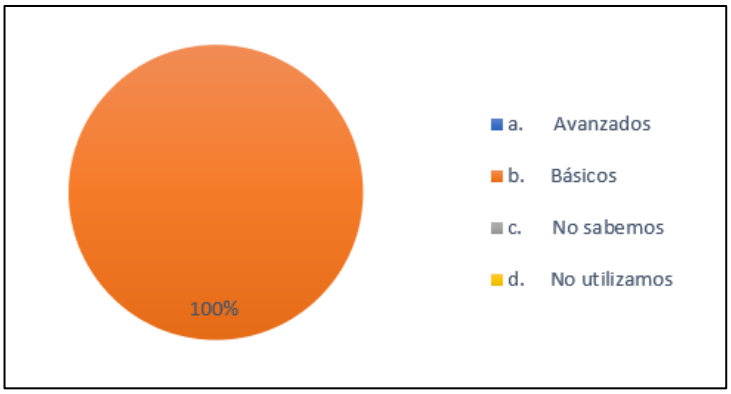


Gráfico 6: Encuesta al personal de TI, pregunta 6

Elaborado por: Investigador

Al analizar los resultados presentados en el ***Gráfico 6***, se evidencia que el 100% de las personas encuestadas considera que las herramientas y sistemas de

seguridad utilizados son básicos. A partir de esta constatación, se concluye que las herramientas actuales carecen de un nivel de sofisticación necesario, lo cual las hace susceptibles de ser vulneradas con relativa facilidad.

Pregunta Nro.7: ¿Conoce el proceso proactivo de detección de amenazas (Threat Hunting) y su importancia para la seguridad de la información?

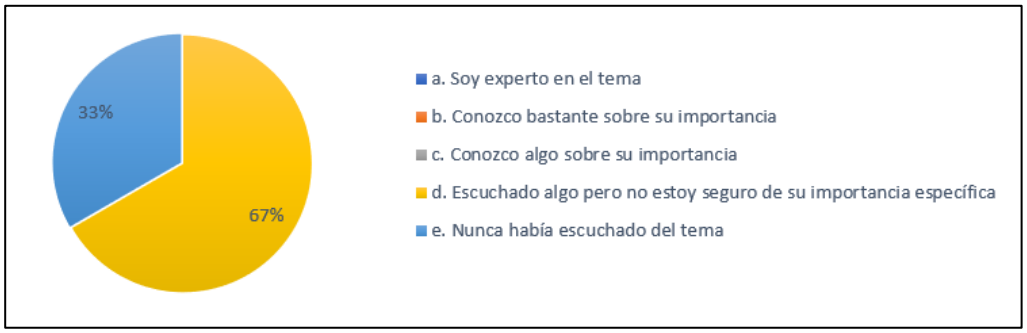


Gráfico 7: Encuesta al personal de TI, pregunta 7

Elaboradopor: Investigador

Con base en los resultados presentados en el ***Gráfico 7***, se puede observar que el 67% del personal encuestado ha escuchado hablar del proceso de Threat Hunting, aunque no está seguro de su importancia en la seguridad cibernética. Por otro lado, el 33% restante del personal no ha tenido conocimiento ni información sobre este tema. Estos resultados revelan que el personal posee un nivel de conocimiento limitado acerca del proceso de Threat Hunting y su relevancia en la protección contra amenazas cibernéticas.

Para abordar esta falta de conocimiento, se recomienda implementar medidas que promuevan la concienciación y la capacitación sobre el proceso de Threat Hunting. Esto podría incluir la realización de talleres, sesiones de formación o la incorporación de material educativo para que el personal pueda comprender mejor la importancia y los beneficios de esta práctica en la seguridad de la organización. Al fortalecer el entendimiento del personal acerca del Threat Hunting, se puede mejorar la capacidad de detección y respuesta ante posibles amenazascibernéticas.

Pregunta Nro.8: ¿Está de acuerdo con la implementación del proceso Threat Hunting dentro de la institución?

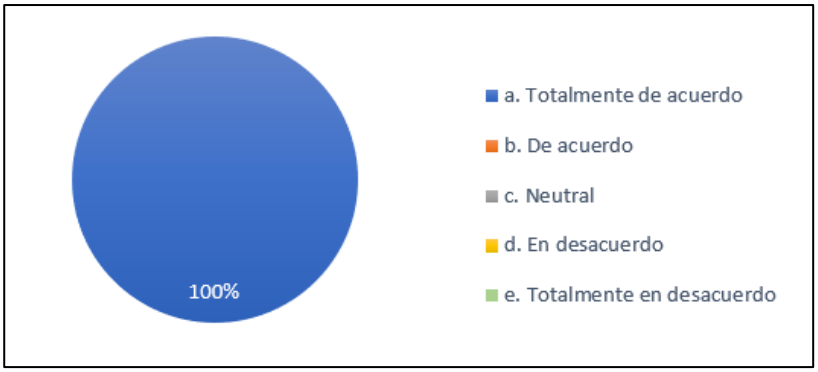


Gráfico 8: Encuesta al personal de TI, pregunta 8

Elaborado por: Investigador

De acuerdo con los resultados obtenidos y representados en el ***Gráfico 8***, se observa que el 100% de los encuestados están totalmente de acuerdo en implementar el proceso Threat Hunting. Concluyendo así que la entidad requiere de nuevas medidas de seguridad.

Pregunta Nro.9: ¿En qué medida cree que la implementación del proceso Threat Hunting es compatible con la estrategia general de seguridad de la organización?

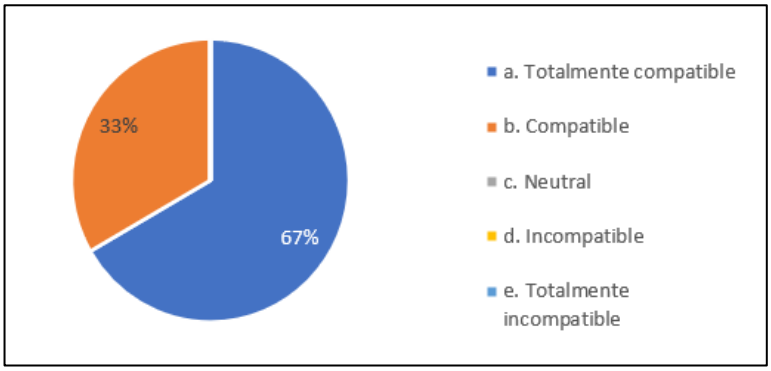


Gráfico 9: Encuesta al personal de TI, pregunta 9

Elaborado por: Investigador

De acuerdo con los resultados obtenidos y representados en el ***Gráfico 9,*** se observa que el 67% de los encuestados consideran que el proceso Threat Hunting es totalmente compatible para ser implementado dentro de la institución, mientras

que, el 33% lo considera compatible. Concluyendo así que los encargados del departamento de TI están seguros de que la infraestructura de red de la institución es compatible con el proceso Threat Hunting.

Pregunta Nro.10: ¿Cómo cree que afectaría la implementación del proceso Threat Hunting a los procesos actuales de seguridad de la organización?

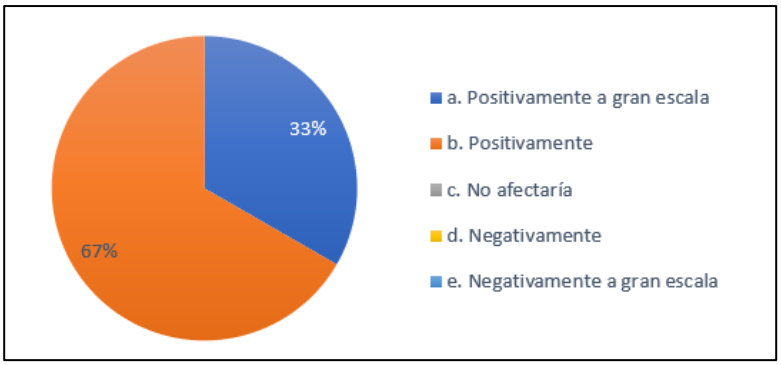


Gráfico 10: Encuesta al personal de TI, pregunta 10

Elaborado por: Investigador

Con los datos obtenidos representados en el ***Gráfico 10***, se puede notar que el 67% de los encargados los cuales fueron encuestados respondieron que la implementación del proceso afectara positivamente a la institución, por otro lado, el 33% consideraron que afectará positivamente a gran escala. Con esto se concluye que la correcta implementación del método podría traer efectos positivos a la entidad.

ENCUESTA DIRIGIDA A LOS FUNCIONARIOS DEL CBA.

Pregunta Nro.1: ¿Cree que la seguridad de la información es importante para la institución?

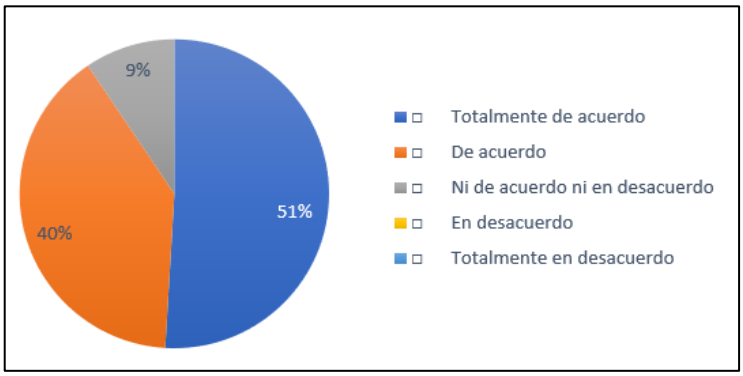


Gráfico 11: Encuesta a los funcionarios del CBA, pregunta 1

Elaborado por: Investigador

Según los resultados del ***Gráfico 11***, se destaca que el 51% de las personas encuestadas están totalmente de acuerdo en que la seguridad de la red es de gran importancia para la institución. Además, un 40% de los encuestados están de acuerdo, mientras que solo un 9% no expresó una postura clara. Estos resultados indican que la mayoría de los funcionarios del CBA son conscientes de la importancia crucial de la seguridad en la red para la institución.

Pregunta Nro.2: ¿Conoce los riesgos a los que está expuesta la empresa en cuanto a seguridad de la información?

Gráfico 12: Encuesta a los funcionarios del CBA, pregunta 2

Elaborado por: Investigador

En los resultados obtenidos representados en el ***Gráfico 12***, se puede observar que el 49% de los encuestados conocen los riesgos a los que están expuestos en caso de un ataque cibernético, por otro lado, el 30% no saben nada al respecto, el 13% del personal ha escuchado del tema, pero no conoce los riesgos, y el 8% conoce algunos de los riesgos mas no son conscientes de los riesgos. Con esto se concluye que la mayoría de los funcionarios saben de lo riesgoso y peligroso que puede ser un ataque. Sin embargo, el resto de los funcionarios no saben nada con respecto a la seguridad de la red.

Pregunta Nro.3: ¿Cree que la empresa debería implementar medidas de seguridad proactivas para prevenir ataques cibernéticos?

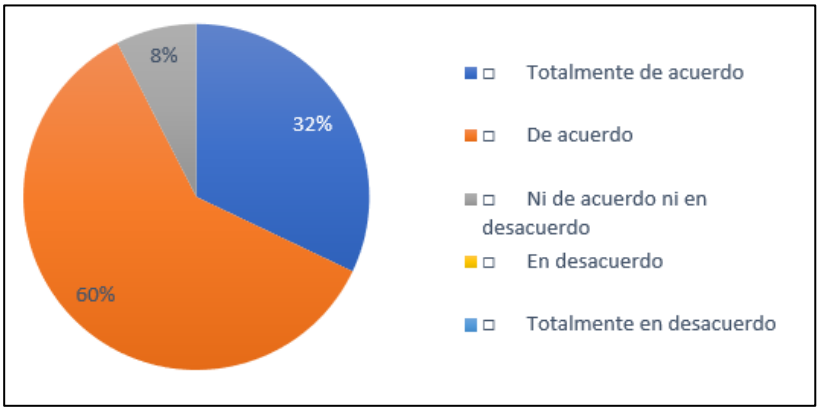


Gráfico 13:Encuesta a los funcionarios del CBA, pregunta 3

Elaborado por: Investigador

De acuerdo con los resultados que se pueden observar en el ***Gráfico 13***, se destaca que el 60% de los encuestados está de acuerdo en implementar nuevas medidas de seguridad con el fin de fortalecerlas. Además, el 32% de los encuestados está totalmente de acuerdo con la implantación de estas medidas de seguridad, mientras que el 8% mantiene una postura neutral. En conclusión, la mayoría del personal sometido a la encuesta apoya la implementación de nuevas medidas de seguridad.

Pregunta Nro.4: ¿Considera que los empleados de la empresa están capacitados para reconocer amenazas de seguridad en línea?

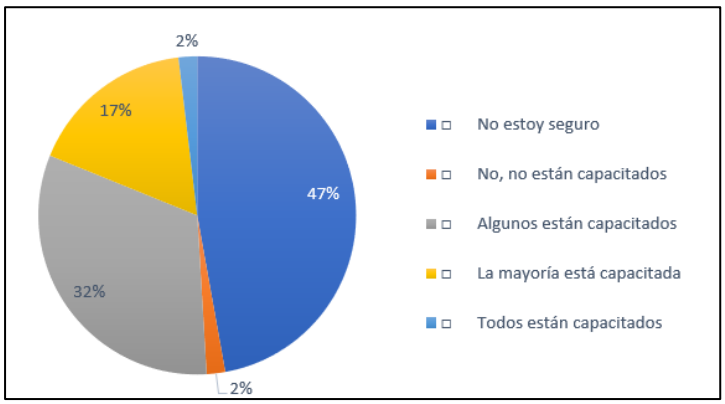


Gráfico 14: Encuesta a los funcionarios del CBA, pregunta 4

Elaborado por: Investigador

Según el ***Gráfico 14***, que refleja los resultados de la encuesta, se destaca que el 47% de los encuestados no está seguro de que los empleados del departamento de TI estén capacitados para reconocer las amenazas dentro de la institución. Por otro lado, el 32% piensa que algunos están capacitados, el 17% considera que la mayoría de los empleados están capacitados, el 2% baraja la idea de que los empleados no están capacitados y el 2% restante no está seguro de su nivel de capacitación. Esto indica que existe incertidumbre entre los funcionales acerca de la capacitación de los encargados de TI en cuanto a la seguridad. Sin embargo, es importante destacar que una gran parte de ellos considera que la mayoría de los integrantes del departamento de TI están capacitados, mientras que el resto opina que no lo están. En resumen, se puede concluir que, aunque hay cierta incertidumbre sobre la capacitación del personal de TI en la detección de amenazas, una parte considerable de los encuestados confía en que la mayoría de los empleados del departamento de TI están capacitados en este aspecto.

Pregunta Nro.5: ¿Qué tan seguido recibe información o capacitación acerca de seguridad de la información?

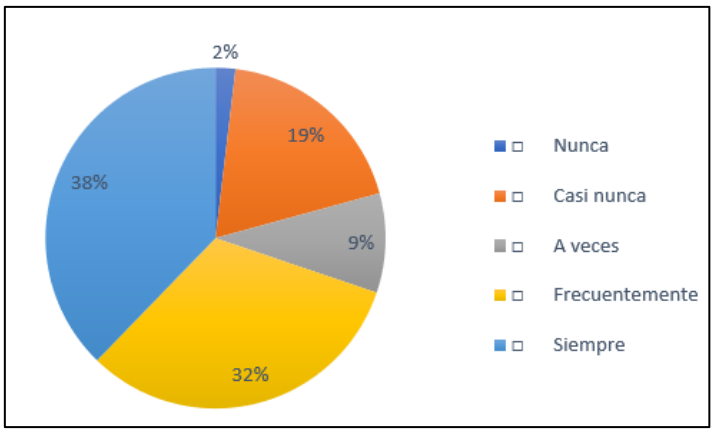


Gráfico 15: Encuesta a los funcionarios del CBA, pregunta 5

Elaborado por: Investigador

Los resultados obtenidos representados en el ***Gráfico 15***, dan a denotar que 38% de los funcionarios siempre reciben capacitaciones sobre la seguridad de la información, mientras que el 32% la reciben frecuentemente, un 19% del personal casi nunca reciben capacitaciones, el 9% lo recibe a veces y un 2% nunca ha recibido capacitaciones. Con esto se da entender que gran parte del personal del CBA si reciben capacitaciones sobre la seguridad de la información, aunque para algunos no sean tan seguidas dichas capacitaciones.

Pregunta Nro.6: ¿Crees que las medidas de seguridad de la información en la empresa son adecuadas?

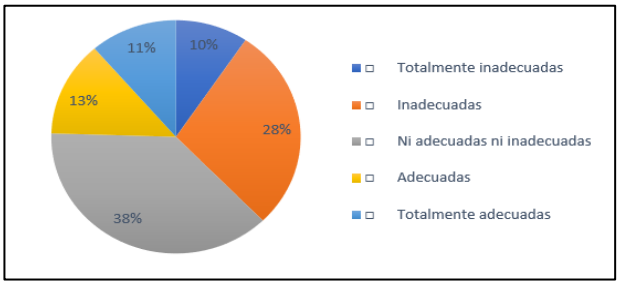


Gráfico 16: Encuesta a los funcionarios del CBA, pregunta 6

Elaborado por: Investigador

De acuerdo con el ***Gráfico 16***, el cual representa los resultados de la encuesta, el 38% de los empleados son neutrales al calificar las medidas de seguridad en la información designándoles que ni son adecuadas ni inadecuadas, el 28% las califican como inadecuadas, el 13% las considera adecuadas, el 11% piensa que las medidas de seguridad son totalmente adecuadas y el 10% las denomina como totalmente inadecuada. Concluyendo con que el personal del CBA no consideran como adecuadas las actuales medidas de seguridad en la empresa.

Pregunta Nro.7: ¿Cómo calificaría la importancia de la seguridad de la información en su trabajo diario?

