

UNIVERSIDAD NACIONAL PEDRO RUÍZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE INGENIERÍA EN
COMPUTACIÓN E INFORMÁTICA



TESIS

**“Detección de ataques y mitigación de vulnerabilidades de los servicios web de
la municipalidad provincial de Chiclayo”**

Presentada para obtener el Título Profesional de:
Ingeniero (a) en Computación e Informática

INVESTIGADORES:

Bach. Flores Miñope Rossmery
Bach. Ticona Tapia Brenis Fernando

ASESOR:

Dr. Ing. Carrión Barco Gilberto

LAMBAYEQUE, 2024

UNIVERSIDAD NACIONAL PEDRO RUÍZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE INGENIERÍA EN
COMPUTACIÓN E INFORMÁTICA



TESIS

**“Detección de ataques y mitigación de vulnerabilidades de los servicios web
de la municipalidad provincial de Chiclayo”**

Presentado por:

Bach. Flores Miñope Rossmery
Autor

Bach. Ticona Tapia Brenis Fernando
Autor

Dr. Ing. Carrión Barco Gilberto
Asesor

UNIVERSIDAD NACIONAL PEDRO RUÍZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE INGENIERÍA EN
COMPUTACIÓN E INFORMÁTICA



TESIS

**“Detección de ataques y mitigación de vulnerabilidades de los servicios web de
la municipalidad provincial de Chiclayo”**

Aprobado por los Miembros del Jurado:

Dr. Ing. Denny John Fuentes Adrianzén
Presidente

M. Sc. Ing. Janet Rosario Aquino Lalupú
Secretario

Mg. Ing. Freddy William Campos Flores
Vocal

ACTA DE SUSTENTACIÓN (Copia)



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DECANATO
Ciudad Universitaria - Lambayeque



ACTA DE SUSTENTACIÓN VIRTUAL N° 003-2024-D/FACFyM

Siendo las 10:00 am del día jueves 01 de febrero del 2024, se reunieron vía plataforma virtual, <https://meet.google.com/eku-xsyb-mgn?authuser=0> los miembros del jurado evaluador de la Tesis titulada:

"DETECCIÓN DE ATAQUES Y MITIGACIÓN DE VULNERABILIDADES DE LOS SERVICIOS WEB DE LA MUNICIPALIDAD PROVINCIAL DE CHICLAYO"

Designados por Resolución N° 302-2023-VIRTUAL-D/FACFyM de fecha 14 de abril del 2023.

Con la finalidad de evaluar y calificar la sustentación de la tesis antes mencionada, conformada por los siguientes docentes:

Dr. Ing. Denny John Fuentes Adrianzén	Presidente
M.Sc. Ing. Janet del Rosario Aquino Lalupú	Secretario
Mg. Ing. Freddy William Campos Flores	Vocal

La tesis fue asesorada por el Dr. Ing. Gilberto Carrión Barco, nombrado por Resolución N° 302-2023 D/FACFyM de fecha 14 de abril del 2023.


El Acto de Sustentación fue autorizado por Resolución N° 067-2024 D/FACFyM de fecha 19 de enero del 2024.

La Tesis fue presentada y sustentada por los Bachilleres: *Ticona Tapia Brenis Fernando y Flores Miñope Rossmery* y tuvo una duración de 40 minutos.

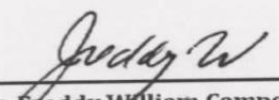
Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado se procedió a la calificación respectiva, otorgándole el Calificativo de **18 (Dieciocho)** en la escala vigesimal, mención **Muy Bueno**.

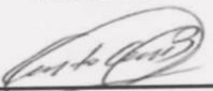
Por lo que quedan aptos para obtener el Título Profesional de **Ingeniero en Computación e Informática**, de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ciencias Físicas y Matemáticas y la Universidad Nacional Pedro Ruiz Gallo.

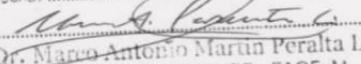
Siendo las 10:50 am se dio por concluido el presente acto académico, dándose conformidad al presente acto con la firma de los miembros del jurado.


Dr. Ing. Denny John Fuentes Adrianzén
Presidente


M.Sc. Ing. Janet del Rosario Aquino Lalupú
Secretario


Mg. Ing. Freddy William Campos Flores
Vocal


Dr. Ing. Gilberto Carrión Barco
Asesor

CERTIFICO: Que, es copia fiel del original
Fecha: 02/02/2024

Dr. Marco Antonio Martín Peralta Lui
SECRETARIO DOCENTE - FACFyM
VÁLIDO PARA TRÁMITES INTERNOS DE LA UNPRG

CONSTANCIA DE SIMILITUD 01



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
UNIDAD DE INVESTIGACION



CONSTANCIA DE SIMILITUD N° 006-2024- VIRTUAL-UI-FACFyM

El que suscribe, Director de la Unidad de Investigación de la Facultad de Ciencias Físicas y Matemáticas de la Universidad Nacional Pedro Ruiz Gallo, hace constar:

Que, el (la) Bachiller **TICONA TAPIA BRENIS FERNANDO**, de la Escuela Profesional de **COMPUTACION E INFORMATICA**, ha cumplido con presentar la **SIMILITUD DE ORIGINALIDAD DE LA TESIS (TURNITIN)**, como requisito indispensable para la sustentación de la tesis, según detalle:}

- **TÍTULO DE LA TESIS:** “DETECCIÓN DE ATAQUES Y MITIGACIÓN DE VULNERABILIDADES DE LOS SERVICIOS WEB DE LA MUNICIPALIDAD PROVINCIAL DE CHICLAYO.”

- **ÍNDICE DE SIMILITUD:** 13%

- **ASESOR:** Dr. Ing. Gilberto Carrión Barco

Se expide la presente constancia, para la tramitación del Título Profesional, dispuesto en la Directiva para la evaluación de originalidad de los documentos académicos, de investigación formativa y para la obtención de Grados y Títulos de la UNPRG.

Lambayeque, 26 de febrero de 2024

Dr. WALTER ARRIAGA DELGADO
DIRECTOR - UNIDAD DE INVESTIGACIÓN

CONSTANCIA DE SIMILITUD 02



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
UNIDAD DE INVESTIGACION



CONSTANCIA DE SIMILITUD N° 005-2024- VIRTUAL-UI-FACFyM

El que suscribe, Director de la Unidad de Investigación de la Facultad de Ciencias Físicas y Matemáticas de la Universidad Nacional Pedro Ruiz Gallo, hace constar:

Que, el (la) Bachiller **FLORES MIÑOPE ROSSMERY**, de la Escuela Profesional de **INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA**, ha cumplido con presentar la **SIMILITUD DE ORIGINALIDAD DE LA TESIS (TURNITIN)**, como requisito indispensable para la sustentación de la tesis, según detalle:

- **TÍTULO DE LA TESIS:** “DETECCIÓN DE ATAQUES Y MITIGACIÓN DE VULNERABILIDADES DE LOS SERVICIOS WEB DE LA MUNICIPALIDAD PROVINCIAL DE CHICLAYO.”