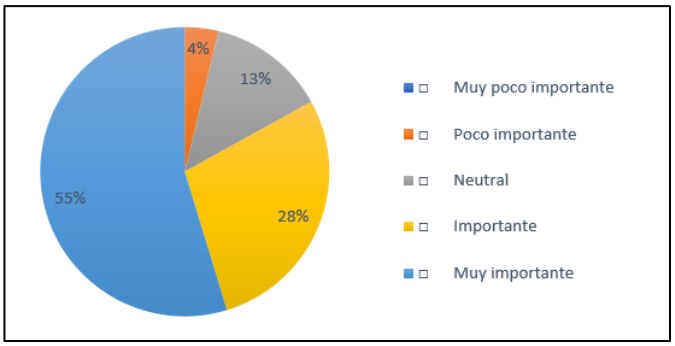


Gráfico 17: Encuesta a los funcionarios del CBA, pregunta 7

Elaborado por: Investigador

De acuerdo con los resultados obtenidos y mostrados en el ***Gráfico 17***, se observa que el 55% de los funcionarios del CBA califican la importancia de la seguridad en su trabajo diario como “muy importante”, el 28% lo definen como importante, el 13% son neutrales en sus respuestas y el 4% no lo consideran

importantes. Concluyendo que, salvo algunas excepciones para la mayor parte del personal del CBA la seguridad de la información en su trabajo diario es importante y hay que salvaguardarla.

Pregunta Nro.8: ¿Crees que la empresa debería invertir más recursos en seguridad de la información?

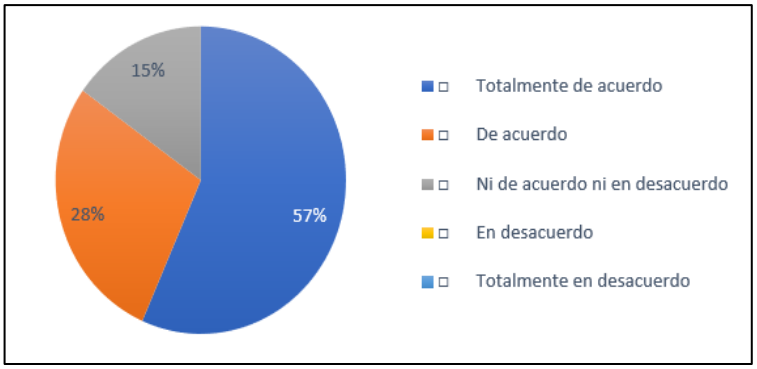


Gráfico 18: Encuesta a los funcionarios del CBA, pregunta 8

Elaborado por: Investigador

En los resultados que se representan en el ***Gráfico 18***, el 57% de los encuestados están totalmente de acuerdo en que se deben invertir más recursos monetarios en la mejora de la seguridad de la información, mientras el 28% del personal están de acuerdo y el 15% no están ni de acuerdo ni en desacuerdo. Concluyendo así que el personal del CBA se preocupa de la seguridad de la información y de la integridad de la red.

Pregunta Nro.9: ¿Conoce el proceso proactivo de detección de amenazas (Threat Hunting) y su importancia para la seguridad de la información?

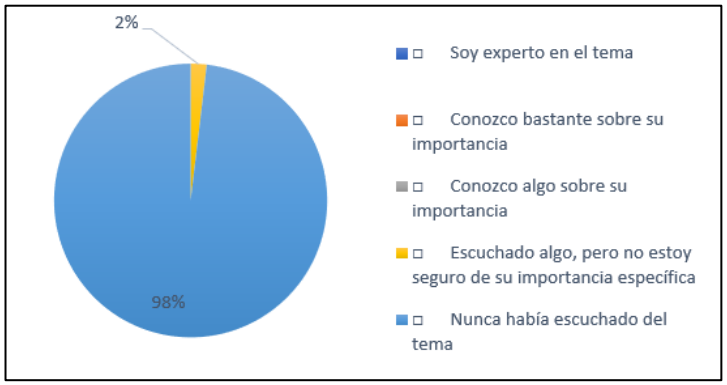


Gráfico 19: Encuesta a los funcionarios del CBA, pregunta 9

Elaborado por: Investigador

Según los resultados mostrados en el ***Gráfico 19***, se observa que el 98% del personar nunca ha escuchado del proceso proactivo de amenazas y el 2% ha escuchado de dicho proceso más no está seguro de su importancia. Concluyendo así que el personal no conoce ni sabe de la funcionalidad del proceso Threat Hunting.

Pregunta Nro.10: ¿Cree que los procesos de seguridad de la información afectan negativamente la productividad en la empresa?

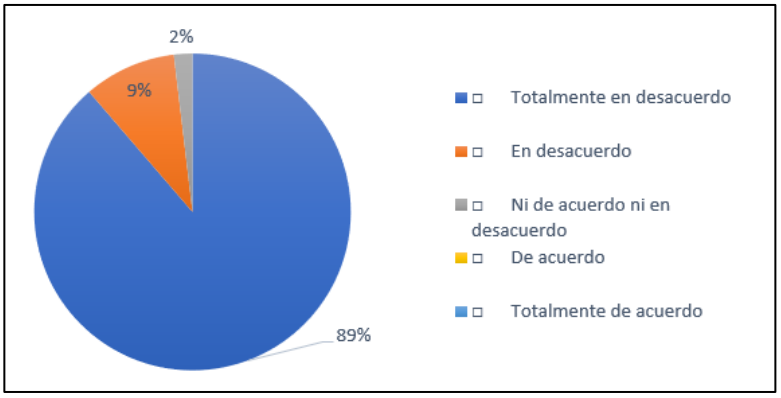


Gráfico 20: Encuesta a los funcionarios del CBA, pregunta 10

Elaborado por: Investigador

Según los resultados obtenidos reflejados en el ***Gráfico 20***, dan a denotar que el 89% del personal cree que la implantación del proceso no tendrá resultados negativos dentro de la institución, mientras que, el 9% están en desacuerdo a que el proceso conlleve consecuencias negativas, y el 2% es neutral en su respuesta.

Concluyendo así que el personal acepta de buena manera la propuesta de implementar un proceso proactivo dentro de la institución para fortalecer la seguridad de la información.

CAPÍTULO III.- RESULTADOS Y DISCUSIÓN

3.1. Análisis y discusión de los resultados

3.1.1. Análisis de la herramienta de monitoreo.

Se realizó un análisis de las herramientas de monitoreo para determinar la más adecuada para el entorno de red como se detalla en la tabla 3.

Tabla 3:Análisis de las herramientas de monitoreo[17-26]

Herramienta	Descripción	Actividad
Wireshark	Wireshark es una herramienta de análisis de protocolos de red de código abierto ampliamente utilizada.	Captura y analiza el tráfico de red en tiempo real y también permite abrir archivos de captura previamente guardados para su análisis.
Nmap	Nmap es una herramienta opensource multiplataforma enfocada en la ciberseguridad de las redes.	Obtiene información como resultado del escaneo de red y de los puertos
OpenVAS	OpenVAS es una herramienta de escaneo de vulnerabilidades de código abierto que ofrece un conjunto completo de funciones para evaluar la seguridad de sistemas y redes.	OpenVAS ofrece una amplia gama de capacidades que abarcan tanto pruebas autenticadas como no autenticadas. Puede realizar escaneos en varios protocolos industriales y de Internet, ya sean de alto o bajo nivel.
Nessus	Nessus es un software de escaneo de vulnerabilidades de la infraestructura de red, compatible con múltiples plataformas.	Nessus consta de dos componentes principales: nessusd y Nessus cliente. Nessusd es el demonio o servicio que se ejecuta en el sistema objetivo y realiza el escaneo de vulnerabilidades.
Metasploit	Metasploit es una conocida plataforma de pruebas de penetración y desarrollo de exploits utilizada por profesionales de la seguridad y hackers éticos.	Metasploit proporciona un conjunto completo de herramientas y recursos para descubrir vulnerabilidades, desarrollar exploits y llevar a cabo pruebas de penetración en sistemas y redes.

OSSEC	OSSEC (Open Source Security) es un sistema de detección de intrusiones de código abierto que se utiliza para monitorear y analizar la seguridad de sistemas y redes.	Proporciona una amplia gama de funciones de seguridad, incluyendo la detección de intrusiones, la prevención de ataques y la gestión de registros.
Suricata	Suricata es un motor de detección y prevención de intrusiones de red de código abierto y basado en reglas. Se utiliza para analizar el tráfico de red en busca de patrones y comportamientos maliciosos, y puede detectar y prevenir una amplia gama de amenazas y ataques.	Proporciona una capa adicional de protección al analizar y detectar actividades maliciosas en tiempo real, lo que ayuda a prevenir ataques y reducir el tiempo de respuesta a incidentes de seguridad.

Elaborado por: El investigador

Ventajas y desventajas

Tabla 4: Ventajas y desventajas de las herramientas

Herramienta	Ventajas	Desventajas
Wireshark	- Amplia compatibilidad y soporte para una amplia variedad de protocolos de red ¨[17].	- Interfaz gráfica compleja para usuarios no técnicos [17].
Nmap	- Escaneo rápido y eficiente de redes y puertos [18].	- Requiere conocimientos técnicos avanzados para su configuración y uso [18].
OpenVAS	- Escaneo de vulnerabilidades completo y exhaustivo [19].	- Puede generar falsos positivos y requiere configuración adecuada para un análisis preciso [19]
Nessus	- Amplia base de datos de vulnerabilidades y escaneos eficientes [20].	- Versión gratuita limitada en funcionalidades y uso para uso comercial [20].
Metasploit	- Amplio conjunto de herramientas y exploits para pruebas de penetración [21].	- Requiere conocimientos técnicos avanzados para su configuración y uso [21].
OSSEC	- Monitoreo de intrusiones en tiempo real y capacidad de respuesta automatizada [22].	- Configuración inicial y ajustes pueden ser complejos para usuarios no técnicos [22].
Suricata	- Detección y prevención de intrusiones en tiempo real con reglas personalizables [23].	- Requiere recursos de hardware significativos para un rendimiento óptimo [23].

Advanced IP Scanner	- Escaneo rápido y detallado de dispositivos en la red local [24].	- Limitado a la detección de dispositivos en la red local, no es adecuado para escaneos de red más amplios [24].
Snort	- Detección en tiempo real de intrusiones y ataques en la red [25].	- Requiere configuración y mantenimiento constantes para mantenerse actualizado con las amenazas actuales [25].
Burp Suite	- Amplias capacidades de prueba de seguridad de aplicaciones web y detección de vulnerabilidades [26].	- Versión gratuita limitada en funcionalidades y uso para uso comercial [26].

Elaborado por: El investigador

El análisis realizado en las ***Tablas 3*** y ***4***, permitió seleccionar las herramientas Wireshark, Nessus y Advanced IP Scanner para la evaluación de tráfico y para la captura de paquetes y escaneo de la red, lo que permite identificar actividad sospechosa y vulnerabilidades para un posterior análisis de las actividades encontradas.

3.1.2. Elementos de la red

La red, se considera como una red pequeña que cuenta con 17 host dispositivos finales, de los cuales 14 son computadoras de escritorio. La red incluye un Firewall modelo FortiGate 300E y sus características se muestran en la ***Tabla 5,*** además de dos switches y un router sus características se muestran en la ***Tabla 6, 7 y 8*** respectivamente.

Tabla 5: Características de equipos de seguridad

Proveedor	**Fortinet**
Rendimiento de Firewall	Hasta 10 Gbps de rendimiento de firewall
Rendimiento de IPS	Hasta 3 Gbps de rendimiento de prevención de intrusos (IPS)
Rendimiento de IPS	Hasta 4 Gbps de rendimiento de VPN

Puertos	2x puertos WAN 10/100/1000 Mbps 16x puertos LAN 10/100/1000 Mbps 2x puertos SFP+ 10Gbps
Capacidad de VPN	Hasta 5,000 túneles VPN concurrentes
Conexiones simultáneas	Hasta 2 millones de conexiones simultáneas
Seguridad avanzada	Características avanzadas de seguridad, como filtrado de URL, filtrado de aplicaciones, inspección SSL, prevención de intrusiones y más
Direcconamiento IP	Clase C 192.168.1.4
Macara de subred	255.255.255.0
Puerta de enlace	192.168.1.1

Elaborado por: El investigador

El Firewall se ubica en un punto estratégico dentro de la red para poder gestionar la seguridad de los servidores.

Tabla 6: Switch de la Red

Característica	Descripción
Modelo	Cisco SG200-26P
Puertos	26 puertos Ethernet 10/100/1000
PoE (Power over Ethernet)	Sí (Compatible con IEEE 802.3af y 802.3at)
PoE Budget	Hasta 180 W
Capacidad de conmutación	52 Gbps
Rendimiento	Hasta 38.69 Mpps (millones de paquetes por segundo)
VLANs	Admite hasta 256 VLANs

QoS (Calidad de servicio)	Sí (Soporte para 8 colas de prioridad y clasificación basada en 802.1p)
Seguridad	Listas de control de acceso (ACL), autenticación 802.1X, VLAN de invitados, seguridad de puerto
Gestión	Web GUI, línea de comandos (CLI), SNMP v1/v2c/v3, RMON
Montaje	Montaje en rack de 19 pulgadas
Alimentación	Fuente de alimentación interna
Dimensiones (An x Al x Pr)	44.0 cm x 4.4 cm x 25.7 cm

Elaborado por: El investigador

Tabla 7: Switch 2 de la red

Característica	Descripción
Modelo	HP 1920-16G Switch
Puertos	16 puertos Gigabit Ethernet (10/100/1000 Mbps) 2 ranuras de expansión SFP (Small Form-factor Pluggable) para conectividad de fibra óptica
Capacidad de conmutación	32 Gbps
Capacidad de reenvío	23.8 Mpps
VLANs	Admite hasta 64 VLANs VLAN de voz con detección automática de telefonía IP Asignación de VLAN basada en la dirección MAC del cliente
Seguridad	Control de acceso basado en puertos (802.1X) Listas de control de acceso (ACL) Autenticación RADIUS/TACACS+ Detección de bucles y protección STP (Spanning Tree Protocol)

Administración	Interfaz de línea de comandos (CLI)
Dimensiones (An x Al x Pr)	44 cm x 4.4 cm x 24.6 cm
Peso	2.54 kg

Elaborado por: El investigador

Tabla 8: Router de la red

Característica	**Descripción**
Modelo	HP R110 Router
Interfaces de red	4 puertos LAN 10/100 Mbps 1 puerto WAN 10/100 Mbps
Protocolos de enrutamiento	Static Routing RIP v1/v2 IGMP Proxy
Seguridad	Firewall integrado con filtrado de paquetes y prevención de DoS Filtrado de direcciones IP y de MAC VPN (Virtual Private Network) compatible con IPSec
Conectividad inalámbrica	Wi-Fi 802.11b/g/n (opcional)
Antenas	2 antenas internas (en caso de contar con la opción Wi-Fi)
Administración	Interfaz web de administración Soporte para SNMP
Dimensiones (An x Al x Pr)	20.5 cm x 4.5 cm x 12.8 cm
Peso	0.28 kg

Elaborado por: El investigador

VALORACIÓN DE LOS ACTIVOS DE SEGURIDAD

Los sistemas de seguridad son fundamentales en la red por lo que resulta importante valorar cada uno de estos, acorde a la información presentada en las tablas 9, 10, 11, 12 y 13.

En la tabla 9 se valoraron los dispositivos considerados como activos de seguridad y se excluyeron a los dispositivos finales por que se desea una tener una vista únicamente a los sistemas que forman parte de la seguridad de la red

Tabla 9: Activos de los sistemas de seguridad [27].

ACTIVOS DE LOS SISTEMAS DE SEGURIDAD						
Nro. Activo	**Proceso Macro**	**Subproceso**	**Tipo de activo**	**Nombre**	**Descripción del activo**	**Ubicación**
A1	**Apoyo de Tecnologías de la Información**	Infraestructura	Hardware	Routers	conexión entre equipos.	Matriz X-1
A2			Hardware	Firewall Fortigate	Controla los posibles peligros de la red	Matriz X-1
A3		Redes y comunicaciones	Redes	Switch Cisco SG200-26P	Gestiona el paso de paquetes en la Red	Matriz X-1
A4			Redes	Switch HP 1920-16G	Gestiona el paso de paquetes en la red	Matriz X-1
A5		Aplicaciones informáticas	Software	Antivirus	Gestiona la seguridad de los dispositivos	Matriz X-1
A6			Software	Servicio Email Simbra	Servicio que Permite intercambiar Correos electrónicos dentro de la institución.	Matriz X-1
A7		Talento Humano	Personal	Asistente de TI	Personal que brinda soporte	Matriz X-1
A8			Personal	Jefe de TI	Personal encargado de todas las gestiones de TI.	Matriz X-1

Elaborado por: El investigador

Criterios de valoración en términos de Confidencialidad.

Tabla 10: Valoración de términos de Confidencialidad [27].

Confidencialidad	**Criterio**
Alto (3)	La revelación indebida de información tiene un impacto de gran importancia para la institución.
Medio (2)	La revelación indebida de información tiene un impacto limitado para la institución.
Bajo (1)	La revelación indebida de información no tiene un impacto de gran importancia para la institución.

Elaborado por: El investigador

Criterios de valoración en términos de integridad.

Tabla 11: Valoración de términos de integridad [27].

Integridad	**Criterio**
Alto (3)	La eliminación o modificación indebida de información tiene un impacto de gran importancia para la institución.
Medio (2)	La eliminación o modificación indebida de información tiene un impacto considerable para la institución.
Bajo (1)	La eliminación o modificación indebida de información tiene un impacto leve para la institución.

Elaborado por: El investigador

Criterios de valoración en términos de disponibilidad.

Tabla 12: Valoración de términos de disponibilidad [27].

Disponibilidad	**Criterio**
Alto (3)	La perturbación al acceso de la información tiene un impacto de gran importancia para la institución.
Medio (2)	La perturbación al acceso de la información tiene un impacto considerable para la institución.
Bajo (1)	La perturbación al acceso de la información tiene un efecto mínimo para la institución.

Elaborado por: El investigador

Con todos estos criterios es necesario realizar la valoración de los activos de información, mismo que están ubicados en el edificio matriz denominado **"Matriz X-1".** En la tabla 13 se realiza una valoración de los activos tomando como base la "Guía para la gestión de riesgos de seguridad de la información" emitida por el ministerio de telecomunicaciones y de la sociedad de la información de la república del Ecuador [27].

Para calcular el impacto de un activo, se emplea la siguiente fórmula para cada uno de ellos:

$$VA = \frac{C + I + D}{3}$$

En esta fórmula, se suman los tres parámetros y se divide el resultado entre tres. A continuación, se presenta la tabla de valoración de los dispositivos, donde se ha aplicado la fórmula a cada uno de ellos.

La valoración de confidencialidad, integridad y disponibilidad fue llevada a cabo por el administrador de TI, quien posee más de 15 años de experiencia en el campo y conoce la realidad de la red.