- **ÍNDICE DE SIMILITUD:** 13%

- **ASESOR:** Dr. Ing. Gilberto Carrión Barco

Se expide la presente constancia, para la tramitación del Título Profesional, dispuesto en la Directiva para la evaluación de originalidad de los documentos académicos, de investigación formativa y para la obtención de Grados y Títulos de la UNPRG.

Lambayeque, 26 de febrero de 2024

Dr. WALTER ARRIAGA DELGADO
DIRECTOR - UNIDAD DE INVESTIGACIÓN

DECLARACIÓN JURADA DE ORIGINALIDAD

Nosotros, Flores Miñope Rossmery y Ticona Tapia Brenis Fernando en condición de Bachilleres en Ingeniería en Computación e Informática, investigadores principales, y el Dr. Ing. Carrión Barco Gilberto, asesor del Trabajo de Investigación “Detección de ataques y mitigación de vulnerabilidades de los servicios web de la municipalidad provincial de Chiclayo”, declaramos bajo juramento que este trabajo no ha sido plagiado, ni contiene datos falsos. En caso se evidenciara lo contrario, asumimos responsablemente la anulación de este informe y por ende el proceso administrativo a que hubiera lugar, que puede conducir a la anulación del título o grado emitido como consecuencia de este informe.

Lambayeque, febrero 2024



Bach. Flores Miñope Rossmery

Autora



Bach. Ticona Tapia Brenis Fernando

Autor



Dr. Ing. Carrión Barco Gilberto

Asesor

DEDICATORIA

A Dios por ser el siempre mi guía, a mis padres Mery Miñope Effio y Pedro Flores Farroñay, a mis hermanos Leydi Karen y Pedro David, a mi abuelita Zoila, a mi amor Brenis Fernando y a mí tío Jose B. Flores, por ser ellos mi motor y motivo, que me demostraron siempre su amor, me alentaron y apoyaron incondicionalmente en todo momento para poder cumplir mis metas. Sin ellos no lo hubiese logrado.

Rossmery.

Dedico este proyecto a mis padres María y Alejandro por el sacrificio y esfuerzo realizado, a mis hermanos Estrella y Brayan por su apoyo incondicional, a mis abuelitas Armandina Alarcón y Ascensión Valdivia, que desde el cielo me iluminan para salir adelante, a mi amor y compañera de tesis Rossmery por su tiempo y dedicación y a mi familia por ser mi mayor motivación para poder cumplir mis metas.

Brenis f.

AGRADECIMIENTO

Primeramente, agradecemos a Dios, por la vida, la salud que nos brinda y por siempre guiar nuestros caminos para ser personas y profesionales de bien.

A nuestros padres y hermanos por su amor y apoyo incondicional para lograr nuestros objetivos y por estar siempre cuando los necesitamos, inculcándonos valores y brindándonos consejos, sin ellos no habiéramos llegado hasta donde estamos.

A los docentes de nuestra querida escuela profesional de Ingeniería en Computación e Informática, por brindarnos los conocimientos necesarios para desarrollarnos profesionalmente. A nuestro asesor, el doctor ingeniero Gilberto Carrión Barco por su tiempo, su apoyo para el desarrollo de nuestra tesis, por guiarnos y brindarnos consejos para crecer profesionalmente.

Los Autores.

ÍNDICE

ACTA DE SUSTENTACIÓN (Copia).....	I
CONSTANCIA DE SIMILITUD 01	II
CONSTANCIA DE SIMILITUD 02	III
DECLARACIÓN JURADA DE ORIGINALIDAD	IV
DEDICATORIA	V
AGRADECIMIENTO	VI
RESUMEN	XIII
ABSTRACT.....	XIV
INTRODUCCIÓN	1
CAPÍTULO I. DISEÑO TEÓRICO	4
1.1. Antecedentes	4
1.1.1. Antecedentes Internacionales.....	4
1.1.2. Antecedentes Nacionales	5
1.1.3. Antecedentes Regionales	6
1.2. Bases teóricas	7
1.2.1. Ataque Informático	7
1.2.1.1 Ataques de Reconocimiento.....	7
1.2.1.2 Ataques de acceso	8
1.2.1.3 Ataques de Denegación de Servicio DoS.....	10
1.2.2. Vulnerabilidad Informática	11
1.2.3. Servicio Web.....	12
1.2.4. Servicios Web Municipales	13
1.2.5. Ethical Hacking.....	15
1.2.6. Pentesting.....	17
1.2.7. SIEM.....	17
1.2.7.1 Capacidades de un SIEM	18
1.2.7.2 Ventajas de un SIEM.....	20
1.2.8. Ciberseguridad	21
1.2.9. Software de virtualización Virtual Box	22

1.2.10. Sistema Operativo Kali Linux	23
1.2.11. Sistema Operativo Centos	24
1.2.12. Sistema Operativo Security Onion.....	25
1.3. Bases conceptuales	27
1.3.1. Operacionalización de Variables	27
CAPÍTULO II. MÉTODOS Y MATERIALES.....	28
2.1. Tipo de Investigación	28
2.2. Diseño de contrastación de hipótesis	28
2.3. Población y muestra	30
2.4. Técnicas, instrumentos, equipos y materiales	31
CAPÍTULO III. RESULTADOS Y DISCUSIÓN.....	33
3.1. Implementación del sistema de gestión de eventos e información de seguridad -SIEM	33
3.2. Detección de ataques en la aplicación web sisgedo	35
3.2.1. Análisis de vulnerabilidades de la aplicación web sisgedo v.2.0	36
3.2.2. Ejecución y detección de ataques	44
3.3. Mitigación de vulnerabilidades	60
3.4. Seguimiento y control con la herramienta SIEM	65
CAPÍTULO IV. CONCLUSIONES	66
CAPÍTULO V. RECOMENDACIONES	67
REFERENCIAS.....	68
ANEXOS	74
ANEXO 01: GUÍA DE IMPLEMENTACIÓN DEL ENTORNO VIRTUAL	74
ANEXO 02: OFICIO DE AUTORIZACIÓN PARA REALIZAR EL PROYECTO	104