Tabla 13: Valoración de los activos [27].

VALORACION DE LOS ACTIVOS DE INFORMACION						
Nro Activo	Nombre Activo	Tipo desoporte	Valoración de Impacto			
			C: Confidencialidad I: Integridad D: Disponibilidad			
			C	I	D	VA
A1	Router	Físico y Lógico	1	1	2	1,33
A2	Red de datos	Físico	1	1	2	1,33
A3	Firewall Fortigate	Físico y Lógico	3	2	2	2,33
A4	Switch Cisco SG200-26P	Físico y Lógico	1	1	3	1,67
A5	Switch HP 1920-16G	Físico y Lógico	1	1	2	1,33
A6	Enlaces de internet	Físico y Lógico	1	1	1	1,00
A7	Antivirus	Lógico	2	2	1	1,67

Elaborado por: El investigador

Considerando que el firewall es el equipo con más valoración, es este el sistema en el que se enfocarán las acciones necesarias para obtener los datos requeridos para planificar una contramedida que sea útil para la entidad.

3.1.3. Lenguaje de análisis de datos

- **Python**

El lenguaje de programación Python destaca por su facilidad de comprensión y versatilidad, lo que lo convierte en una herramienta muy útil en diversas áreas de TI. Al ser un lenguaje interpretativo, permite una programación más ágil y rápida al tiempo que brinda una amplia gama de librerías predeterminadas. Además, ofrece la flexibilidad de importar librerías adicionales según las necesidades específicas del proyecto, lo que potencia su aplicabilidad en diferentes contextos y escenarios. Con Python, es posible abordar una amplia variedad de tareas y proyectos, desde desarrollo web hasta análisis de datos y automatización de tareas, lo que lo convierte en una opción destacada en el mundo de la programación. Su popularidad y comunidad activa también contribuyen a su crecimiento constante y actualización, brindando a los desarrolladores una solución confiable y en constante evolución para enfrentar los desafíos tecnológicos actuales [28].

- **Matlab**

Matlab es una poderosa herramienta de programación con aplicaciones en diversos campos, incluyendo ciencias, ingeniería, salud y tecnologías emergentes. Su enfoque está especialmente diseñado para abordar problemas matemáticos y su aplicación computacional en entornos técnicos. Una de sus principales fortalezas radica en su extensa biblioteca, que integra una amplia variedad de funciones para el análisis numérico, facilitando la resolución de complejas ecuaciones y cálculos matemáticos. Esta versatilidad y capacidad de abordar tareas específicas en distintas disciplinas lo convierten en una herramienta altamente valorada por profesionales y académicos. Además, Matlab permite la creación y ejecución de algoritmos personalizados, lo que posibilita la implementación de soluciones adaptadas a necesidades particulares [29].

3.1.4. Recopilación de información

Con el objetivo de lograr una visualización más clara y comprensible de la red, se elaboró un diagrama que representa de manera gráfica los distintos elementos que conforman la estructura de la red así también como su topología. Este diagrama

se lo puede visualizar en el gráfico 21, proporcionando una representación visual que facilita la comprensión de la disposición y la interconexión de los elementos de la red.

ESQUEMA DE LA RED

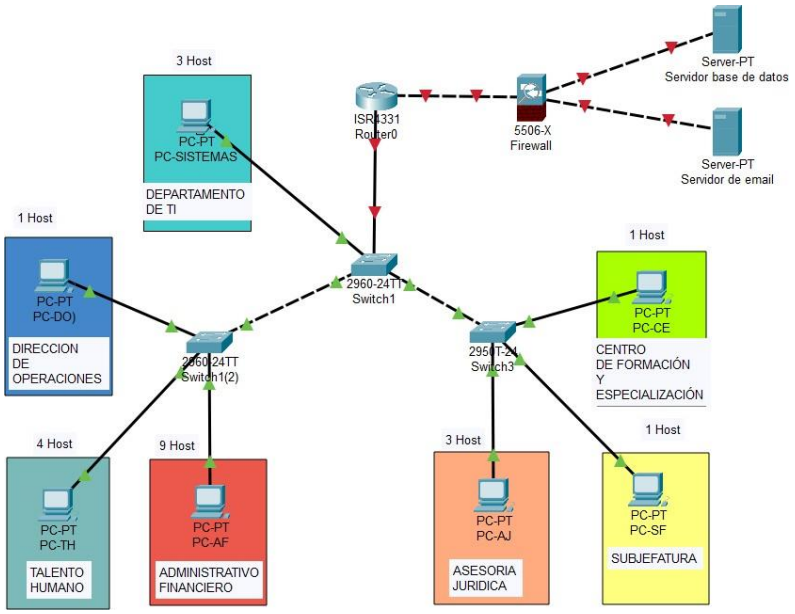


Gráfico 21: Esquema de la red

Elaborado por: El investigador

Una vez que se estableció con claridad la topología de la red y se identificaron tanto los sistemas finales como los de seguridad presentes, se procedió a realizar una investigación detallada utilizando la información recopilada a partir de un escaneo, el cual se describe de manera exhaustiva en el ***Anexo 1.***

Para realizar el análisis actual de la red se han considerado parámetros como:

- **Registros de Eventos:** Los sistemas de seguridad generan registros de eventos que proporcionan detalles sobre actividades realizadas en la red, como intentos de acceso, cambios en configuraciones, inicio de sesión de usuarios y otros eventos relevantes. Estos registros pueden ser analizados para identificar patrones anómalos o actividades sospechosas [10].

- **Tráfico de Red**: El análisis del tráfico de red permite identificar patrones de comunicación entre dispositivos. Puede revelar actividad maliciosa, como intentos de intrusión, escaneos de puertos, tráfico inusual o conexiones salientes no autorizadas [11].

- **Detección de Malware:** Los sistemas de seguridad pueden detectar la presencia de malware, virus y otro software malicioso que pueda estar presente en la red. Esto puede incluir análisis de archivos, detección de patrones y comportamientos inusuales [12].

- **Análisis de Puertos Abiertos:** El escaneo de puertos abiertos en los dispositivos de la red ayuda a identificar posibles vulnerabilidades. Puertos no autorizados o inseguros pueden ser explotados por atacantes para comprometer la seguridad [13].

ANALISIS DE LA ESTRUCTURA DE RED

Se ha implementado un minucioso proceso de monitoreo de red con las herramientas Wireshark, Nessus y Advance IP Scanner, tal como se describe en el ***anexo 1***, en donde se detalla los puertos abiertos y el analisis de los logs propio del proceso Threat Hunting. Como resultado de este proceso, se han recopilado y evaluado datos relevantes, los cuales se presentan a continuación en las tablas *14, 15 y 16* :

FIREWALL

Tabla 14: Resultado del escaneo al firewall

	IP	Puertos abiertos	Vulnerabilidades	Nivel de contraseña
Host 1	192.168.1.1	22(SSH), 80 (HTTP), 443 (HTTPS)	Ataques de inyección de código mediante su gestor Web por falta de actualización (CVE-2020-29015)	Débil

Elaborado por: El investigador

SERVIDORES

Tabla 15: Resultado del escaneo de servidores

	IP	Puertos abiertos	Archivo de registros de eventos	Vulnerabilidades	Nivel de contraseña
Host 2	192.168.1.4	22(SSH), 135(RPC), 139(NetBIOS), 445(SMB)	/opt/zimbra/log/mailbox.log	Dropbear SSH Server < 2016.72	Débil
Host 3	192.168.1.6	111(RPC)	Ninguno	Dropbear SSH Server < 2016.72	Débil

Elaborado por: El investigador

Computadores

Tabla 16: Resultado de escaneo de computadores

	IP	Puertos abiertos	Archivo de registros de eventos	Nro de Evento	Vulnerabilidades	Nivel de contraseña
Host 4	192.168.1.9	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 5	192.168.1.11	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 6	192.168.1.12	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 7	192.168.1.15	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 8	192.168.1.16	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 9	192.168.1.18	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 10	192.168.1.22	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 11	192.168.1.24	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 12	192.168.1.25	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil

Host 13	192.168.1.26	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 14	192.168.1.27	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 15	192.168.1.29	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 16	192.168.1.30	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil
Host 17	192.168.1.38	22 (SSH), 80 (HTTP)	C:\Windows\System32\ winevt\Logs	4625	Dropbear SSH Server < 2016.72	Débil

Gráfico 24: Host 4

Elaborado por: El investigador

3.1.5 Patrones de anomalías encontradas

Mediante el monitoreo de la red, se lograron identificar patrones inherentes a diversos elementos presentes en dicha infraestructura, los cuales pueden desempeñar un papel crucial en la explotación de vulnerabilidades en los sistemas:

Ataque de fuerza bruta

Tabla 17: Patrones del ataque de fuerza bruta

Patrones de Anomalías	Información	Host
Puertos	22(SSH)	1, 2, 4, 5 , 6 , 7, 8, 9, 10 , 11, 12, 13, 14, 15, 16
Archivos log	C:\Windows\System32\winevt\Logs	5 , 6 , 7, 8, 9, 10 , 11, 12, 13, 14, 15, 16
Nro. de evento	4625	5 , 6 , 7, 8, 9, 10 , 11, 12, 13, 14, 15, 16
Vulnerabilidad	Algoritmos de intercambio de claves débiles SSH habilitados	5 , 6 , 7, 8, 9, 10 , 11, 12, 13, 14, 15, 16

Elaborado por: El investigador

Ataque de inyección de código

Tabla 18: Patrones de ataque de inyección de código.

Patrones de Anomalías	Información	Host
Puertos	80 (HTTP), 443 (HTTPS)	1, 2, 4, 5 , 6 , 7, 8, 9, 10 , 11, 12, 13, 14, 15, 16
Archivos log	-	-

Ataque de DoS

Tabla 19: Patrones del ataque de DoS

Patrones de Anomalías	Información	Host
Puertos	80 (HTTP), 443 (HTTPS)	1, 2, 4, 5 , 6 , 7, 8, 9, 10 , 11, 12, 13, 14, 15, 16
Archivos log	/var/log/syslog	1, 2, 3

Ataque Phishing

Tabla 20: Patrones del ataque phishing

Patrones de Anomalías	Información	Host
Puertos	-	-
Archivos log	opt/zimbra/log/mailbox. log	2

Elaborado por: El investigador

Ataque Ransomware

Tabla 21: Patrones del ataque ransomware

Patrones de Anomalías	Información	Host
Puertos	139 (NetBIOS), 445 (SMB)	2
Archivos log	-	-

Elaborado por: El investigador

Características de Ataque de fuerza bruta

Tabla 22: Características del ataque de fuerza bruta

Característica	Descripción
Tipo de Ataque	Ataque de fuerza bruta
Objetivo	Adivinar o descifrar contraseñas mediante la prueba sistemática de todas las combinaciones posibles
Medio de Ataque	Acceso directo a servicios o sistemas protegidos por contraseñas.
Puertos Vulnerables	SSH (22)
Archivos de Log	/var/log/auth.log C:\Windows\System32\winevt\Logs

Elaborado por: El investigador

Características de Ataque DDoS

Tabla 23: Características de Ataque DDoS

Característica	Descripción
Tipo de Ataque	Ataque de Denegación de Servicio Distribuido (DDoS)
Objetivo	Sobrecargar un servicio o recurso con tráfico malicioso, causando la indisponibilidad de este.
Medio de Ataque	Envío masivo de tráfico desde múltiples fuentes hacia un objetivo común

Puertos Vulnerables	Puertos comunes asociados con servicios de red, como HTTP (80), HTTPS (443)
Archivos de Log	var/log/syslog

Elaborado por: El investigador

Características de Ataques de inyección de código

Tabla 24: Características de Ataque de inyección de código

Característica	Descripción
Tipo de Ataque	Ataque de Inyección de Código
Objetivo	Insertar código malicioso en una aplicación o sistema vulnerable
Método de Ataque	Aprovechamiento de entradas no validadas o mal sanitizadas en formularios, consultas o comandos
Puertos Vulnerables	(80), HTTPS (443).
Archivos de Log	-

Elaborado por: El investigador

Características de ataques phishing

Tabla 25: Características de Ataques Phishing

Característica	Descripción
Tipo de Ataque	Phishing
Objetivo	Engañar a los usuarios para obtener información confidencial, como contraseñas o datos bancarios
Medio de Ataque	Correo electrónico, mensajes instantáneos, mensajes de texto, llamadas telefónicas, redes sociales
Puertos Vulnerables	-
Archivos de Log	opt/zimbra/log/mailbox.log

Elaborado por: El investigador

Características de ataques Ransomware

Tabla 26: Características de Ataques de Ransomware

Característica	Descripción
Tipo de Ataque	Ataque de Ransomware
Objetivo	Cifrar los archivos y sistemas de una víctima y exigir un rescate a cambio de su liberación
Método de Ataque	Distribución a través de correos electrónicos de phishing, exploit kits, descargas maliciosas
Puertos Vulnerables	SMB (445), NetBios (139)
Archivos de Log	-

Elaborado por: El investigador

Valoración de los tipos de ataques

Para poder planificar una contramedida se tomó en cuenta ciertas métricas para calcular el nivel de riesgo al que está expuesto la red.

Nivel de amenaza

Tabla 27: Valoración del nivel de amenaza [27].

Nivel de amenaza	**Criterio**
Alto (3)	Probabilidad muy alta de que pueda ocurrir
Medio (2)	Probabilidad moderada de que pueda ocurrir
Bajo (1)	Probabilidad baja de que pueda ocurrir

Elaborado por: El investigador

Nivel de vulnerabilidades

Tabla 28: Valoración de nivel de vulnerabilidades [27].

Nivel de vulnerabilidades	**Criterio**
Alto (3)	Probabilidad muy alta
Medio (2)	Probabilidad moderada
Bajo (1)	Probabilidad baja

Elaborado por: El investigador

Valoración de riesgos

Con todos estos criterios es necesario realizar un cálculo del nivel de riesgo**.** En la tabla 26 se realiza una valoración de los activos tomando como base la "Guía para la gestión de riesgos de seguridad de la información" emitida por el ministerio de telecomunicaciones y de la sociedad de la información de la república del Ecuador, y con el criterio del ingeniero Willian Silva, experto en TI con más de 15 años de experiencia se valoró el nivel de amenaza y el nivel de vulnerabilidad y aplicando la siguiente formula se obtuvo el nivel de riesgo.

$$NA = \frac{A + V}{2}$$

Tabla 29: Valoración de posibles riesgos [27].

VALORACION DE LOS POSIBLES RIESGOS				
Nro	**Tipo de Ataque**	Valoración de riesgo		
		A: Nivel amenaza V: Nivel de vulnerabilidad		
		A	V	VR
1	Ataque de fuerza bruta	3	3	3
2	Ataque de DDoS	2	2	2
3	Ataque de inyección de código	2	2	2
4	Ataque de phishing	1	1	1
5	Ataque de ransomware	0	1	0,5

Elaborado por: El investigador

3.2. Desarrollo de la propuesta

Para el desarrollo del presente proyecto es necesario el uso de un lenguaje que sea útil para cubrir las condiciones y necesidades del entorno de trabajo. Además de proporcionar un análisis de los datos.

3.2.1. Metodología de desarrollo

El proceso proactivo Threat Hunting tiene un valor agregado siendo este una metodología base que se aplica dependiendo de los diferentes recursos y necesidades de la infraestructura de red. Pero es necesario complementar las actividades y tareas necesarias con una metodología ágil para el correcto control y ejecución de las acciones que se requieran.

3.2.2. Cuadro comparativo de las metodologías ágiles.

Tabla 30: Cuadro comparativo de las metodologías ágiles

	Kanban	**Kaizen**	**Waterfall**
Tamaño del proyecto	Proyectos de diferentes tamaños. [35]	Proyectos de tamaño pequeño. [36]	Proyectos de gran envergadura y complejidad. [37]
Tamaño del equipo	Sin restricciones específicas de tamaño de equipo. [35]	Mas de una persona. [36]	Equipos grandes y jerárquicos. [37]
Marco de tiempo	Mantiene su foco en ítems individuales en cada momento [35]	3 semanas. [36]	Secuencial, con fases bien definidas. [37]
Gestión de requerimientos	Tableros Kanban [35]	Sprint. [36]	documentación exhaustiva [37]
Desarrollo	Gradual y Evolutivo [35]	Rápido y dinámico [36]	Secuencial Y lineal [37]
Complejidad de Diseño	Diseño visual Sencillo [35]	Diseño simple.[36]	Diseño visual Simple [37]
Ventajas	Mejora la eficiencia y la visibilidad [35]	Mayor colaboración y transparencia. [36]	Fácil de entender y seguir [37]
Desventajas	No es adecuado para proyectos complejos [35]	Puede ser desafiante para equipos grandes. [36]	Poco flexible y adaptable [37]

Elaborado por: El investigador

En este proyecto se decidió implementar la metodología Kanban, la cual tiene como objetivo mejorar la gestión y visualización del proceso mediante el uso de tableros. Estos tableros constan de 4 columnas y límites de trabajo en progreso (WIP), lo que permite una gestión más eficiente del flujo de trabajo. Con esto, se busca facilitar la organización y el seguimiento de las tareas del proyecto, al tiempo que se visualiza de manera clara el flujo de trabajo y se establecen límites

para mantener un control adecuado del trabajo en curso.

- Visualizar el flujo de trabajo
- Límites WIP (Work in progress)
- Flujo de trabajo

3.2.3. Fase de Visualización de trabajo

Se ha creado un tablero Kanban utilizando la aplicación MaisterTask para visualizar el flujo de trabajo. El tablero consta de tres columnas principales: "Por hacer", "En progreso" y "Completado". Esta configuración permite realizar un seguimiento claro y ordenado de las tareas a medida que avanzan en el proceso. Además, la aplicación también ofrece funcionalidades adicionales, como la capacidad de controlar el tiempo dedicado a cada tarea en particular. Esto resulta beneficioso para mejorar la productividad y la gestión efectiva del tiempo en el proyecto.

3.2.4. Fase 2: Limitar el WIP

Esta opción ayuda a gestionar de mejor manera el límite de tareas a realizarse con el cual se evita la acumulación de trabajo sin terminar. No hay una cantidad especifica acerca de un límite de tareas porque esta sé específica de acuerdo con cada persona u organización y la prioridad que manejen.

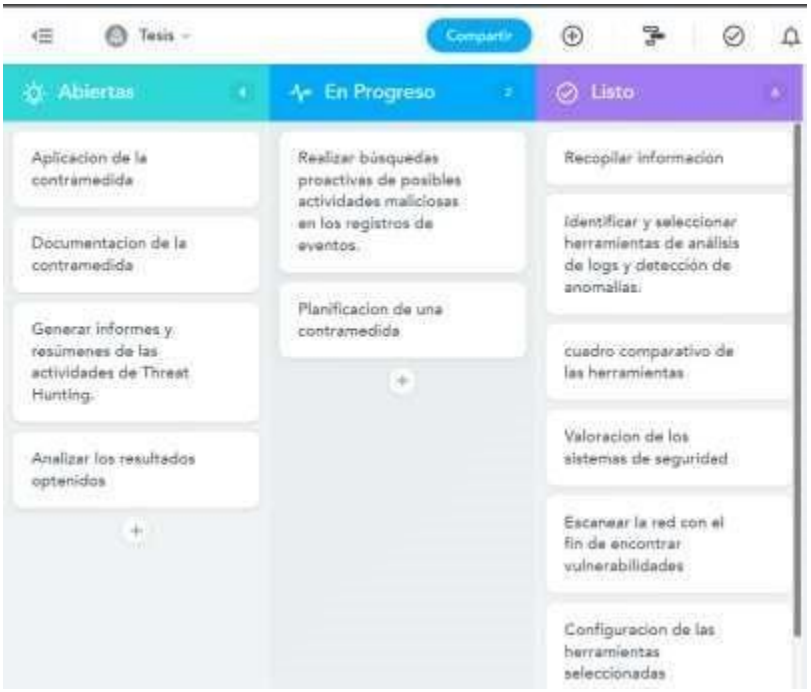


Gráfico 22: Tablero Kanban

Elaborado por: El investigador

3.2.5. Fase 3: Flujo de trabajo

Gráfico 23: Diagrama de fujo de trabajo

Elaborado por: El investigador

3.2.6. Fase de planificación de las contramedidas.

Con las características claramente definidas y teniendo en cuenta todas las vulnerabilidades encontradas en la infraestructura de red, se ha realizado una planificación de contramedidas efectivas. Estas contramedidas se centran en los puntos débiles identificados, con el objetivo de fortalecer la seguridad de la red.

A continuación, se detallan las contramedidas planificadas:

Planificación contra un Ataque de fuerza bruta

La planificación se pudo llegar a establecer gracias a las vulnerabilidades y características encontradas con el proceso realizado previamente. Las planificaciones realizadas son:

Planificación P-1-1

Tabla 31: Planificación Nro. 1

Código	**Responsable**		**Prioridad**	
P-1-1	Administrador de TI		Alta	
Paso	**Actividad**	**Descripción**	**Archivos Log**	**Mitigación**
1	Uso de contraseñas fuertes	Educar a los usuarios sobre la importancia de utilizar contraseñas seguras, establecer cumplir una política de contraseñas seguras	Registros de cambio de contraseñas	Establecer una política para la generación de contraseñas robustas para los usuarios de la institución

Elaborado por: El investigador

Política para la generación de contraseñas fuertes

Se creó una política de generación de contraseñas, la cual fortalecerá la asignación de contraseñas. La política consiste en las siguientes normas:

1. **Longitud:** Esta regla establece que la longitud de la contraseña deberá ser mínima de 12 caracteres.
2. **Combinación:** La contraseña deberá combinarse con caracteres alfanuméricos y especiales. Por ejemplo, al menos una letra mayúscula, una letra minúscula, un número y un carácter especial sin una combinación especifica.
3. **Información personal:** Prohibido el uso de información personal como nombres, fechas de nacimiento o números de identidad.
4. **Caducidad y cambio regular:** Establecer una política de caducidad de

contraseñas que requiera a los usuarios cambiar sus contraseñas cada 90 días o según lo establecido por la organización.

5. **Restricción de reutilización:** Impedir que los integrantes de la red utilicen contraseñas previamente utilizadas, manteniendo un historial de contraseñas anteriores y evitando su reutilización durante un período de tiempo determinado.

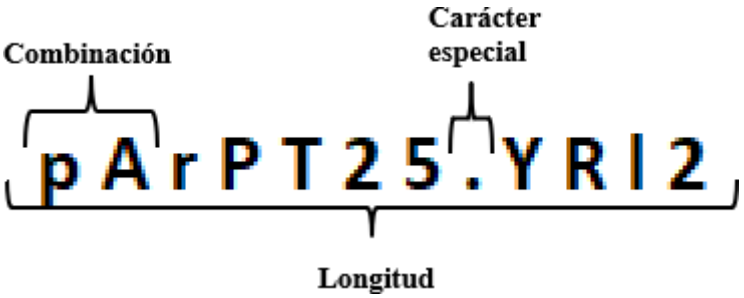


Gráfico 24: Política de contraseña

Elaborado por: El investigador

Planificación contra un Ataque de DDoS

Planificación P-2-1

Tabla 32: Planificación Nro. 2

Código	**Responsable**		**Prioridad**	
P-2-1	Asistente de TI		**Alto**	
Paso	**Actividad**	**Descripción**	**Archivos Log**	**Mitigación**
1	Implementar un firewall de red.	Formular configuraciones para el firewall de red para filtrar y bloquear tráfico sospechoso o malicioso.	Registros del firewall	Generar reglas de firewall para bloquear direcciones IP sospechosas o patrones de tráfico asociados a ataques DDoS.

Elaborado por: El investigador

Reglas para la configuración del Firewall REGLA 1

1. **config firewall address:**

Este comando indica la configuración una dirección IP en el firewall.

- El siguiente comando edit "IP_sospechosa_1" crea una nueva entrada para una dirección IP sospechosa específica. Puedes reemplazar "IP_sospechosa_1" con un nombre más descriptivo.
- set subnet <IP_sospechosa_1>/32 establece la dirección IP y la máscara de subred. En este caso, se utiliza "/32" para especificar una sola dirección IP.

2. **config firewall policy:**

Este comando indica a configuración una política de firewall.

- El siguiente comando edit 1 crea una nueva entrada para una política de firewall específica. Puedes reemplazar "1" con un número de política diferente si es necesario.
- set name "Bloquear IP sospechosa 1" asigna un nombre descriptivo a la política de firewall.
- set srcintf "LAN" especifica la interfaz de origen desde donde se originará el tráfico. Puedes reemplazar "LAN" con la interfaz correspondiente en tu entorno.
- set dstintf "WAN" especifica la interfaz de destino a la que se dirigirá el tráfico. Puedes reemplazar "WAN" con la interfaz correspondiente en tu entorno.
- set srcaddr "IP_sospechosa_1" indica la dirección IP sospechosa que se bloqueará. Debe coincidir con la entrada configurada anteriormente en config firewall address.
- set action deny establece la acción a "denegar", lo que significa que el tráfico de la dirección IP sospechosa será bloqueado.
- set schedule "always" indica que la política estará activa en todo momento.

```
config firewall address
    edit "IP_sospechosa_1"
        set subnet <IP_sospechosa_1>/32
        next
    end

config firewall policy
    edit 1
        set name "Bloquear IP sospechosa 1"
        set srcintf "LAN"
        set dstintf "WAN"
        set srcaddr "IP_sospechosa_1"
        set action deny
        set schedule "always"
        next
    end
```

Gráfico 25: Regla 1 para configuración de firewall

Elaborado por: El investigador

REGLA 2

1. config firewall address

- edit "Rango_IP_sospechoso": Se crea una entrada en la configuración de direcciones del firewall con el nombre "Rango_IP_sospechoso". Esto permite definir un rango de direcciones IP sospechosas que se utilizará posteriormente en una política de firewall.
- set start-ip <IP_inicial>: Se establece la dirección IP inicial del rango sospechoso.
- set end-ip <IP_final>: Se establece la dirección IP final del rango sospechoso.
- next: Se indica que se ha terminado la configuración de la dirección y se pasa al siguiente elemento.

2. config firewall policy

- **edit 2:** Se crea una entrada en la configuración de políticas del firewall con el número 2.

- **set name "Bloquear Rango de IP sospechoso":** Se asigna un nombre descriptivo a esta política de firewall, que en este caso indica que se bloqueará un rango de direcciones IP sospechosas.
- **set srcintf "LAN":** Se especifica la interfaz de origen de la política, en este caso, "LAN" (red local).
- **set dstintf "WAN":** Se especifica la interfaz de destino de la política, en este caso, "WAN" (red externa o Internet).
- **set srcaddr "Rango_IP_sospechoso":** Se indica que la dirección de origen permitida para esta política es el rango de direcciones IP sospechosas previamente definido.
- **set action deny:** Se establece la acción de la política como "deny" (denegar), lo que significa que se bloquearán todas las conexiones provenientes de las direcciones IP sospechosas.
- **set schedule "always":** Se establece el horario de aplicación de la política como "always" (siempre), lo que significa que la política estará en efecto en todo momento.
- **next:** Se indica que se ha terminado la configuración de la política y se pasa al siguiente elemento.

```
config firewall address
    edit "Rango_IP_sospechoso"
        set start-ip <IP_inicial>
        set end-ip <IP_final>
        next
    end

config firewall policy
    edit 2
        set name "Bloquear Rango de IP sospechoso"
        set srcintf "LAN"
        set dstintf "WAN"
        set srcaddr "Rango_IP_sospechoso"
        set action deny
        set schedule "always"
        next
    end
```

Gráfico 26: Regla 2 configuración de firewall

Elaborado por: El investigador

Planificación contra un Ataque de DDoS

Planificación P-3-1

Tabla 33: Planificación Nro. 3

Código	**Responsable**		**Prioridad**
P-2-2	Asistente de TI		**Alto**
Paso	**Actividad**	**Descripción**	**Mitigación**
1	Actualización y parcheo de sistemas	Mantener los sistemas y Aplicaciones actualizados con los últimos parches de Seguridad	Generar una política de gestión de parches y mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad para corregir vulnerabilidades conocidas y minimizar la exposición a posibles ataques.

Elaborado por: El investigador

POLÍTICA DE SEGURIDAD GENERADA PARA MANTENERACTUALIZADAS LOS SISTEMAS.

1. **Objetivo:**
   - Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad para corregir vulnerabilidades conocidas y minimizar la exposición a posibles ataques.
2. **Responsabilidades:**

- **Equipo de Seguridad:**
  - Realizar seguimiento de las actualizaciones de seguridad disponibles para los sistemas y aplicaciones utilizados en la infraestructura.
  - Evaluar la criticidad de los parches y determinar su aplicabilidad en función de los riesgos y la compatibilidad con la infraestructura existente.
  - Coordinar y planificar la implementación de los parches de seguridad en colaboración con los administradores de sistemas y los responsables de las aplicaciones.

- Administradores de Sistemas:
    - Mantener un inventario actualizado de los sistemas y aplicaciones utilizados en la infraestructura.
    - Monitorear y recibir las notificaciones de los proveedores sobre las actualizaciones de seguridad disponibles.
    - Realizar pruebas de compatibilidad de los parches en entornos de desarrollo o pruebas antes de implementarlos en los entornos de producción.
    - Implementar los parches de seguridad de acuerdo con la planificación establecida por el equipo de seguridad.

3. Proceso de Gestión de Parches:

a) Identificación de Parches:

- Recopilar información sobre los parches de seguridad disponibles a través de fuentes confiables, como los proveedores de sistemas y aplicaciones, sitios web de seguridad y boletines de seguridad.
- Evaluar la criticidad de los parches en función de las vulnerabilidades que corrigen y su impacto potencial en la infraestructura.

b) Evaluación y Priorización de Parches:

- Determinar la aplicabilidad de los parches a los sistemas y aplicaciones utilizados en la infraestructura.
- Evaluar el riesgo asociado con la vulnerabilidad corregida por el parche y establecer una prioridad basada en la criticidad y el impacto potencial.

c) Pruebas y Validación:

- Realizar pruebas de compatibilidad de los parches en entornos de desarrollo o pruebas para garantizar que no afecten el funcionamiento normal de los sistemas y aplicaciones.
- Validar la efectividad de los parches mediante pruebas de seguridad adicionales para verificar que las vulnerabilidades corregidas estén mitigadas**.**

d) Implementación de Parches:

- Establecer una planificación para la implementación de los parches, considerando los tiempos de mantenimiento programados y el impacto en los usuarios y los servicios.
- Implementar los parches en los entornos de producción siguiendo las mejores prácticas de implementación y minimizando las interrupciones en el servicio.

e) Monitoreo y Seguimiento:

- Realizar un seguimiento continuo de las actualizaciones de seguridad y las vulnerabilidades conocidas para garantizar que los sistemas y aplicaciones estén siempre actualizados.
- Monitorear los sistemas y aplicaciones en busca de posibles problemas o incompatibilidades causadas por los parches implementados.

4. Comunicación y Concientización:

- Informar a los usuarios y las partes interesadas sobre la importancia de mantener los sistemas y aplicaciones actualizados.
- Proporcionar orientación y materiales educativos sobre las mejores prácticas de seguridad y la importancia de aplicar los parches de seguridad.

CAPÍTULO IV.- CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- Recolectando la información sobre sistemas de seguridad de la infraestructura de red, se logró identificar de manera proactiva posibles amenazas y vulnerabilidades con el uso de herramientas como Nessus encontrando 25 vulnerabilidades en 16 host escaneados destacando los puertos expuestos y los archivos ***log*** que fueron analizados con un código realizado en el lenguaje Python que se encuentra en el ***anexo 1,*** este enfoque permitió tener una visión más clara y detallada de la situación de seguridad en la institución.

- Durante el proceso de identificación de patrones, se consideraron todas las vulnerabilidades encontradas, como los puertos 139 y 445 que están abiertos en modo escucha, propensos a ataques de ransomware, la debilidad de las contraseñas y los archivos log registrados con múltiples intentos de inicio de sesión. Esto ayudó a realizar una relación de las vulnerabilidades y los ataques investigando el comportamiento de las diferentes amenazas.

- La planificación de las contramedidas se llevó a cabo considerando el nivel de riesgo, el cual fue calculado mediante la suma del nivel de amenaza y el nivel de vulnerabilidad, dividido entre dos. Este proceso se aplicó para cada posible tipo de ataque. Tomando como ejemplo el ataque de fuerza bruta, el cual recibió una calificación de amenaza de 3 debido a las debilidades en las contraseñas utilizadas y a la falta de una política para la generación de contraseñas seguras. Por otro lado, el nivel de vulnerabilidad se calificó con un valor de 3, ya que el monitoreo reveló diversas vulnerabilidades asociadas a este tipo de ataque, como el puerto 22 (SSH) abierto y la detección de algoritmos de intercambio de claves débiles habilitos, dando como resultado un nivel de riesgo de 3 concluyendo que es necesaria la planificación de una contramedida contra esta amenaza. Se priorizaron aquellas medidas que reforzaban los puntos críticos y que proporcionaban una mayor protección contra los posibles ataques.

- La documentación se realizó al registrar el proceso aplicado en cada paso, iniciando con el escaneo de la red, en dónde se expusieron las debilidades existentes, con algunos puntos a destacar como los puertos abiertos 80 (HTTP) y 443 (HTTPS), que estaban expuestos a amenazas como un ataque DoS; por otra parte, la ausencia de reglas de configuración del firewall y el nulo control de manejo de versiones de los softwares de los sistemas fueron otros factores a considerar.

- Se documentó el proceso de identificación de patrones asociados a las amenazas, lo cual involucró investigar su comportamiento. Un ejemplo claro de esto es el ataque de fuerza bruta, que puede ocurrir a través del puerto 22 debido a la falta de contraseñas seguras. Como contramedida, se diseñó una política de generación de contraseñas robustas. Esta política implica que las contraseñas deben tener una longitud mínima de 12 caracteres y deben ser una combinación aleatoria de letras, números y caracteres especiales.

4.2. Recomendaciones

- Se recomienda capacitar al personal encargado del monitoreo de la red, de forma periódica, cada 6 meses especialmente en el uso de herramientas de monitoreo y administración, como Nessus y Advance IP scanner, para garantizar la correcta ejecución y aplicación de dichas herramientas para la identificación de posibles ataques e intentos de penetración, así como capacitaciones a todo el personal, para evitar ser víctimas de ataques por phishing e ingeniería social.

- Se recomienda implementar reglas de detección de amenazas, como la búsqueda de cadenas sospechosas en los archivos, especificando un parámetro, dependiendo de lo que se analice, como las letras “MZP” que son distintivas de ataques ransomware, usándolas como expresiones regulares para el descubrimiento de patrones sospechosos. Para facilitar la asociación de las vulnerabilidades con los tipos de ataques potenciales, se sugiere el uso del software Yara, porque ofrece

opciones avanzadas para crear y aplicar reglas personalizadas según las necesidades de la red y del administrador del sistema.

- Se recomienda establecer una política de colaboración y comunicación efectiva entre el personal del equipo de seguridad y de otros departamentos de la organización, a través de la realización de reuniones frecuentes para la socialización de las políticas de seguridad que se establecieron, y la forma correcta de la implementación.

- Se recomienda documentar el proceso en base a estándares de seguridad como GDPR o ISO 27001, así se garantiza un seguimiento y evaluación continuos de las medidas de seguridad implementadas, y se establecen posibles mejoras y actualizaciones futuras para la infraestructura de la red

BIBLIOGRAFÍA.

[1] I. G. Bernala, "Ataques Informáticos Basados en la Integridad de la Información, Experiencias de práctica, vol. 2, May 2015. Accessed: Dec. 05, 2022. [Online]. Available: http://www.unsis.edu.mx/revista/doc/vol2num5/A4_Ataques_Info.pdf

[2] R. Bello, W. Andrés, Medina Becerra, F. Andrés, M. Lara, and J. Alonso, "Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas Methodologies for cyber security risk assessment applied to SCADA systems for power companies Contenido," ISSN, vol. 41, p. 7.

[3] M. D. Lozano Alvarez and M. A. Correa Mesa, "Análisis de las vulnerabilidades de la infraestructura tecnológica mediante testing de caja blanca, bajo la norma ISO

27005 en la compañía Caracol Radio, nodo principal Bogotá," Universidad Cooperativa de Colombia Facultad de Ingeniería Programa de Ingeniería en Sistemas Seccional Bogotá D.C., Bogotá, 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://repository.ucc.edu.co/bitstream/20.500.12494/16502/1/2020_Analisis_Vulnerabilidades_Infraestructura.pdf

[4] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," Frontiers in Computer Science, vol. 3, Mar. 2021, doi: 10.3389/FCOMP.2021.563060.