ÍNDICE DE TABLAS

Tabla 1	Operacionalización de variables	27
Tabla 2	Escala para la valoración de los niveles de afectación.....	28
Tabla 3	Escala para la valoración de los niveles de riesgo	29
Tabla 4	Escala para la valoración de los niveles de impacto	29
Tabla 5	Servicios web de la municipalidad provincial de Chiclayo.	30

ÍNDICE DE FIGURAS

Figura 1	Simulación de un ataque de DDoS	11
Figura 2	Fases del ethical hacking	17
Figura 3	Virtual Box	23
Figura 4	Kali Linux.....	24
Figura 5	CLI de Centos.....	24
Figura 6	Sistema Operativo Security Onion	26
Figura 7	Interfaz de Virtual Box	33
Figura 8	Características de la máquina virtual security onion	34
Figura 9	Diagrama del entorno Virtual	35
Figura 10	Prueba de conexión con la máquina objetivo	36
Figura 11	Iniciando zend server desde centos	37
Figura 12	Interfaz de administración de zen server	37
Figura 13	Interfaz del servicio web Sisgedo.....	38
Figura 14	Escaneo de puertos con nmap.....	39
Figura 15	Script para el escaneo de vulnerabilidades con nmap	40
Figura 16	Escaneo de vulnerabilidades I del puerto 80 con nmap.....	41
Figura 17	Escaneo de vulnerabilidades II del puerto 80 con nmap	41
Figura 18	Escaneo de vulnerabilidades III del puerto 80 con nmap.....	42
Figura 19	Escaneo de vulnerabilidades IV del puerto 80 con nmap.....	42
Figura 20	Escaneo de vulnerabilidades del puerto 5432 con nmap	43
Figura 21	Ejecución de ataque 01 con nmap	44
Figura 22	Interfaz de inicio de sesión de la herramienta sguil.....	45
Figura 23	Interfaz de selección de interfaces de red.....	46
Figura 24	Eventos registrados durante el ataque 01 con sguil I.....	47
Figura 25	Eventos registrados durante el ataque 01 con sguil II	47
Figura 26	Transcripción de paquetes de red capturado.....	48
Figura 27	Información de los hosts conectados I en la red con networkminer	49
Figura 27	Información de los hosts conectados I en la red con networkminer	49
Figura 29	Información de la sesión activa con networkminer	50
Figura 30	Detalle de los parámetros del tráfico de red con networkminer	50
Figura 31	Eventos registrados de manera agrupada con squert	51
Figura 32	Eventos correlacionados con squert	51
Figura 33	Eventos correlacionados con squert II.....	52
Figura 34	Interfaz de Resumen de la herramienta squert.....	52
Figura 35	Ejecución de ataque 02 con nmap	53
Figura 36	Eventos registrados durante el ataque 02 con sguil I.....	54
Figura 37	Eventos registrados durante el ataque 02 con sguil II	54
Figura 38	Transcripción de paquetes de red capturado.....	55
Figura 39	Información de los hosts conectados I en la red con networkminer	55
Figura 40	Información de los hosts conectados II en la red con networkminer	56
Figura 41	Información de las sesiones activas del tráfico de red con networkminer	56
Figura 42	Información de los parámetros del tráfico de red con networkminer	57
Figura 43	Eventos registrados de manera agrupada con squert	57

Figura 44	Eventos correlacionados con squert I	58
Figura 45	Eventos correlacionados con squert II	58
Figura 46	Interfaz de Resumen de la herramienta squert	59
Figura 47	Interfaz de Resumen de la herramienta squert II	59
Figura 48	Vista de geolocalización con Squert	60
Figura 49	Eventos registrados durante el escaneo de vulnerabilidades del puerto 80 con sgul II	60
Figura 50	Eventos registrados durante el escaneo de vulnerabilidades del puerto 80 con sgul II	61
Figura 51	Escaneo de vulnerabilidades después de la mitigación 01	61
Figura 52	Eventos registrados con sgul después de la mitigación.	62
Figura 53	Eventos registrados durante el escaneo de vulnerabilidades del puerto 80 con sgul II	62
Figura 54	Escaneo de vulnerabilidades después de la mitigación 02	63
Figura 55	Transcripción de los eventos registrados después de la mitigación 02	64
Figura 56	Topología de la Propuesta a implementar	65
Figura 57	Página Oficial del Software de Virtualización Virtual Box	74
Figura 58	Instaladores Virtual Box	75
Figura 59	Proceso de Instalación de Virtual Box	75
Figura 60	Interfaz principal de Virtual Box	76
Figura 61	Interfaz principal de Virtual Box	77
Figura 62	Interfaz del sistema de archivos local	78
Figura 63	Interfaz del sistema de archivos local	78
Figura 64	Interfaz de inicio de sesión	79
Figura 63	Interfaz de escritorio de Kali linux	79
Figura 66	Importación de Servicio virtualizado	80
Figura 67	Importación de Servicio virtualizado II	81
Figura 68	Interfaz de preferencias de servicio	81
Figura 69	Interfaz de inicialización de la máquina virtual security onion	82
Figura 70	Interfaz de inicio de sesión	83
Figura 71	Interfaz del escritorio del Security Onion	83
Figura 72	Importación de servicio virtualizado	84
Figura 73	Interfaz del servicio a importar	84
Figura 74	Interfaz de Preferencias de servicio	85
Figura 75	Interfaz de inicialización de Centos 7	86
Figura 76	Interfaz de Inicio de Sesión Centos 7	86
Figura 77	Información del servidor centos 7	87
Figura 78	Interfaz de configuración de las Máquinas virtuales	88
Figura 79	Interfaz de configuración de la máquina virtual Kali Linux	89
Figura 80	Interfaz de configuración de la máquina virtual centos 7	89
Figura 81	Interfaz gráfica de la máquina virtual Kali linux	90
Figura 82	Interfaz de configuración de red Kali linux	91
Figura 83	Interfaz de información de la interfaz de red	91
Figura 84	Script para editar archivo de configuración de red	92
Figura 85	Parámetros del archivo de configuración de red	92
Figura 86	Parámetros del archivo de configuración de red	93
Figura 87	Pruebas de conexión I	94

Figura 88	Pruebas de conexión II	95
Figura 89	Pruebas de conexión III	95
Figura 90	Script para extraer el framework zendserver	96
Figura 91	Ruta de la carpeta del Zend Server	96
Figura 92	Archivo ejecutable de Zend Server	96
Figura 93	Ruta del archivo de configuración de Zend Server	97
Figura 94	Edición del archivo de configuración de Zend Server	97
Figura 95	Framework Zend Server iniciado	98
Figura 96	Interfaz de administración de Zend Server.....	98
Figura 97	Instalación del SGBD PostgreSQL	99
Figura 98	Ruta del archivo de configuración del SGBD PostgreSQL.....	99
Figura 99	Edición del archivo de configuración del SGBD PostgreSQL	99
Figura 100	Reinicio del SGBD PostgreSQL	100
Figura 101	Configuración de regla en el firewall	100
Figura 102	Actualización de configuraciones del firewall	100
Figura 103	Estado del servicio PostgreSQL	101
Figura 104	Ruta del archivo de conexión de la aplicación web Sisgedo	102
Figura 105	Parámetros del archivo de conexión de la aplicación web Sisgedo.....	102
Figura 106	Configuración de regla en el firewall	102
Figura 107	Actualización de configuraciones del firewall	103
Figura 108	Aplicación web Sisgedo	103

RESUMEN

En la actualidad la información se ha convertido en el activo más importante para las empresas y para las personas, esto a medida que se intensifica el uso de las redes sociales, portales web, servicios de correo electrónico entre otros. Asimismo, el Internet de las Cosas permite la interconexión de cualquier dispositivo u objeto doméstico o rural que esté preparado electrónicamente para su interacción.

Tanto las empresas como las personas se han visto vulnerables al exponer inconscientemente su información, mucho más aun un buen número de empresas no cuentan con sistemas especializados en gestión y control de amenazas como un SIEM, y tampoco cuentan con personal especializado para realizar un análisis exhaustivo de vulnerabilidades para de esa manera mitigar los ataques de ciberseguridad generados.

La presente investigación es de tipo tecnológica experimental porque nos permitió demostrar de manera real la implementación de un sistema de gestión de eventos e información de seguridad SIEM para la Municipalidad Provincial de Chiclayo.

Palabras Claves: Ataque informático, Vulnerabilidad, Sistema de gestión de eventos e información de seguridad, Servicios Web.

ABSTRACT

Nowadays, information has become the most important asset for companies and individuals, as the use of social networks, web portals, email services, among others, intensifies. Likewise, the Internet of Things allows the interconnection of any device or domestic or rural object that is electronically prepared for interaction.

Both companies and individuals have been made vulnerable by unconsciously exposing their information, much more a good number of companies do not have specialized threat management and control systems such as a SIEM, nor do they have specialized personnel to perform a comprehensive analysis of vulnerabilities to mitigate cybersecurity attacks generated.

This research is of a technological-experimental type because it allowed us to demonstrate in a real way the implementation of a security information and event management system - SIEM for the Provincial Municipality of Chiclayo.

Keywords: Computer attack, Vulnerability, Security information and event management system, Web Services.

INTRODUCCIÓN

El continuo avance y dependencia de las tecnologías de la información y comunicaciones a nivel mundial han llevado a los actores responsables de las amenazas informáticas a diseñar formas más sofisticadas de acceder, inspeccionar y manipular los sistemas de infraestructura de TI, de manera que las organizaciones se han visto obligadas a disponer de las últimas tecnologías para hacer frente a estos ataques y sus posibles impactos, además de adoptar distintas estrategias de ciberseguridad para mitigarlos. Según la revista IT Digital Media Group (2022) refiere que los ataques cibernéticos son el quinto riesgo más importante a nivel mundial, colocando a la ciberseguridad en la lista de prioridades de las organizaciones. Así mismo se muestran los principales ciberataques clasificados por la compañía de software especializada en ciberseguridad ESET de acuerdo a su nivel de impacto y sofisticación son: ciberataques contra ucrania, conti en Costa Rica, ransomware dirigidos a EE. UU, ataques de Lapsus a grandes empresas, ataque a la cruz roja internacional, etc.

En España son cada vez más frecuentes los ataques informáticos dirigidos particularmente a la administración pública, según el diario El Español (2023) los factores que han contribuido de que ocurran estos ataques informáticos se debe a las conectividades de alta velocidad, al internet de las cosas, el uso de las redes sociales y el teletrabajo. En consecuencia, todos estos factores han expuesto diferentes vulnerabilidades afectando tanto a las entidades públicas como a los ciudadanos, y aumentando en un 45.5% los ataques en el año 2022. De esta forma han obligado a las empresas a adquirir tecnologías y soluciones en ciberseguridad para protegerse ante estos ataques.

Latinoamérica no se encuentra preparada ante la ocurrencia de distintos ataques informáticos debido a que el gobierno no establece políticas de ciberseguridad. Como señala el Diario El Comercio (2022), Latinoamérica sufrió un promedio de 137 mil millones de intentos de ataques informáticos en el 2022, que representan un aumento del 50 % en comparación al año 2021. El Perú tuvo un promedio de 5,2 mil millones de tentativas de ataques informáticos en el 2022, que representa un incremento del 10%, distinto al periodo del año 2021.

La municipalidad provincial de Chiclayo es una institución pública que forma parte del estado y contribuye a la realización de sus fines, está ubicada en la calle Elías Aguirre 240, Chiclayo, tiene como misión promover la adecuada prestación de los servicios públicos y garantizar el desarrollo integral de la población de la provincia de Chiclayo. Actualmente la municipalidad provincial de Chiclayo cuenta con un centro de datos con servidores especializados que almacenan toda la información de los servicios web que ofrece. Estos servicios web son de suma importancia para la institución debido a que permiten atender de manera eficiente y eficaz a los administrados y brindar una información exacta y oportuna a los funcionarios para una mejor toma de decisiones, puesto que es importante resguardar la información ante posibles ataques informáticos.

Por otra parte, la municipalidad provincial de Chiclayo no cuenta con un sistema de gestión de eventos e información de seguridad SIEM, actuando de manera tardía ante posibles ataques que puedan recibir los sistemas informáticos y así producirse pérdidas de información. Por otra parte, se vienen suscitando constantes caídas de los servicios web ocasionando pérdidas económicas para la municipalidad. Aparte de ello no cuenta con personal especializado en seguridad informática o afines, carece de políticas y planes de respuesta ante incidentes de seguridad de la información, convirtiéndose en un blanco fácil para los atacantes informáticos.

Este proyecto de investigación se justifica porque su desarrollo busca beneficiar a la municipalidad alertando sobre los posibles ataques informáticos que ocurran en la red, garantizando la disponibilidad de la información, y ofreciendo un marco de trabajo para la respuesta ante incidentes de seguridad de la información en toda la institución.