[5] J. Morales, "Influencia del COVID 19 en el incremento de los Ciberataques a Nivel

Mundial," Accessed: Feb. 01, 2023. [Online]. Available: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/11574/Ataques%20ciberneticos_Trabajo%20grado_Juan%20Morales_v2.pdf?sequence=1&isAllowed=y

[6] M. I. Romero Castro et al., "Introducción a la seguridad informática y el análisis

de vulnerabilidades," 3Ciencias, Oct. 2018. Accessed: Dec. 05, 2022. [Online]. Available: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridadinform%C3%A1tica.pdf

[7] J. J. Quinatoa Medina and J. J. Villares Jimenez, "Diseño e Implementación de BOTS para Automatizar Tareas de Búsqueda y Análisis de Vulnerabilidades en Sistemas Web," Universidad de las Fuerzas Armadas, Santo Domingo de los Tsáchilas, 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://repositorio.espe.edu.ec/bitstream/21000/32801/1/T-ESPESD-003246.pdf

[8] Pierre Salinas Tomapasca, Carlos Mendoza de los Santos, "Ciberseguridad para Cajas Municipales en Tiempos de Crisis", Escuela de Posgrado Y Estudios Continuos, Tesis para optar al grado de Maestro, 2020.

[9] Z. Jadidi and Y. Lu, "A Threat Hunting Framework for Industrial Control Systems",
IEEE Access, vol. 9, pp. 53638-53650, 2021, doi: 10.1109/ACCESS.2021.3133260.

[10] M. R. Fatemi, A. A. Ghorbani, and J. J. McNally, "Threat-Hunting in Windows Environment Using Host-based Log Data", Bachelor of Science in Software Engineering Thesis, Dec. 2019.

[11] T. Fin, D. E. Grado, F. Cesar, and G. Gil, "Threat hunting con la pila ELK", SANS Institute, 2018.

[12] A. Azmoodeh, A. Dehghantanha, M. Conti, and K. K. R. Choo, "Detecting CryptoRansomware in IoT Networks Based on Energy Consumption Footprint", Journal of Ambient Intelligence and Humanized Computing, vol. 9, no. 4, pp. 1141-1152, Aug. 2018, doi: 10.1007/S12652-017-0558-5.

[13] I. G. IBernala, "Ataques Informáticos Basados en la Integridad de la Información," Experiencias de practica , vol. 2, May 2015, Accessed: Dec. 05, 2022. [Online].
Available: http://www.unsis.edu.mx/revista/doc/vol2num5/A4_Ataques_Info.pdf

[14] J. M. Hernández-Suárez, J. Sánchez-García, N. Medina-Medina, and M. A. TrujilloRodríguez, "Arquitecturas empresariales de tecnología de la información," Rev. Tecnol. Marcha, vol. 32, no. 5, pp. 85-105, 2019.

[15] O. Salazar-García, E. Gómez-González, and M. Moya-Fuentes, "A survey on intrusion detection systems in computer networks," Journal of Network and Computer Applications, vol. 183, p. 102944, 2021. DOI: 10.1016/j.jnca.2021.102944.

[16] M. A. Abdelraheem, "Cybersecurity Techniques and Methodologies: A Comprehensive Survey," arXiv preprint arXiv:1904.09698, 2019.

[17] R. Sharpe, E. Warnicke, and U. Lamping, "Wireshark User's Guide Version 4.1.0 Preface Foreword", Accessed: May 15, 2023. [Online]. Available: https://gitlab.com/wireshark/wireshark/-/wikis/.

[18] "Nmap: the Network Mapper - Free Security Scanner." https://nmap.org/ (accessed May 15, 2023).

[19] U. DE Politécnica Cartagena, A. Barquero Pastor Director, M. Dolores Cano Baños Codirector, and I. Alexander Bello Tasic, "Estudio comparativo entre OpenVas y Wazuh".

[20] M. González, "Protocolo de gestión de vulnerabilidades," Escuela Técnica Superior de Ingeniería Universidad de Sevilla, Sevilla, 2019. Accessed: May 15, 2023. [Online]. Available: https://idus.us.es/bitstream/handle/11441/86018/TFG2187-GONZALEZ.pdf?sequence=1&isAllowed=y

[21] S. Rahalkar, "Metasploit 5.0 for Beginners." http://mogesec.com/wpcontent/uploads/2021/12/Metasploit-5.0-for-Beginners.pdf (accessed May 15, 2023).

[22] A. Hay, D. Cid, and R. Bray, "OSSEC Host-Based Intrusion Detection Guide", Accessed: May 15, 2023. [Online]. Available: www.sans.edu

[23] J. Astudillo Herrera, F. O. Flores, A. J. Macías, and A. Aranda, “Adaptación del IDS/IPS Suricata para que se pueda convertir en una solución empresarial”.

[24] “Advanced IP Scanner – Explorador de redes de descarga gratuita.” https://www.advanced-ip-scanner.com/es/ (accessed May 15, 2023).

[25] H. Luisa and H. Santiago, “Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red ,” *Revista Cubana de Ciencias Informáticas*, vol. 15, no. 3, 2021, Accessed: May 15, 2023. [Online]. Available: http://rcci.uci.cuPág.55-73https://orcid.org/0000-0002-81979956YudithMenesesConislla3https://orcid.org/0000-0002-7646-5512

[26] G. Castillo, “Burp Suite: Qué es y cómo se utiliza |,” Feb. 14, 2023. https://www.innovaciondigital360.com/cyber-security/burp-suite-que-es-comose-utiliza/ (accessed May 15, 2023).

[27] “Guía para la gestión de riesgos de seguridad de la información,” 2020, Accessed: Jul. 19, 2023. [Online]. Available: https://www.gobiernoelectronico.gob.ec/wpcontent/uploads/2020/04/GUÍA-PARA-LA-GESTIÓN-DE-RIESGOS-DESEGURIDAD-DE-LA- INFORMACIÓN-ABRIL-2020.pdf

[28] Veliz Donoso Sebastián, “Python Básico Para Hackers y Pentester.”

[29] J. E. Márquez Díaz, *Matlab para ciencias e ingeniería*. Editorial Neogranadina, 2021. Accessed: Jul. 18, 2023. [Online]. Available: https://editorial.unimilitar.edu.co/index.php/editorial/catalog/view/71/160/331

[30] P. Jazmín and P. Zamora, “ESCUELA DE INGENIERIA EN SISTEMAS”.

[31] J. E. Martínez-Lozano and P. S. Atencio Ortiz, “Creación de un ataque DDoS utilizando HTTP-GET Flood a partir de la metodología Cyber Kill,” 2019. http://www.scielo.org.co/pdf/itec/v16n1/1692-1798-itec-16-01-41.pdf (accessed Jul. 2, 2023).

[32] C. A. Chicaiza, M. A. Hallo, and G. L. Suntaxi, “Guía multimedia para la

prevención y detección de vulnerabilidades de inyección sql durante desarrollo de aplicaciones web (PyDISQL)", doi: 10.54808/CISCI2022.01.109.

[33] J. Guaña-Moya, P. del Carmen Jaramillo-Flores, E. Rafael Mora-Zambrano, M. Chiluisa-Chiluisa, D. Naranjo-Villota, and L. Gerardo Larrea-Torres, "Ataques de phishing y cómo prevenirlos Phishing attacks and how to prevent them".

[34] A. Azmoodeh, A. Dehghantanha, M. Conti, and K. K. R. Choo, "Detecting cryptoransomware in IoT networks based on energy consumption footprint," *J Ambient Intell Humaniz Comput*, vol. 9, no. 4, pp. 1141–1152, Aug. 2018, doi: 10.1007/S12652-017-0558-5.

[35] L. Castellano Lendínez, "Kanban. Metodología para aumentar la eficiencia de los procesos," vol. 8, no. 1, pp. 30–41, 2019, doi: 10.17993/3ctecno/2019.

[36] "Método Kaizen: definición, pasos y ejemplos." https://blog.hubspot.es/sales/metodo-kaizen (accessed Aug. 23, 2023).J. D. Velázquez Camacho, "Desarrollo en Cascada (Waterfall) VS Desarrollo AgileSCRUM", Accessed: Jun. 19, 2023. [Online]. Available:

[37] OWASP, "OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation," 2023. https://owasp.org/ (accessed Jun. 19, 2023).

[38] R. McRee, "PHPIDS: Attack my website, please!", Accessed: Jun. 20, 2023. [Online]. Available: https://holisticinfosec.io/toolsmith/pdf/july2008.pdf

[39] OWASP, "OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation," 2023. https://owasp.org/ (accessed Jul. 19, 2023).

[40] R. McRee, "PHPIDS: Attack my website, please!", Accessed: Jul. 19, 2023. [Online]. Available: https://holisticinfosec.io/toolsmith/pdf/july2008.pdf

[41] G. Franco, G. Betarte, R. Martinez, and M. Rodriguez, "Integración del WAF ModSecurity y la plataforma para inteligencia de amenazas MISP".

[42] G. Morling, "Jakarta Bean Validation specification".

[43] Django, "Validators | Django documentation | Django." https://docs.djangoproject.com/en/4.2/ref/validators/ (accessed Jul. 19, 2023).

ANEXOS
Anexo 1:

Proceso de escaneo.

Para llevar a cabo el escaneo de la red, se utilizaron las herramientas Wireshark, Nessus y Advanced IP Scanner. Es fundamental estar conectado a la red para llevar a cabo el proceso de monitoreo. El administrador de la red ha designado específicamente la dirección IP 192.168.1.69 con fines investigativos para llevar a cabo dicho procedimiento.

Monitoreo con Wireshark

Primero se realiza la ejecución de la herramienta Wireshark para analizar el tráfico de la red general de la red en busca de actividad que se puede considerar sospechosa.

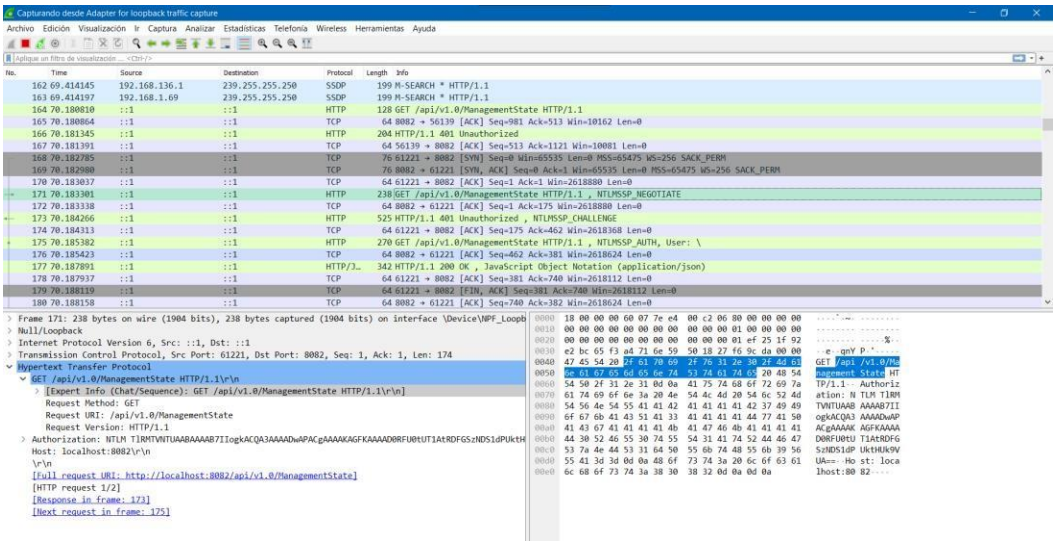


Gráfico 27: Ejecución de Wireshark

Elaborado por: El investigador

Utilizando esta herramienta, se logró detectar un intento de inicio de sesión fallido a través del protocolo HTTP. Este evento se describió en el mensaje GET HTTP con el token NTLMSSP_NEGOTIATE. Este proceso fue replicado en todos los dispositivos finales de la red.

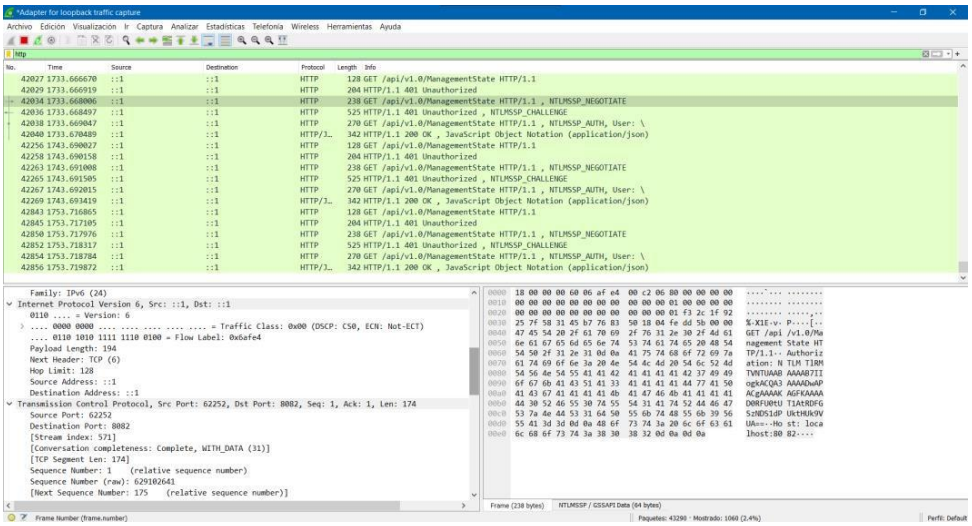


Gráfico 28: Registros de Wireshark

Elaborado por: El investigador

Monitoreo con Nessus

El paso subsiguiente consistió en llevar a cabo un escaneo de la red utilizando la herramienta Nessus, comenzando por el escaneo del firewall configurando con la dirección ip correspondiente con el fin de encontrar vulnerabilidades en este dispositivo.

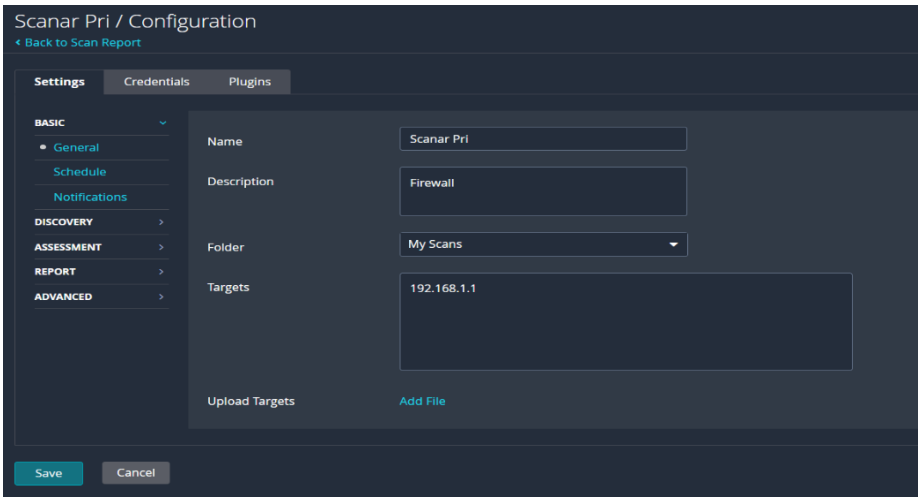


Gráfico 29: Configuración para escaneo con la herramienta Nessus

Elaborado por: El investigador

El escaneo tomó aproximadamente 10 minutos para completarse, arrojando un total de 18 vulnerabilidades, que incluyeron algunas de nivel medio y otras de información.

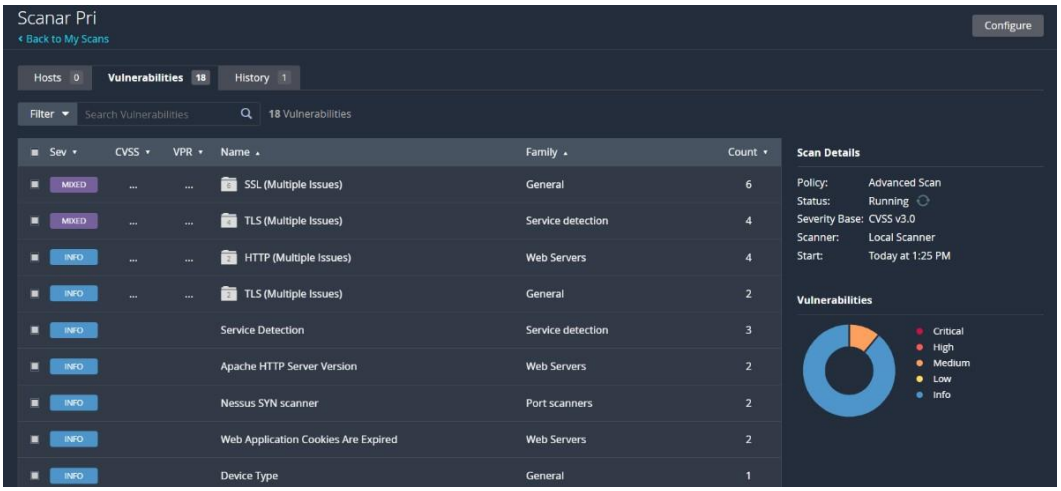


Gráfico 30: Resultados de la ejecución.
Elaborado por: El investigador

Ahora para un escaneo más general se ingresa el rango de IP's de toda la red para encontrar todas las vulnerabilidades que se puedan encontrar en los diferentes hots.