En cuanto a la formulación del problema de la presente investigación se plantea la siguiente interrogante: ¿De qué manera se podrá realizar la detección de ataques y mitigación de vulnerabilidades de los servicios web de la municipalidad provincial de Chiclayo?

El presente estudio tiene como objetivo principal detectar los ataques y mitigar las vulnerabilidades de los servicios web de la municipalidad provincial de Chiclayo, así mismo se propone como objetivos específicos los siguientes: (1). Implementar un sistema de gestión de eventos e información de seguridad – SIEM para la municipalidad provincial de Chiclayo, (2). Realizar la detección de ataques en los servicios web de la municipalidad provincial de Chiclayo. (3). Mitigar las vulnerabilidades comunes de los servicios web de la municipalidad provincial de Chiclayo. (4). Realizar el seguimiento y control por medio del SIEM.

Finalmente se plantea la siguiente hipótesis: Con la implementación de un sistema de gestión de eventos e información de seguridad – SIEM se logrará detectar ataques para ejecutar la mitigación de vulnerabilidades de los servicios web en la municipalidad provincial de Chiclayo.

CAPÍTULO I. DISEÑO TEÓRICO

1.1. Antecedentes

1.1.1. Antecedentes Internacionales

Rodríguez & Mena (2019) en su investigación tuvo como objetivo proponer la detección y mitigación de ataques de DDos en las redes institucionales DGI para proteger las redes internas de la Institución, para ello se propuso implementar el Firewall Sophos XG 210 UTM como mecanismo de seguridad en la red, obteniendo como resultados el buen control y uso eficaz del tráfico en la red interna y externa, evitando amenazas, virus, bloqueando páginas maliciosas, bloqueos de malware. Llegando a concluir que con la implementación de la propuesta se logró detectar y mitigar cualquier ataque DDoS que provenga de cualquier lugar protegiendo los activos informáticos, además de brindar seguridad entre los servicios online y comunicaciones entre las sucursales que brinda la DGI hacia sus colaboradores.

Rosero (2020) en su indagación el objetivo fue diseñar e implementar un modelo de precisión con el fin de detectar y mitigar ataques phishing en cualquier correo electrónico, haciendo uso de técnicas de minería de datos. Para ello se utilizó una de las metodologías como es CRISP-DM. Este modelo mencionado generó la detección que reconoce a un correo como phishing, obteniendo como resultado la funcionalidad del modelo, a un 97% de precisión en la detección de correos infectados con phishing. Llegando a la conclusión que la aplicación de la metodología CRISP-DM, fue de gran importancia ya que facilitó el diseño e implementación del modelo mencionado, permitiendo cumplir con el correcto proceso de minería de datos, además de enfocar claramente los objetivos del modelo y negocio.

Benavides et al. (2020) en su artículo científico tuvieron como objetivo proporcionar a los usuarios finales e investigadores, una visión distinta a los usuales tipos de ataques de Phishing en la ingeniería social y la solución para mitigarlos. Para ello se realizó una investigación minuciosa sobre las variables de estudio, para poder identificar y clasificar los distintos tipos de ataques de ingeniería social, posteriormente encontrar los medios para que los ataques pueden ser mitigados. Además de instruir y dar a entender los conceptos básicos de este tipo de ciberataque al usuario sobre la utilización de técnicas como Machine Learning y Deep Learning. Para ello se aplicó cuatro soluciones basadas en algoritmos de Deep Learning como son: Recurrent Neural Network (RNN), Deep Boltzmann Machine (DBN), Deep Neural Network (DNN) y Convolutional Neural Network (CNN). Concluyendo que los medios más efectivos para la mitigación de ataques para Zero Day en phishing, son mediante los algoritmos Machine Learning y mediante Deep Learning, además de cumplir con la concientización al usuario con los enfoques antiphishing establecidos.

1.1.2. Antecedentes Nacionales

Espinoza (2022) en su investigación propuso desarrollar e implementar un firewall que se basa en el sistema operativo de software libre pfSense, el cual logre mitigar en las revisiones técnicas las vulnerabilidades informáticas de las empresas en la ciudad de Tacna, luego de implementar el firewall en la arquitectura de la red y realizar simulaciones de ataques cibernéticos como phishing y man-in-the-middle, los resultados fueron exitosos para la mitigación de estos ataques, logrando enviar alertas (logs) al administrador cada vez que se presentaba algún ataque. Llegando a la conclusión que utilizando el Firewall de Software libre con Pfsense se logró mitigar las vulnerabilidades

a las que la empresa estuvo expuesta, además de una rápida respuesta y alerta de mitigación frente las amenazas detectadas internas o externas de la empresa.

Estela (2020) en su investigación tuvo como objetivo Implementar una solución Security Information and Event Management (SIEM) para detectar vulnerabilidades y amenazas expuestas en las plataformas informáticas y redes de una entidad financiera, para ello se utilizó metodologías y una combinación de buenas prácticas como son: Scrum, PMBOK y la guía de IBMSe clasifica en cinco fases que son: inicio, planificación, configuración e implementación, seguimiento y control y cierre. Llegando así a la conclusión de que usando el SIEM junto con controles de endpoints, redes y checkers, se logró mitigar los riesgos de amenazas de forma más rápida y eficiente evitando daños económicos y de información, además se logró priorizar las alertas de seguridad, haciendo que las investigaciones del SOC se enfoquen en los incidentes sospechosos de alta probabilidad de la entidad financiera.

1.1.3. Antecedentes Regionales

Clavo (2022) en su indagación el objetivo fue analizar y realizar comparaciones de técnicas de mitigación de ataques de DDoS en Cloud Computing (servicios en la nube). Siendo la muestra de estudio nueve técnicas de mitigación tres de ellas fueron las más efectivas. Teniendo como resultados que las técnicas de mitigación más eficientes después de ser comparadas son Hybrid Cloud Bases Firewalling, Mitigating DDoS Attacks y Enhanced EDoS-Shield, ya que poseen características compatibles y aceptables para utilizarlas en los servicios en la nube o cloud computing. Concluyendo que las técnicas de mitigación mencionadas hacen más eficaces los recursos del entorno de trabajo.

Rodríguez (2018) el objetivo de su investigación fue implementar un prototipo que logre detectar y mitigar ataques de Denegación de Servicios DoS de los servicios web para conservar la operabilidad de los servicios proporcionados por el servidor, que sean económicos y seguros. Dando como resultado detectar un ataque Denegación de Servicios para a posterior mitigarlo, conservando la operabilidad del servicio para los usuarios. Concluyendo que la propuesta influye positivamente en la detección y mitigación de un ataque de Denegación de Servicios DoS logrando obtener indicadores positivos bastante altos con respecto a la operabilidad del servicio web.