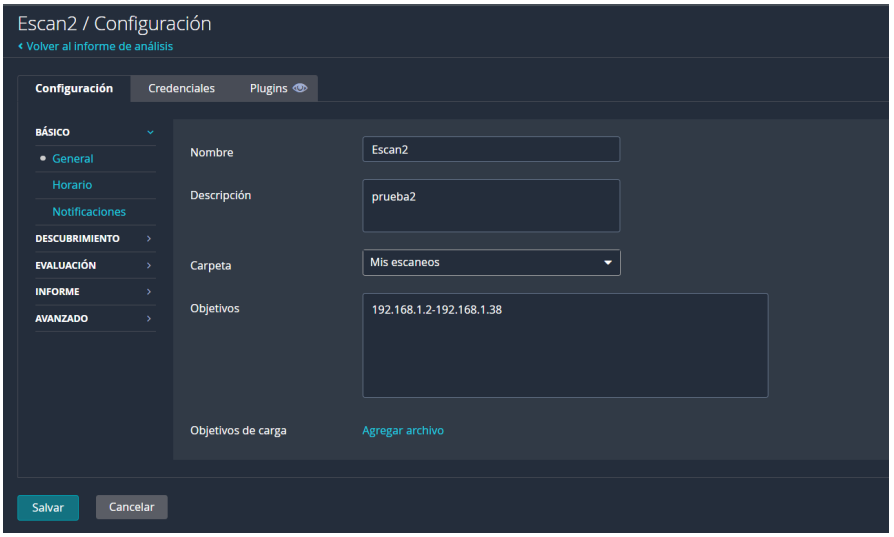


Gráfico 31: Escaneo general con Nessus

Elaborado por: El investigador

Se puede evidenciar los puertos abiertos que fueron identificados durante el proceso.

Gráfico 32: Puertos vulnerables

Elaborado por: El investigador

El proceso de escaneo de la red llevó aproximadamente una hora y treinta minutos en completarse. Durante este tiempo, se detectaron un total de 25 vulnerabilidades en los 16 hosts monitoreados. Es importante destacar que entre estas detecciones se incluyeron vulnerabilidades en estados críticos, altos y medios en los sistemas escaneados.

Gráfico 33: Escaneo general con Nessus

Elaborado por: El investigador

El escaneo reveló que le red cuenta con unos riesgos críticos como la falta de actualización del Dropbear SSH Server generando multiples vulnerabilidades y poniendo en riesgo la integridad de la red.

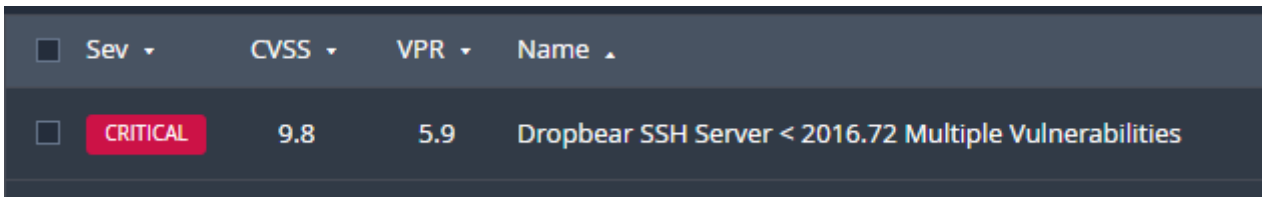


Gráfico 34: Amenaza critica

Elaborado por: El investigador

Monitoreo con Advance IP scanner

Para el monitoreo con la herramienta Advance IP scanner. Se colocó el rango de red para poder visualizar todos las ip's de los distintos dispositivos que se encuentran en la red. No se detectó ninguna IP sospechosa al realizar el escaneo. En este caso el rango de la red fumas extenso para poder identificar ip`s sospechosas que no deberían formar parte de la red.

Gráfico 35: Ejecución de la herramienta Advance IP Scanner

Elaborado por: El investigador

El monitoreo no detecto ninguna ip sospechosa, sin embargo, es importante monitorear la red con frecuencia para no ser sorprendido por al algún atacante.

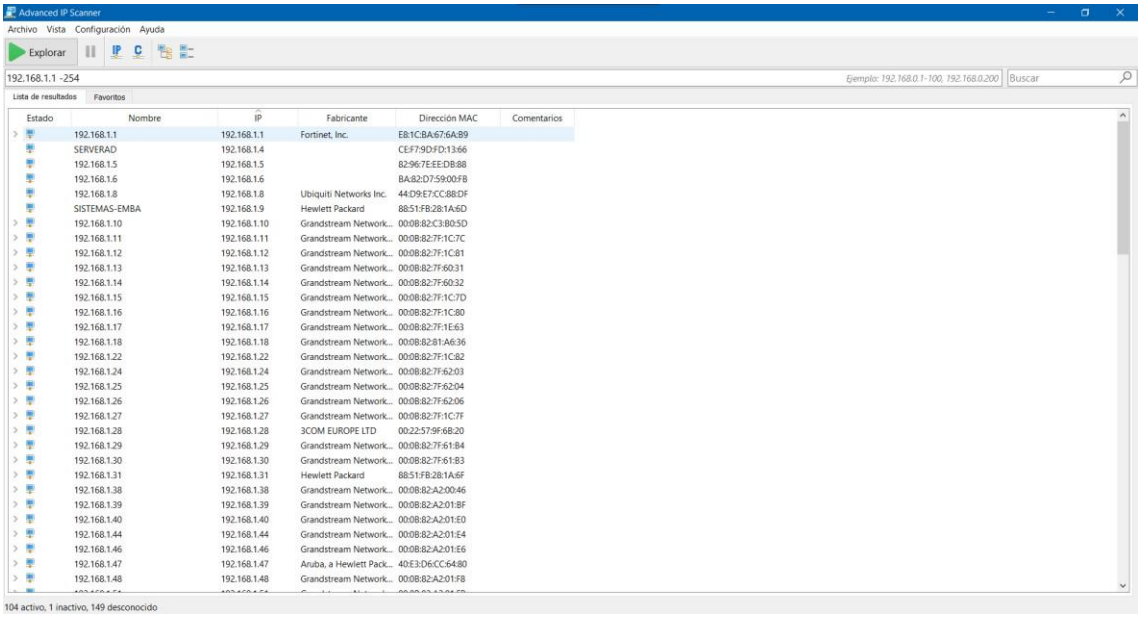


Gráfico 36: Resultado escaneo con Advance Ip scanner

Elaborado por: El investigador

Análisis de archivos log

Con relación al análisis de los archivos de registro, se elaboró un código en Python para los sistemas con distribución Unix/Linux para facilitar este proceso. Para los sistemas basados en Windows, se llevó a cabo un análisis manual mediante el uso del Visualizador de Eventos.

Código de análisis de archivos log

```
def analizar_archivo_log(archivo_ruta, patron_buscado, ip_objetivo):
    try:
        # Abre el archivo en modo de lectura
        with open(archivo_ruta, 'r') as archivo:
            # Imprime un mensaje indicando el inicio del análisis
            print(f"Analizando el archivo de registro en '{archivo_ruta}'...")
```

```
        # Lee todas las líneas del archivo y las almacena en una lista
        lineas = archivo.readlines()

        # Itera sobre cada línea del archivo junto con su número de línea (enumerado desde 1)
        for numero_linea, linea in enumerate(lineas, start=1):
            # Comprueba si la dirección IP objetivo y el patrón buscado están presentes en la línea actual
            if ip_objetivo in linea and patron_buscado in linea:
                # Si se cumplen las condiciones anteriores, imprime un mensaje indicando la coincidencia
                print(f"Se encontró '{patron_buscado}' en la línea {numero_linea} para la IP {ip_objetivo}:")
                # Imprime la línea completa que coincide con los criterios
                print(linea)

    # Manejo de excepción en caso de que el archivo no se encuentre
    except FileNotFoundError:
        print(f"El archivo '{archivo_ruta}' no fue encontrado.")

# Ruta del archivo de registro, patrón a buscar y dirección IP objetivo
archivo_log_ruta = 'Archivo.log'
patron_buscado = 'Patron busqueda'
ip_objetivo = 'Ip_objetivo'

# Llamada a la función para analizar el archivo
analizar_archivo_log(archivo_log_ruta, patron_buscado, ip_objetivo)
```

En el código se define una función llamada analizar_archivo_log que acepta tres argumentos: archivo_ruta, patron_buscado e ip_objetivo.

Se intenta abrir el archivo especificado en la ruta archivo_ruta en modo de lectura ('r').

Dentro de un bloque ***with***, el archivo se abrirá y se gestionará automáticamente el cierre una vez finalizado el bloque.

Se imprime un mensaje indicando que se está analizando el archivo de registro en la ruta especificada.

Se lee cada línea del archivo y se almacenan en una lista llamada lineas.

Se itera sobre cada línea del archivo junto con su número de línea correspondiente (comenzando desde 1) utilizando la función ***enumerate***.

Para cada línea, se comprueba si tanto el patrón buscado patron_buscado como la dirección IP objetivo ip_objetivo están presentes en la línea actual.

Si ambos criterios se cumplen, se imprime un mensaje que indica la coincidencia del patrón en la línea específica para la dirección IP objetivo.

Luego se imprime la línea completa en la que se encontró la coincidencia.

Se incluye una estructura de manejo de excepciones para el caso en que el archivo especificado no pueda ser encontrado (excepción FileNotFoundError).

En ese caso, se imprime un mensaje de error indicando que el archivo no fue encontrado.

Se proporcionan valores de ejemplo para las variables archivo_log_ruta, patron_buscado e ip_objetivo.

Luego, se llama a la función analizar_archivo_log con estos valores para iniciar el análisis del archivo.

La ejecución del código dio como resultado lo siguiente:

Analizando el archivo auth.log con el patron `Failed password` se encontró que se han registrado varios errores de inicio de sesión .

```
Analizando el archivo de registro en '/var/log/auth.log'
Se encontró 'Failed password' en la línea 1 para la IP 192.168.1.4:
Jul 23 10:00:15 server sshd[1234]: Failed password for user john from 192.168.1.4 port 22 ssh2
Se encontró 'Failed password' en la línea 3 para la IP 192.168.1.4:
Jul 23 10:05:45 server sshd[9012]: Failed password for invalid user admin from 192.168.1.4 port 22 ssh2
```

Para el análisis de registros log en los sistemas con sistemas Windows se realizó un proceso manual

Gráfico 37: Resultado de la ejecución del código

Elaborado por: El investigador

Se llevaron a cabo análisis adicionales de archivos, sin embargo, no se encontraron datos relevantes ni indicios que sugirieran la presencia de algún tipo de anomalía.

Como con el análisis del directorio /var/log/mail.log donde el resultado fue "FileNotFoundError", aunque es importante analizar los archivos con frecuencia junto con el monitorio de la red.

Análisis manual de los archivos log

Se llevó a cabo un análisis manual de los logs con el propósito de demostrar diversas técnicas de análisis de datos. Esta técnica es una de las más comunes en el ámbito de la ciberseguridad, ya que posibilita una comprensión más exhaustiva de la actividad en la red y resalta la relevancia de los registros log en la seguridad de dicha red.

El análisis se realizó remotamente utilizando el software AnyDesk, que es el programa designado por la institución para tareas a distancia. Con el objetivo de no interrumpir las actividades de los funcionarios, se eligió un horario adecuado para desempeñar esta labor.
Este proceso se llevó a cabo durante un período de cuatro días, con el propósito de analizar cada uno de los hosts utilizando el visor de Windows.

Gráfico 38: Visor de eventos de Windows

Elaborado por: El investigador

Se accedió al directorio C:\Windows\System32\winevt\Logs

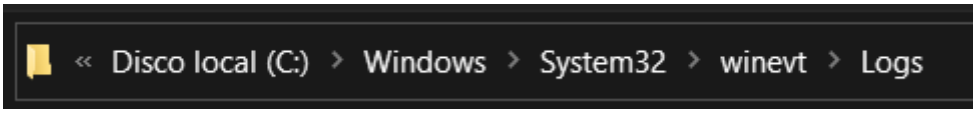


Gráfico 39: Directorio del archivo log en Windows

Elaborado por: El investigador

Se identificaron varios registros relacionados con el inicio de sesión fallido, con el ID 4625.

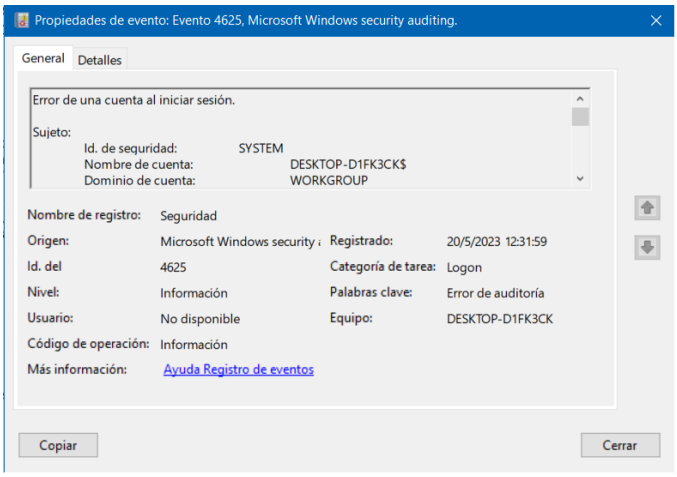


Gráfico 40: Registro del evento.

Elaborado por: El investigador

Al finalizar el análisis se descubrió el mismo registro en todos los dispositivos finales de red.

Anexo 2:

Manual de Threat Hunting.

UNIVERSIDAD TECNICA DE AMBATO

Facultad de Ingeniería en Sistemas, electrónica e industrial

2023

MANUAL DE APLICACIÓN DEL PROCESO PROACTVO THREAT HUNTING

Carrera de Tecnologías de la información

Bryan Jardiel

Avilés Vasco

CONTENIDO

RECONOCIMIENTO DE LA RED

Antes de comenzar con este proceso se debe conocer la infraestructura de la red, es necesario realizar un diagrama de la red para así tener una visión más amplia del entorno de trabajo.

ESQUEMA DE LA RED

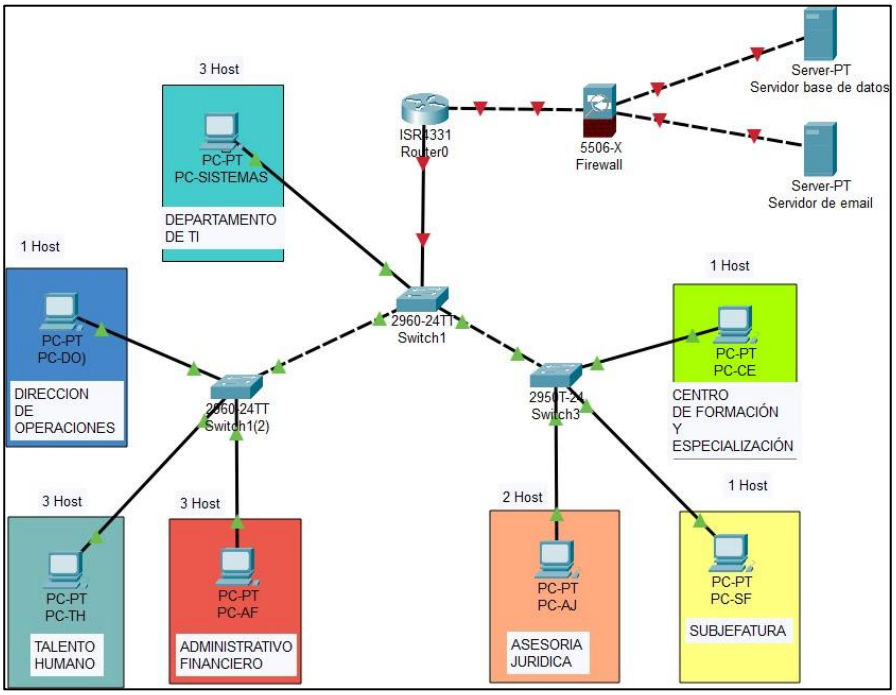


Gráfico 1: Esquema de la red

La red cuenta con un total de 19 host, entre ellos un firewall, 2 servidores y 14 dispositivos finales. Para un mejor conocimiento de la red es recomendable saber las características de los dispositivos.

FASES DEL PROCESO PROACTIVO THREAT HUNTING

La aplicación del proceso de Threat Hunting es una metodología proactiva que puede llevarse a cabo de diversas formas. Las fases a considerar en el proceso de Threat Hunting dependen en gran medida de las necesidades de la red, y en general, no existen reglas rígidas para su implementación. Sin embargo, existen ciertas bases desde las cuales se puede comenzar.

1. Generar Hipótesis.
2. Recopilar información.
3. Monitorear la red.
4. Identificar patrones de las amenazas.
5. Planificar las contramedidas.
6. Documentar los resultados de las contramedidas.

Dentro de la infraestructura de red del cuerpo de bomberos, las fases 1 y 2 no resultan necesarias. La fase 1 no se llevará a cabo debido a que el proceso se extenderá por toda la infraestructura de red en lugar de una zona específica. En cuanto a la fase 2, se prescinde de su realización dado que la topología de la red ya es conocida, al igual que los dispositivos y direcciones IP correspondientes.

Las que si tomaros en cuenta serán:

1. Monitoreo de la red.
2. Identificar patrones de las amenazas.
3. Planificar las contramedidas.
4. Documentar los resultados.

FASE 1: ESCANEO DE LA RED

PASO 1: Selección de herramientas

Antes de iniciar el proceso de escaneo, es esencial seleccionar las herramientas adecuadas que se van a emplear. Esta elección se basa en la facilidad de uso y en el conocimiento del personal. En este sentido, se ha decidido utilizar Wireshark, Nessus y Advanced Scan Ip, debido a la experiencia previa en el manejo de estas herramientas. Estas opciones se ajustan al nivel de destreza y familiaridad del equipo con el objetivo de llevar a cabo un monitoreo efectivo de la red. Se sugiere utilizar la última versión de los programas, y adicionalmente, utilizar otras herramientas acordes al avance tecnológico.

Es fundamental descargar e instalar todas las herramientas desde sus fuentes oficiales. En ningún caso se recomienda utilizar versiones piratas o ilegales, especialmente si alguna de estas herramientas es de pago.

PASO 2: Uso de wireshark.

1. Abrir Wireshark, asegurándose que esté conectado a la red.

Gráfico 2: Ejecución de Wireshark

2. Al hacer clic en el botón de inicio situado en la esquina superior izquierda, Wireshark iniciará la captura de todo el tráfico de red que atraviese la interfaz.

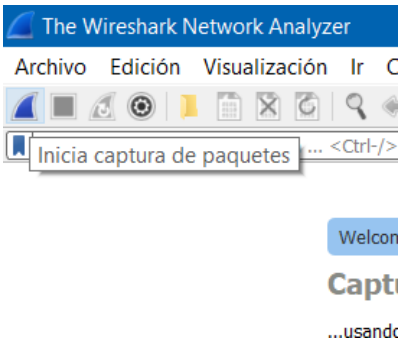


Gráfico 3: Inicio de Wireshark

3. Comenzar con el análisis de los registros en busca de actividades que puedan considerarse inusuales en la red. En este caso se han registrado múltiples intentos fallidos de inicio de sesión. Si estas actividades se perciben como una amenaza real, es fundamental tomar las medidas pertinentes o las que se consideren necesarias para garantizar la seguridad de la infraestructura de la red.