1.2. Bases teóricas

1.2.1. Ataque Informático

Cuando se habla de un ataque informático se refiere a un intento de comprometer la seguridad informática de un sistema, con el fin de causar un daño intencional que afecte su funcionamiento. De acuerdo con Optical Networks (2021) describe que los “Ataques informáticos son un intento organizado e intencionado que busca explorar alguna vulnerabilidad o debilidad en las redes o sistemas informáticos tanto en software o hardware, con el objetivo de obtener algún beneficio económico”.

Según Ariganello (2020) refiere que existen diferentes tipos de ataques de red que son clasificados de la siguiente manera para poder mitigarlos.

1.2.1.1 Ataques de Reconocimiento

En este tipo de ataques es en donde se realiza el hallazgo y mapeo no autorizado de servicios, sistemas o vulnerabilidades. Estos ataques son precursores con la intención de ganar acceso no autorizado a una red o interrumpir el funcionamiento de la misma.

- **Sniffers de paquetes**

En este tipo de ataques se hace uso de herramientas de captura de paquetes para analizar el tráfico de la red, la tarjeta de red del dispositivo del atacante se configura en modo promiscuo, lo que le permite procesar los paquetes que transitan en una red, una vez capturados los paquetes se puede leer la información que contienen para un mejor entendimiento del sistema.

- **Barridos de ping**

Este tipo de ataques permite conocer qué hosts están disponibles en una red. Se lleva a cabo haciendo ping (utilidad del protocolo IP que permite verificar la disponibilidad de un host) a una serie de direcciones IP, aquellas que contesten el ping están activas en la red.

- **Escaneo de puertos**

Generalmente este tipo de ataques se realiza después de un barrido de ping. Una vez conocidos los hosts disponibles en una red, un escaneo de puertos proporciona información con respecto a los servicios disponibles (puertos abiertos) en ese host.

- **Búsquedas de información en internet**

Este tipo de ataques pueden revelar información sobre quién posee un dominio en particular y qué direcciones han sido asignadas a ese dominio.

1.2.1.2 Ataques de acceso

Los ataques de acceso utilizan las debilidades conocidas de los servicios de protocolo de transferencia de archivos, de autenticación y servicios web para poder

acceder a la base de datos e información no autorizada. Los ataques de acceso pueden clasificarse en cuatro tipos.

- **Ataques de contraseña**

Este tipo de ataques se pueden desarrollar con programas de detección de paquetes obteniendo así cuentas y contraseñas de usuario que se difunden como texto no cifrado. Los daños a contraseñas pueden aludir a las tentativas de inicio de sesión en un recurso compartido, como un servidor o enrutador para reconocer una cuenta o contraseña de usuario. Estas tentativas se denominan ataques de fuerza bruta.

- **Explotación de la confianza**

Este tipo de ataque aprovecha los privilegios del sistema no autorizados, logrando comprometer el objetivo.

- **Redirección de puerto**

Se usa un sistema ya comprometido como punto de partida para ataques contra otros objetivos. Se instala una herramienta de intrusión en el sistema comprometido para el direccionamiento de sesiones.

- **Ataque Man in the Middle**

Que significa Hombre de ataque en el centro, este radica en que el atacante se encuentra en el centro de una comunicación entre dos partes legítimas los cuales pueden leer o cambiar los datos transferidos entre las ambas partes.

- **Desbordamiento de buffer**

El resultado de este ataque es que los datos válidos se sobrescriben o explotan para permitir la ejecución de código malicioso o malintencionado.

1.2.1.3 Ataques de Denegación de Servicio DoS

Este tipo de ciberataque consiste en sobrecargar o inundar una máquina objetivo con solicitudes hasta que el tráfico normal es incapaz de ser procesado, lo que provoca una denegación de servicio a los usuarios.

Los ataques de DoS más comunes son:

- **Ping de la muerte**

Se trata de una solicitud de eco en un paquete IP más grande que el tamaño de paquete máximo de 65535 bytes, mandar un ping de este tamaño puede colapsar el nodo objetivo. Una versión de este ataque bloquea el sistema mediante el envío de fragmentos ICMP que llenan el búfer de recopilación de paquetes al objetivo.

- **Ataque Smurf**

Este tipo de ataque consiste en enviar un gran número de peticiones protocolo de control de mensajes de Internet a direcciones de difusión amplia, con sentido de origen falsificado de la misma red que el atacado. Si el dispositivo de enrutamiento que remite el tráfico a esas direcciones de difusión amplia lo vuelve a remitir a los broadcasts de acceso múltiple, las máquinas responderían a cada paquete.

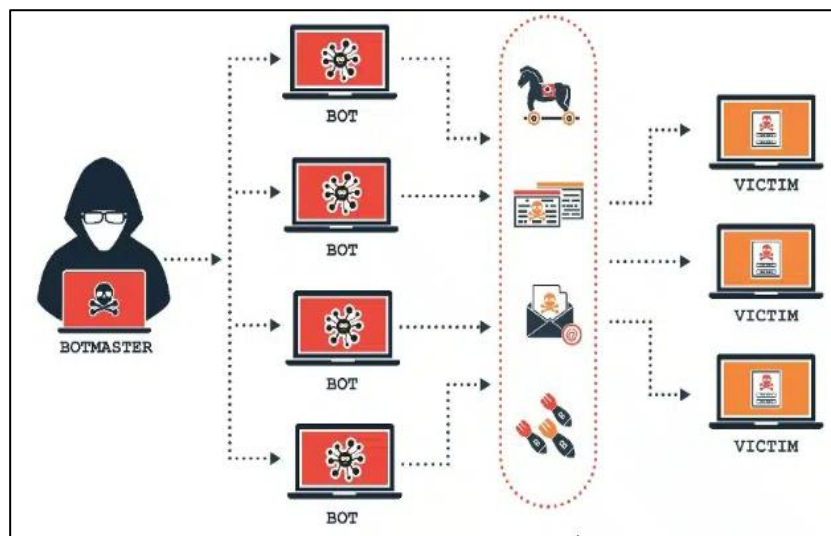
- **Inundación TCP/SYN**

Al enviar una gran cantidad de paquetes TCP SYN con una dirección de origen falsificada, cada paquete se trata como una solicitud de conexión, lo que

hace que el servidor genere una conexión semiabierta, devuelva un paquete TCP SYN-ACK y espere un paquete de respuesta con la dirección del remitente. Sin embargo, la respuesta nunca llega porque la dirección del remitente es falsa. Estas conexiones parcialmente abiertas exceden la cantidad de conexiones disponibles que el servidor puede manejar, por lo que no puede responder a las solicitudes legítimas hasta que finaliza el ataque.