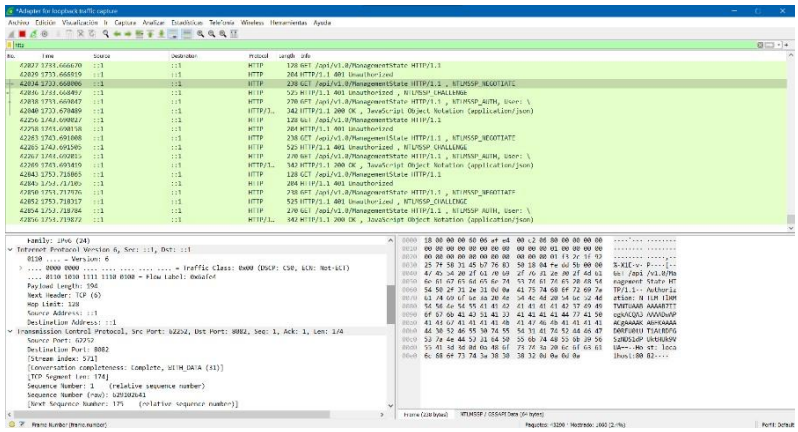


Gráfico 4: Resultados de Wireshark

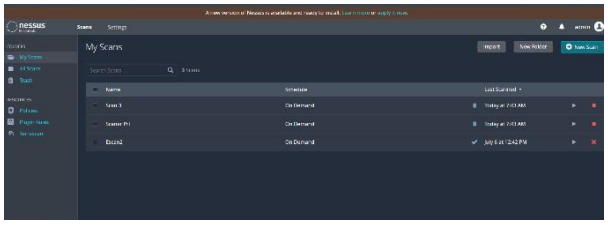
Nota: Si surge alguna actividad que se pueda considerar sospechosa, es fundamental iniciar con un análisis de su origen para determinar su posible naturaleza amenazante. En caso de confirmarse dicha amenaza, se deben aplicar las acciones pertinentes de forma inmediata. Además, se llevarán a cabo monitoreos semanales para detectar posibles amenazas en sus etapas iniciales.

PASO 3: Uso de Nessus

1. Para comenzar, como primer requisito será el crear un usuario y una contraseña con el cual se accederá al dashboard y servicios que ofrece Nessus.

Gráfico 5: Ejecución de Nessus

2. Para comenzar con el escaneo primero se deberá dar clic en "New scan" ubicado en la parte de superior derecho



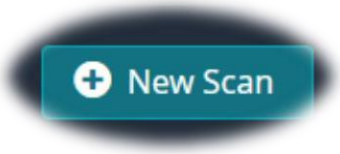


Gráfico 6: Nuevo escaneo

3. El siguiente paso es configurar el escaneo con las opciones que ofrece la herramienta. Se puede ver que existen varias opciones.

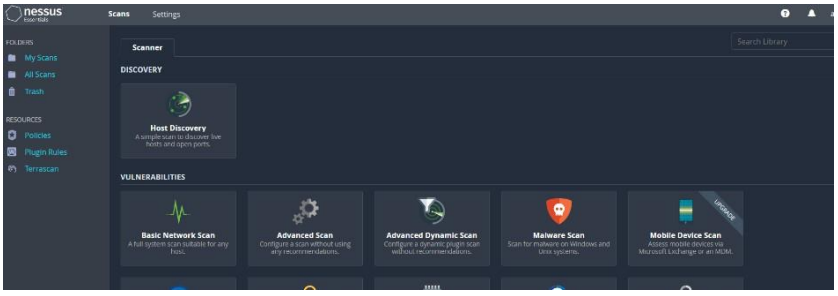


Gráfico 7: Opciones de Nessus

4. La opción más conveniente para la finalidad deseada es un escaneo del firewall en solitario para poder observar de mejor manera las vulnerabilidades que puedan existir.

   - **Configuración del escaneo en el firewall**

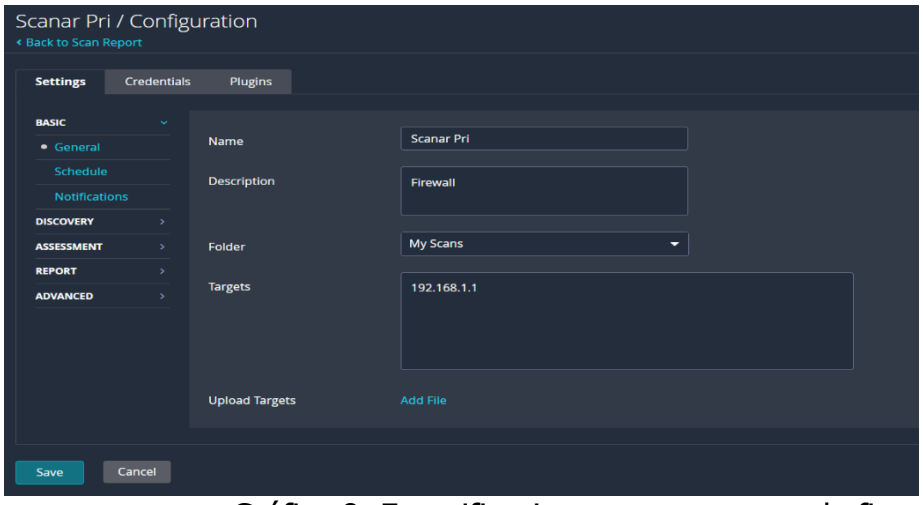


Gráfico 8: Especificaciones para escaneo de firewall

Se especifica la ip específica del firewall para realizar un escaneo y se procede con la ejecución de dicha configuración en busca de vulnerabilidades.

La duración del proceso varía dependiendo de las condiciones y configuraciones específicas del equipo. En este caso particular, el escaneo se completó en aproximadamente 10 minutos. Durante el proceso de escaneo, se identificaron un total de 18 vulnerabilidades. Algunas de ellas fueron calificadas como de riesgo bajo y el resto de información.

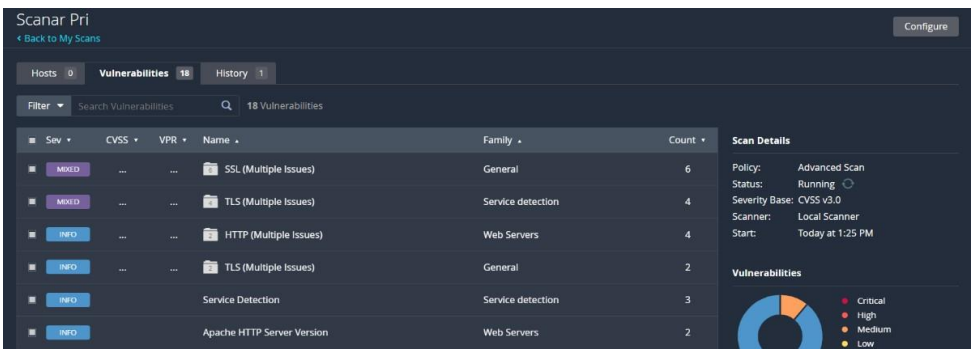


Gráfico 9: Resultados del escaneo del firewall

5. La configuración de la red se establece al introducir los rangos de direcciones IP. Dado que el objetivo es escanear todos los dispositivos en la red, es esencial ingresar un rango de direcciones IP que abarque esta necesidad.

   - **Configuración para la red general**

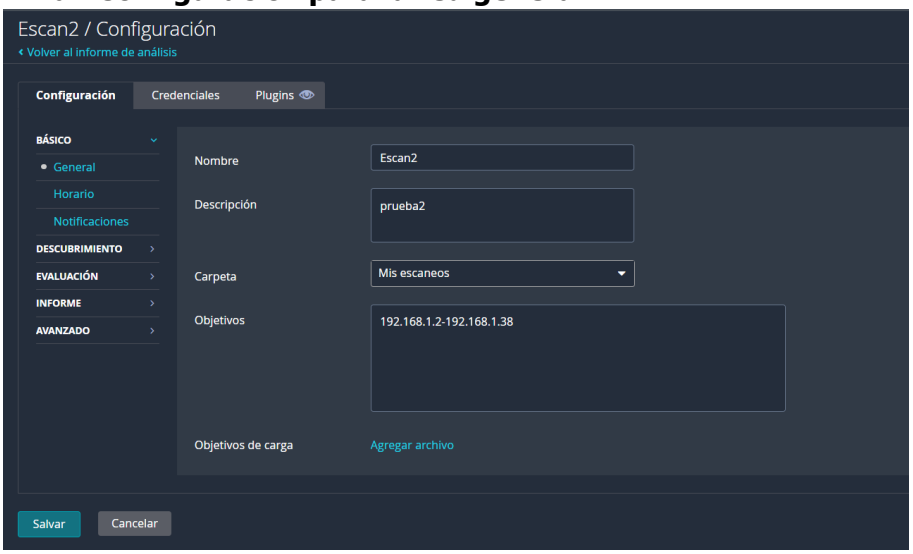


Gráfico 10: Especificaciones para escaneo de la red general

De manera similar, el tiempo aproximado para escanear la red está directamente influenciado por la cantidad de hosts que se incluyan en el proceso.

En esta ocasión, se escanearon un total de 16 hosts, lo que resultó en la detección de 25 vulnerabilidades. Estas vulnerabilidades han sido categorizadas en distintos niveles de gravedad: algunas fueron clasificadas como críticas, indicando un alto nivel de riesgo; otras como bajas, denotando un impacto menor en la seguridad; y finalmente, algunas se consideraron vulnerabilidades de información, que proporcionan valiosa información para posibles ataques.

Gráfico 11: Resultados del escaneo de la red general

Si se detectan vulnerabilidades en estado crítico, es esencial investigar la causa subyacente que las ha generado. En esta situación, es importante considerar las sugerencias brindadas por Nessus y tomar medidas adecuadas para abordarlas. Estas medidas pueden incluir la aplicación de parches, la reconfiguración de sistemas o la implementación de controles de seguridad adicionales para mitigar el riesgo asociado con estas vulnerabilidades críticas.

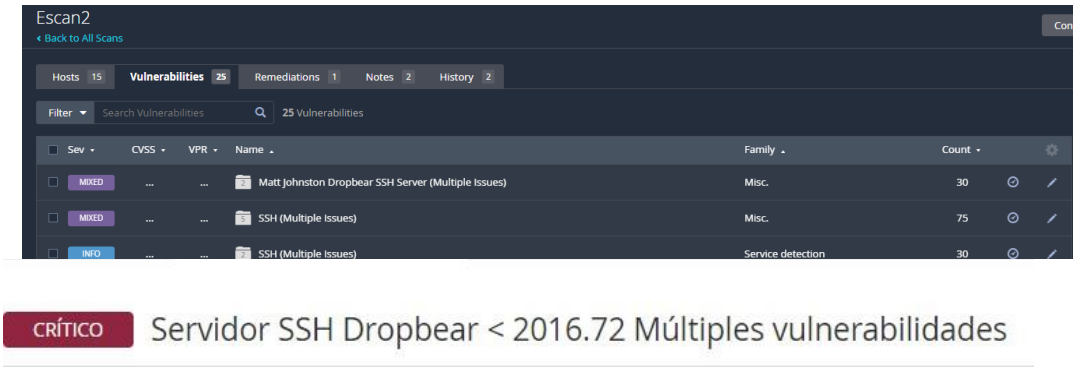


Gráfico 12: Vulnerabilidad de falta de actualización

La herramienta provee toda la información de la vulnerabilidad como se muestra a continuación:

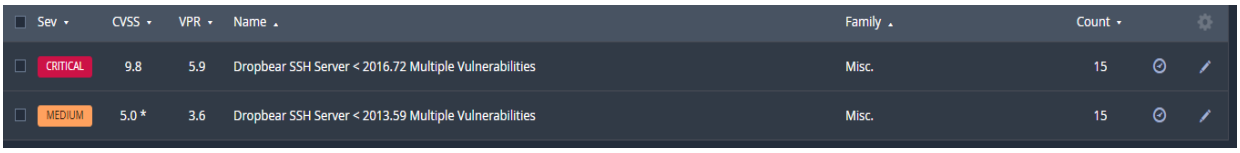


Gráfico 13: Vulnerabilidad de falta de actualización

Y como se mencionó anteriormente se debe tomar en cuenta la solución que propone Nessus.

Solución

Actualice a Dropbear SSH versión 2016.74 o posterior.

Gráfico 14: Versión a actualizar Dropbear SSH

Durante el proceso de escaneo, se identificó la ausencia de una política de actualización de parches para mantener los sistemas al día. Esta carencia puede dar lugar a problemas sustanciales en la red. Por lo tanto, es crucial emprender las acciones pertinentes para evitar poner en riesgo la integridad y seguridad de la infraestructura de la red.

Nota: Es importante destacar que este proceso de escaneo se debe llevar a cabo de manera mensual para garantizar un control continuo de las vulnerabilidades. Además, es recomendable realizar escaneos adicionales en momentos de cambios significativos en los sistemas. Estos cambios pueden incluir actualizaciones de servicios o la instalación de nuevo software que implique ajustes en las configuraciones y parámetros de la red. Estos escaneos preventivos son esenciales para asegurarse de que los cambios no introduzcan nuevas vulnerabilidades en el entorno de la red y para mantener un nivel óptimo de seguridad.

PASO 4: Uso de Advanced IP Scanner

Para iniciar la utilización de la herramienta Advanced IP Scanner, se llevan a cabo los siguientes pasos:

1. Primero se debe ejecutar la herramienta y lo siguiente será colocarel rango de red de los cuales se reportarán vulnerabilidades o comportamientos sospechosos.

Gráfico 15: Ejecución de Advance IP scanner

2. Dar clic en explorar y comenzará el escaneo.

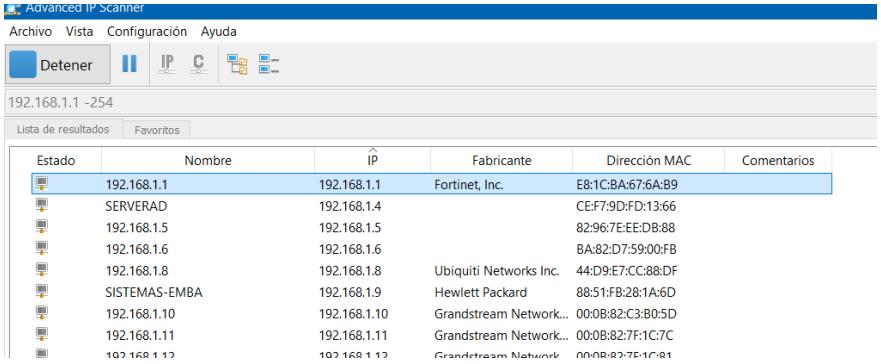


Gráfico 16: Exploración de Advance IP scanner

Durante este proceso de escaneo, se pudo constatar que los equipos se encuentran en un estado de operación normal y no se identificó la presencia de ningún dispositivo sospechoso en la red. Pero en caso de detectar un intruso se debe bloquear la dirección IP del sospechoso de la manera en la que sea pertinente.

Nota: Resulta fundamental llevar a cabo un monitoreo semanal utilizando esta herramienta, especialmente considerando que la red está expuesta a posibles intrusiones debido a la debilidad en las medidas de seguridad, particularmente en lo que respecta a las contraseñas utilizadas.

Mantener un monitoreo constante contribuirá significativamente a identificar y abordar oportunamente cualquier amenaza potencial que pueda surgir.

PASO 5: Análisis de archivos log.

1. Revisar la presencia de registros que se puedan considerar sospechosos en los sistemas que forman parte de la red. Con la ayuda del siguiente código se puede analizar un análisis adecuado en los sistemas con sistemas operativos Unix/Linux.

```
def analizar_archivo_log(archivo_ruta, patron_buscado, ip_objetivo):
    try:
        # Abre el archivo en modo de lectura
        with open(archivo_ruta, 'r') as archivo:
            # Imprime un mensaje indicando el inicio del análisis
            print(f"Analizando el archivo de registro en '{archivo_ruta}'...")

            # Lee todas las líneas del archivo y las almacena en una lista
            lineas = archivo.readlines()

            # Itera sobre cada línea del archivo junto con su número de línea (enumerado desde 1)
            for numero_linea, linea in enumerate(lineas, start=1):
                # Comprueba si la dirección IP objetivo y el patrón buscado están presentes en la línea actual
                if ip_objetivo in linea and patron_buscado in linea:
                    # Si se cumplen las condiciones anteriores, imprime un mensaje indicando la coincidencia
                    print(f"Se encontró '{patron_buscado}' en la línea {numero_linea} para la IP {ip_objetivo}:")
                    # Imprime la línea completa que coincide con los criterios
                    print(linea)

    # Manejo de excepción en caso de que el archivo no se encuentre
    except FileNotFoundError:
        print(f"El archivo '{archivo_ruta}' no fue encontrado.")

# Ruta del archivo de registro, patrón a buscar y dirección IP objetivo
archivo_log_ruta = 'Archivo.log'
patron_buscado = 'Patron busqueda'
ip_objetivo = 'Ip_objetivo'

# Llamada a la función para analizar el archivo
analizar_archivo_log(archivo_log_ruta, patron_buscado, ip_objetivo)
```

Gráfico 17: Código de análisis de archivos log

El cual necesita de parámetro la ruta del archivo, un patrón especifico y una ip la cual será el objetivo de análisis. Se debe reemplazar los datos dependiendo de las necesidades del contexto.

Un ejemplo es el siguiente:

```
Analizando el archivo de registro en '/var/log/auth.log'
Se encontró 'Failed password' en la línea 1 para la IP 192.168.1.4:
Jul 23 10:00:15 server sshd[1234]: Failed password for user john from 192.168.1.4 port 22 ssh2
Se encontró 'Failed password' en la línea 3 para la IP 192.168.1.4:
Jul 23 10:05:45 server sshd[9012]: Failed password for invalid user admin from 192.168.1.4 port 22 ssh2
```

Gráfico 18: Ejemplo de análisis de archivo log.

En el directorio '/var/log/auth.log', se identificó el mensaje 'Failed password', el cual queda registrado cuando un intento de inicio de sesión no tiene éxito. Además de este registro, se incluye la dirección IP del dispositivo involucrado en la acción y el puerto por el cual se llevó a cabo.

La siguiente tabla muestra información que se puede usar de base para el análisis de los archivos log reemplazando los parámetros en el código proporcionado anteriormente.

Patrón de Archivo Log	Descripción
Failed login	Registros de intentos fallidos de inicio de sesión en archivos de autenticación.
Access denied	Entradas que indican acceso denegado a ciertos recursos o servicios.
Successful login	Registros de acceso exitoso a sistemas o aplicaciones.
File not found	Entradas que indican que se intentó acceder a un archivo que no existe.
Connection timeout	Entradas que indican que una conexión se cerró debido a un tiempo de espera agotado.
Malware detection	Registros que indican la detección de archivos maliciosos por parte de software antivirus.

Nota: El escaneo de los archivos log se debe realizar a la par del escaneo, es decir si realiza un escaneo con cualquier herramienta también debe realizar el análisis del archivo log, y en caso de encontrar alguna actividad sospechosa como el registro de varios intentos fallidos de inicio de sesión se debe cambiar todas las contraseñas de los usuarios y los sistemas de la red.

2. Analizar de manera manual el registro de eventos en Windows para complementar la información que se debe tener en cuenta para múltiples situaciones dependiendo del id del evento y determinar si puede llegar a ser una amenaza real. Por ejemplo:

Paso 1: Ingresar al visor de eventos de Windows

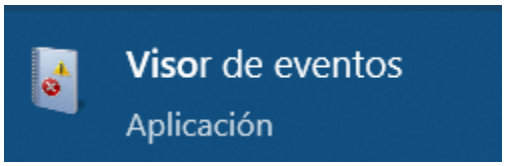


Gráfico 19: Visor de eventos

Paso 2: Para analizar los archivos donde se registran los intentos fallidos de inicio de sesión, es necesario acceder a los registros relacionados con la seguridad e identificar el ID del evento 4625 que en este caso indica un intento fallido de inicio de sesión.

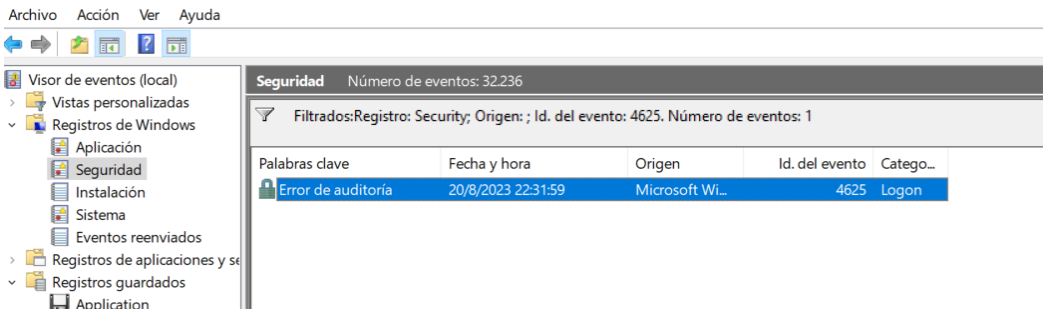


Gráfico 20: Búsqueda de evento

El Visor de Eventos de Windows alberga información esencial que se puede analizar. A continuación, se presenta una tabla que detalla los eventos de Windows que deben ser considerados.

Nombre	ID	Nivel	Evento	Fuentes del evento
Account Lockouts	4740	Informational	Security	Microsoft-Windows-Security-Auditing
User Added to Privileged Group	4728, 4732, 4756	Informational	Security	Microsoft-Windows-Security-Auditing
Security-Enabled group Modification	4735	Informational	Security	Microsoft-Windows-Security-Auditing
Successful User Account Login	4624	Informational	Security	Microsoft-Windows-Security-Auditing
Failed User Account Login	4625	Informational	Security	Microsoft-Windows-Security-Auditing
Account Login with Explicit Credentials	4648	Informational	Security	Microsoft-Windows-Security-Auditing

NOTA: El análisis de estos archivos se debe realizar a la par del análisis de archivos log en los sistemas basados en sistemas Unix/Linux y en caso de determinar que se trata de actividad sospechosa realizar las medidas necesarias para salvaguardar la infraestructura de red.

FASE 2: Identificar patrones de las posibles amenazas.

PASO 1: Relacionar las vulnerabilidades con los posibles ataques que se pueden realizar.

Tipo de ataques	**Archivos Log**	**Nro Evento / Patron evento**	**Puertos**	**Descripción**
Ataque de fuerza bruta	C:\Windows\System32\winevt\Logs	4625 Failed login	SSH (22)	Adivinar o descifrar contraseñas mediante la prueba sistemática detodas las combinacionesposibles
Ataque de DDoS	/var/log/syslog	GET /	HTTP (80), HTTPS (443)	Sobrecargar unservicio o recurso contráfico malicioso, causando la indisponibilidaddel mismo

Ataque de inyección de código	NINGUNO	NINGUNO	HTTP (80), HTTPS (443)	Insertar códigomalicioso en una aplicacióno sistema vulnerable
Ataque de phishing	opt/zimbra/log/mailbox.log	URL	SSH (22)	Engañar a los usuarios para obtener información confidencial,como contraseñas o datos bancarios
Ataque de Ransomware	NINGUNO	NINGUNO	NetBios(139), SMB (445)	Cifrar los archivos y sistemas de unavíctima y exigir un rescate a cambio de su liberación

Una vez claros los tipos de ataques relacionadas con las vulnerabilidades encontradas, se procede con las planificaciones.

La planificación de las contramedidas se debe realizar conforme a las necesidades y debilidades de la infraestructura de red con el fin de fortalecer y salvaguardar la integridad de la red.

FASE 3: Contramedidas

Para planificar las contramedidas se toman en cuenta las distintas amenazas que pueden provocar las vulnerabilidades detectadas, en este caso en concreto y que pueden servir de guía para futuras aplicaciones, se planificaron las siguientes contramedidas.

Contramedida P-1-1

- La planificación que sigue se basa en la detección de diversas vulnerabilidades que podrían potenciar un ataque de fuerza bruta. Como respuesta a esta situación, se planificó una política de creación para contraseñas robustas, lo que contribuirá significativamente a reforzar las áreas identificadas como vulnerables.

Código	**Responsable**		**Prioridad**	
P-1-1	Administrador de TI		Alta	
Paso	**Actividad**	**Descripción**	**Archivos Log**	**Mitigación**
1	Uso de contraseñas fuertes	Educar a los usuarios sobre la importancia de utilizar contraseñas seguras, establecer cumplir una política de contraseñas seguras	Registros de cambio de contraseñas	Establecer una política para la generación de contraseñas robustas para los usuarios de la institución

Contramedida P-2-1

Esta planificación tiene pensado configurar reglas de firewall para bloquear direcciones ip que realicen solicitudes redundantes a recursos específicos.

Código	**Responsable**		**Prioridad**	
P-2-1	Asistente de TI		**Alto**	
Paso	**Actividad**	**Descripción**	**Archivos Log**	**Mitigación**
1	Implementar un firewall de red.	Formular Configuraciones para el firewall de red para filtrar y bloquear tráfico sospechoso o malicioso.	Registros del Firewall	Generar reglas de firewall para bloquear direcciones IP sospechosas o patrones de tráfico asociados a ataques DDoS.

Contramedida P-3-1

- La detección de servicios desactualizados puede resultar crítica en el caso del firewall ya que se puede producir un ataque de inyección de código (CVE-2020-29015) por falta de actualización del FortiWeb. Por esta razón, se ha implementado un control para la gestión de versiones de los programas.

	Responsable		**Prioridad**	
P-2-2	Asistente de TI		**Alto**	
Paso	**Actividad**	**Descripción**	**Archivos Log**	**Mitigación**
1	Actualización y parcheo de sistemas	Mantener los sistemas y aplicaciones actualizados con los últimos parches de Seguridad	Registros de actualización de sistemas	Generar una política de gestión de parches y mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad paracorregir vulnerabilidades conocidas y minimizarla exposición a posibles ataques.

FASE 4: Políticas de seguridad

Planificación P-1-1

Política para la generación de contraseñas fuertes

Se creó una política de generación de contraseñas, la cual fortalecerá la asignación de contraseñas. La política consiste en las siguientes normas:

1. **Longitud:** Esta regla establece que la longitud de la contraseña deberá ser mínima de 12 caracteres.

2. **Combinación:** La contraseña deberá combinarse con caracteres alfanuméricos y especiales. Por ejemplo, al menos una letra mayúscula, unaletra minúscula, un número y un carácter especial sin una combinación especifica.
3. **Información personal:** Prohibido el uso de información personal como nombres, fechas de nacimiento o números de identidad.
4. **Caducidad y cambio regular:** Establecer una política de caducidad de contraseñas que requiera a los usuarios cambiar sus contraseñas cada 90días o según lo establecido por la organización.
5. **Restricción de reutilización:** Impedir que los integrantes de la red utilicen contraseñas previamente utilizadas, manteniendo un historial de contraseñas anteriores y evitando su reutilización durante un período de tiempo determinado.

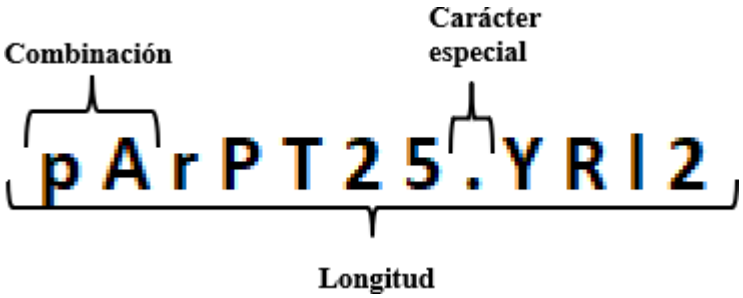


Gráfico 21: Políticas de contraseñas

Planificación P-2-1

Reglas para la configuración del Firewall

REGLA 1

1. **config firewall address:**

Este comando indica la configuración una dirección IP en el firewall.

- El siguiente comando edit "IP_sospechosa_1" crea una nueva entrada para una dirección IP sospechosa específica. Puedes reemplazar "IP_sospechosa_1" con un nombre más descriptivo.
- set subnet <IP_sospechosa_1>/32 establece la dirección IP y la máscara de subred. En este caso, se utiliza "/32" para especificar una sola dirección IP.

2. **config firewall policy:**

Este comando indica a configuración una política de firewall.

- El siguiente comando edit 1 crea una nueva entrada para una política de firewall específica. Puedes reemplazar "1" con un número de política diferente si es necesario.
- set name "Bloquear IP sospechosa 1" asigna un nombre descriptivo a la política de firewall.
- set srcintf "LAN" especifica la interfaz de origen desde donde se originaráel tráfico. Puedes reemplazar "LAN" con la interfaz correspondiente en tu entorno.
- set dstintf "WAN" especifica la interfaz de destino a la que se dirigirá eltráfico. Puedes reemplazar "WAN" con la interfaz correspondiente en tuentorno.
- set srcaddr "IP_sospechosa_1" indica la dirección IP sospechosa que se bloqueará. Debe coincidir con la entrada configurada anteriormente en config firewall address.

- set action deny establece la acción a "denegar", lo que significa que el tráfico de la dirección IP sospechosa será bloqueado.
- set schedule "always" indica que la política estará activa en todomomento.

```
config firewall address
    edit "IP_sospechosa_1"
        set subnet <IP_sospechosa_1>/32
        next
    end

config firewall policy
    edit 1
        set name "Bloquear IP sospechosa 1"
        set srcintf "LAN"
        set dstintf "WAN"
        set srcaddr "IP_sospechosa_1"
        set action deny
        set schedule "always"
        next
    end
```

Gráfico 22: Regla 1 para configuración de firewall

REGLA 2

1. config firewall address

- edit "Rango_IP_sospechoso": Se crea una entrada en la configuración de direcciones del firewall con el nombre "Rango_IP_sospechoso". Esto permite definir un rango de direcciones IP sospechosas que se utilizará posteriormente en una política de firewall.
- set start-ip <IP_inicial>: Se establece la dirección IP inicial del rango sospechoso.
- set end-ip <IP_final>: Se establece la dirección IP final del rango sospechoso.
- next: Se indica que se ha terminado la configuración de la dirección y sepasa al siguiente elemento.

2. config firewall policy

- **edit 2:** Se crea una entrada en la configuración de políticas del firewall conel número 2
- **set name "Bloquear Rango de IP sospechoso":** Se asigna un nombre descriptivo a esta política de firewall, que en este caso indica que se bloqueará un rango de direcciones IP sospechosas.
- **set srcintf "LAN":** Se especifica la interfaz de origen de la política, en este caso, "LAN" (red local).
- **set dstintf "WAN":** Se especifica la interfaz de destino de la política, en este caso, "WAN" (red externa o Internet).
- **set srcaddr "Rango_IP_sospechoso":** Se indica que la dirección de origen permitida para esta política es el rango de direcciones IP sospechosas previamente definido.
- **set action deny:** Se establece la acción de la política como "deny" (denegar), lo que significa que se bloquearán todas las conexiones provenientes de las direcciones IP sospechosas.
- **set schedule "always":** Se establece el horario de aplicación de la política como "always" (siempre), lo que significa que la política estará en efecto entodo momento.
- **next:** Se indica que se ha terminado la configuración de la política y se pasaal siguiente elemento.

```
config firewall address
    edit "Rango_IP_sospechoso"
        set start-ip <IP_inicial>
        set end-ip <IP_final>
        next
    end

config firewall policy
    edit 2
        set name "Bloquear Rango de IP sospechoso"
        set srcintf "LAN"
        set dstintf "WAN"
        set srcaddr "Rango_IP_sospechoso"
        set action deny
        set schedule "always"
        next
    end
```

Gráfico 23: Regla 2 configuración de firewall

Planificación P-2-2

POLÍTICA DE SEGURIDAD GENERADA PARA MANTENER ACTUALIZADAS LOS SISTEMAS.

1. **Objetivo:**
   - Mantener los sistemas y aplicaciones actualizados con los últimos parchesde seguridad para corregir vulnerabilidades conocidas y minimizar la exposición a posibles ataques.
2. **Responsabilidades:**
   - **Equipo de Seguridad:**

     Realizar seguimiento de las actualizaciones de seguridad disponibles para los sistemas y aplicaciones utilizados en la infraestructura.
     - Evaluar la criticidad de los parches y determinar su aplicabilidad en función de los riesgos y la compatibilidad con la infraestructura existente.
     - Coordinar y planificar la implementación de los parches de seguridaden colaboración con los administradores de sistemas y los responsables de las aplicaciones.

- **Administradores de Sistemas:**
  - Mantener un inventario actualizado de los sistemas y aplicaciones utilizados en la infraestructura.
  - Monitorear y recibir las notificaciones de los proveedores sobre las actualizaciones de seguridad disponibles.
  - Realizar pruebas de compatibilidad de los parches en entornos de desarrollo o pruebas antes de implementarlos en los entornos de producción
  - Implementar los parches de seguridad de acuerdo con la planificación establecida por el equipo de seguridad.

3. Proceso de Gestión de Parches:

a) Identificación de Parches:

- Recopilar información sobre los parches de seguridad disponibles a travésde fuentes confiables, como los proveedores de sistemas y aplicaciones,sitios web de seguridad y boletines de seguridad.
- Evaluar la criticidad de los parches en función de las vulnerabilidades que corrigen y su impacto potencial en la infraestructura.

b) Evaluación y Priorización de Parches:

- Determinar la aplicabilidad de los parches a los sistemas y aplicaciones utilizados en la infraestructura.
- Evaluar el riesgo asociado con la vulnerabilidad corregida por el parche y establecer una prioridad basada en la criticidad y el impacto potencial.

c) Pruebas y Validación:

- Realizar pruebas de compatibilidad de los parches en entornos de desarrollo o pruebas para garantizar que no afecten el funcionamiento normal de los sistemas y aplicaciones.
- Validar la efectividad de los parches mediante pruebas de seguridad adicionales para verificar que las vulnerabilidades corregidas estén mitigadas**.**

d) Implementación de Parches:

- Establecer una planificación para la implementación de los parches, considerando los tiempos de mantenimiento programados y el impacto enlos usuarios y los servicios.
- Implementar los parches en los entornos de producción siguiendo las mejores prácticas de implementación y minimizando las interrupciones enel servicio.

e) Monitoreo y Seguimiento:

- Realizar un seguimiento continuo de las actualizaciones de seguridad y las vulnerabilidades conocidas para garantizar que los sistemas y aplicaciones estén siempre actualizados.
- Monitorear los sistemas y aplicaciones en busca de posibles problemas o incompatibilidades causadas por los parches implementados.

4. Comunicación y Concientización:

- Informar a los usuarios y las partes interesadas sobre la importancia de mantener los sistemas y aplicaciones actualizados.
- Proporcionar orientación y materiales educativos sobre las mejores prácticas de seguridad y la importancia de aplicar los parches de seguridad.

ANALISIS.

A continuación, se presenta un análisis de la funcionalidad y los resultados obtenidos alaplicar esta metodología:

Funcionalidad del Threat Hunting:

- El Threat Hunting permitió identificar amenazas y vulnerabilidades de manera proactiva, en lugar de esperar a que se produzca un incidente de seguridad.
- La metodología involucró un análisis de los registros de eventos, logs y tráfico de red para detectar patrones y anomalías que podrían indicar actividad maliciosa.
- El Threat Hunting tuvo en cuenta el contexto de la red y la organización, permitiendo adaptar las técnicas y herramientas de detección a las necesidades específicas.

Anexo 3:
Reporte Nessus

Escan2

Report generated by Nessus™

Thu, 06 Jul 2023 12:42:03 SA Pacific Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.1.11

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report

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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.12

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.13

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.14

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.15

Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	123464	Grandstream SIP Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	21642	Session Initiation Protocol Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.16

Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	123464	Grandstream SIP Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	21642	Session Initiation Protocol Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.17

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.18

Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	70657	SSH Algorithms and Languages Supported

INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.22

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.24

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.25

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.26

Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	123464	Grandstream SIP Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	21642	Session Initiation Protocol Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.27

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.29

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.30

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0score is shown

192.168.1.38

Vulnerabilities Total: 27

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	5.9	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	103515	Grandstream Phone Web Interface Detection
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	106628	lighttpd HTTP Server Detection

* indicates the v3.0 score was not available;
the v2.0score is shown