Figura 1

Simulación de un ataque de DDoS



Fuente: (incibe, 2018)

1.2.2. Vulnerabilidad Informática

Según Romero et al. (2018), describe que “Una vulnerabilidad es un defecto en un sistema que puede ser explotada por un atacante generando riesgos muy altos tanto para la organización o el sistema”.

Según Santos (2022) refiere que “Una vulnerabilidad informática es cualquier fallo o error en el software o en hardware, permitiendo que los atacantes informáticos comprometan la integridad y confidencialidad de los datos que procesa un sistema”.

Según Roa (2018) describe que “Una vulnerabilidad es un defecto que puede ser aprovechada por un atacante, que al ser descubierta el atacante programará un malware que usa esa vulnerabilidad para tomar el control de la máquina o realizar acciones no autorizadas”.

Ambit (2020) refiere que los sistemas y aplicaciones informáticas siempre tienen algún fallo en su diseño, estructura o código que genera alguna vulnerabilidad, por muy pequeño que sea el error, siempre podrá generar una amenaza sobre los sistemas y la información, siendo la puerta de entrada para recibir ataques externos o internos.

Para Ambit (2020) las principales vulnerabilidades suelen producirse en:

- Errores de configuración.
- Errores en la gestión de recursos.
- Errores en los sistemas de validación.
- Errores que permiten el acceso a directorios.
- Errores en la gestión y asignación de permisos.

1.2.3. Servicio Web

Según la IBM (2022), refiere que “Los Servicios Web son aplicaciones independientes y modulares que se pueden describir, publicar, localizar e invocar a través de una red. Implementan una arquitectura orientada a servicios (SOA), que permite compartir recursos y datos de forma flexible y estandarizada”.

Según Lázaro (2018), describe que un Web Service, es un “Modo de comunicación entre dos máquinas o dispositivos conectados a través de una red que se encargan de intercambiar datos entre sistemas o aplicaciones y transmitir respuestas y solicitudes entre servidores”.

Lázaro (2018) refiere que Los Web Services utilizan los siguientes componentes:

- **SOAP**

Que significa Simple Object Access Protocol, es un protocolo basado en XML usado para intercambiar datos e información ya sean para el envío de mensajes o servir de comunicador en internet entre los diferentes sistemas.

- **WSDL:**

Que significa Web Services Description Language, es un lenguaje basado en XML, diseñado por Microsoft e IBM, el cual sirve para detallar, permitir acceso y establecer comunicación entre los servicios web.

- **UDDI:**

Que significa Universal Description, Discovery and Integration, es un estándar basado en XML utilizado para detallar, publicar y encontrar servicios web, verificando cuál de ellos se encuentran disponibles.

1.2.4. Servicios Web Municipales

La municipalidad provincial de Chiclayo actualmente cuenta con los siguientes servicios web municipales:

- **Portal web municipal**

Este servicio ofrece a la ciudadanía el acceso a una serie de recursos que se encuentran integrados con la finalidad de satisfacer necesidades de información sobre temas específicos.

Link del servicio: <https://www.munichiclayo.gob.pe/Portal/>

- **Correo electrónico zimbra**

Este servicio de correo institucional permite recibir y enviar mensajes de manera rápida, participar de videoconferencias y realizar un trabajo colaborativo más eficiente dentro de dicha municipalidad.

Link del servicio: <https://correo.munichiclavo.gob.pe/>

- **Sisgedo**

Este servicio permite administrar de mejor manera la recepción y envío de documentos dentro de dicha municipalidad y al mismo tiempo dar seguimiento a través del número de expediente hasta culminar cada proceso.

Link del servicio: <http://sisgedo.munichiclavo.gob.pe/sisgedonew/app/main.php>

- **Sistema de tarjeta de circulación**

Este servicio nos permite verificar en el sistema ingresando el N° de Placa vehicular si un vehículo cuenta con autorización para transporte público, el cual es expedido por la Sub Gerencia de Transporte de dicha municipalidad.

Link del servicio: <https://www.munichiclavo.gob.pe/Mobile/tuc.html>

- **Sistema de licencia de conducir**

Este servicio permite verificar en el sistema ingresando el N° del documento de Identidad (DNI) si el conductor cuenta con una licencia de conducir la cual es otorgada por la Sub Gerencia de Tránsito y Seguridad Vial de dicha municipalidad.

Link del servicio: <https://www.munichiclavo.gob.pe/Mobile/motos.html>

- **Sistema de registro civil**

Este servicio permite realizar consultas en el sistema sobre los hechos vitales que se registran en la Sub Gerencia de Registro civil.

Link del servicio <https://www.munichiclayo.gob.pe/buscardocs/consultaRC.php>

- **Sistema de licencias de edificación**

Este servicio permite verificar en el sistema ingresando el N° de la licencia de edificación si el predio cuenta con una licencia de edificación la cual es otorgada por la Gerencia de Desarrollo Urbano de dicha municipalidad.

Link del servicio: <https://www.munichiclayo.gob.pe/modLicEdi/Buscar>

1.2.5. Ethical Hacking

Según Astudillo (2018), señala que el ethical hacking es la acción de realizar pruebas de intrusión controladas sobre sistemas informáticos para descubrir vulnerabilidades en los equipos auditados que puedan ser explotadas, utilizando un ambiente supervisado en el que no se ponga en riesgo la operatividad de los servicios informáticos de la organización.

Teniendo en cuenta a Chávez (2021), describe las siguientes fases del ethical hacking:

- **Fase 1: Reconocimiento**

En esta fase se reúnen toda la información posible sobre lo que se tiene como objetivo. Esta fase se divide en information gathering o recolección de información, ingeniería social y doxing.

- **Fase 2: Escaneo y enumeración**

En esta fase se hace uso de la información recopilada y se escanea los puertos, dominios o direcciones IPs de las computadoras, con el fin de realizar un análisis o listar los subdirectorios.

- **Fase 3: Obtener acceso**

En esta fase se ejecuta el ataque, se accede al servidor o a una red inalámbrica analizada previamente que puede ser manual o automático con el fin de obtener acceso no autorizado y efectuar un payload.

- **Fase 4: Mantener acceso**

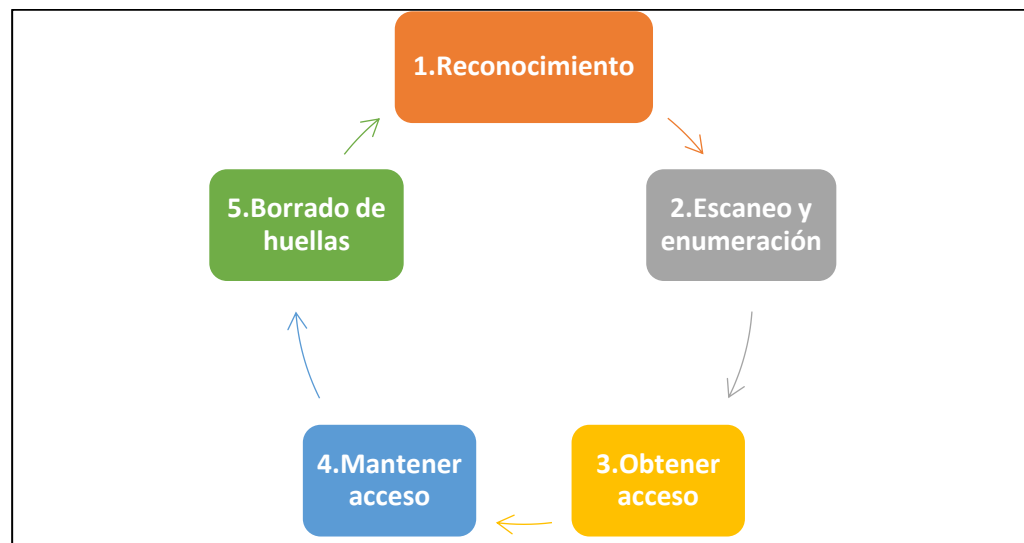
Esta fase se conoce como elevación de privilegios, consiste en que el atacante intenta mantener el acceso a los servicios o redes inalámbricas atacadas las cuales son utilizadas para poder eliminar información, registrar, escanear redes o ejecutar ataques mediante el uso de malwares.

- **Fase 5: borrado de huellas**

En esta fase final, los atacantes intentan no dejar rastros alguno de sus ataques, para ello utilizan técnicas como es eliminar, alterar u ocultar archivos a través de un anonimato usando VPN u otros.

Figura 2

Fases del ethical hacking



Fuente: Elaboración propia.

1.2.6. Pentesting

Según Olivares y Oncins (2018), señalan que el pentesting es un método de prueba de seguridad de los sistemas de información que consiste en simular el ataque de un usuario malintencionado o incluso malware, con la finalidad de encontrar vulnerabilidades explotables y proponer contramedidas destinadas a mejorar la seguridad de un sistema en particular.

Santos (2023), refiere el pentesting o prueba de penetración como un tipo de prueba que utilizan las empresas para realizar un análisis de vulnerabilidades y debilidades en su seguridad informática, que consiste en atacar diferentes entornos o sistemas para detectar y prevenir posibles fallos o ataques.

1.2.7. SIEM

Rouse (2017), refiere que “El sistema SIEM es un enfoque de gestión de la seguridad diseñado para facilitar una visión global de la seguridad de la tecnología de la información de una organización”.

Según Ortega (2021), señala que el sistema de gestión de eventos e información de la seguridad – SIEM es la principal herramienta de un Centro de Operaciones de Seguridad (SOC) ya que permite gestionar los eventos de un sistema de información que puedan afectar a las organizaciones.

Tal como describe Postigo (2020), los sistemas de gestión de eventos e información de seguridad (SIEM) centralizan las operaciones de supervisión de dispositivos perimetrales como switches, routers, cortafuegos, sistemas de detección de intrusos IDS, gestión de servidores de bases de datos, servidores web y cualquier otro tipo de servicios.

1.2.7.1 Capacidades de un SIEM

Tal como describe Ramos (2021), un sistema SIEM es una herramienta clave utilizada por un centro de operaciones SOC para detectar y responder a incidentes, e implementarlo proporcionaría una serie de capacidades entre ellas tenemos:

- **Agregación de datos**

Método o proceso en el que se recopila o administra información obtenida de distintas fuentes.

- **Correlación**

Técnica que consiste en procesar los datos ingresados para transformarlos en información.

- **Alerta:**

Capacidad de realizar un análisis de los eventos que van a ocurrir en el sistema de tal manera que te informan a través de avisos o notificaciones de seguridad.

- **Cuadros de mando:**

El sistema de Gestión de Eventos e Información de Seguridad (SIEM) posee las herramientas de gestión necesarias para poder transformar la información ingresada en indicadores numéricos y gráficos.

- **Cumplimiento:**

Con el sistema de Gestión de Eventos e Información de Seguridad (SIEM) se logra la automatización de la información o datos recopilados las cuales son de importancia para elaborar informes de normativas.

- **Retención:**

Capacidad de gran importancia que posee el sistema de Gestión de Eventos e Información de Seguridad (SIEM) la cual que permite almacenar información a largo plazo.

- **Redundancia:**

Gracias a la duplicación que realiza el sistema de Gestión de Eventos e Información de Seguridad (SIEM) en su base de datos, se puede evitar la pérdida de cualquier información o datos.

- **Escalabilidad:**

Capacidad que posee el sistema de Gestión de Eventos e Información de Seguridad (SIEM) para adaptarse en función al aumento o disminución de las necesidades del sistema.

1.2.7.2 Ventajas de un SIEM

Según Ramos (2021) refiere las siguientes ventajas que aporta un SIEM a nivel de seguridad:

- **Detección Temprana de incidente**

Al realizarse un análisis en tiempo real permite que el SIEM pueda detectar cualquier incidente que se presente y poder realizar acciones necesarias para solucionar o eliminar dichos incidentes evitando daños posteriores.

- **Análisis Forense**

Gracias a la gran capacidad de almacenamiento y búsqueda de eventos de seguridad antiguos que posee el SIEM, es que hace más fácil poder realizar un análisis forense para identificar si algún incidente se ha producido.

- **Centralización de la Información**

El SIEM permite la recopilación oportuna de eventos de dispositivos ya sean de red o seguridad, logrando así la centralización de la información recopilada anteriormente.

- **Ahorro de Recursos**

Al realizarse la recolección de datos e información de manera automatizada se logra significativamente un ahorro de recursos.

- **Identificación de Anomalías**

El SIEM facilita la identificación de anomalías en el funcionamiento de los equipos tras un periodo de aprendizaje, permitiendo descubrir problemas o incluso incidencias en funcionamiento.

1.2.8. Ciberseguridad

Es un conjunto de técnicas, sistemas de gestión y otras medidas que se encargan de la protección de los activos digitales, incluyendo redes, hardware y software, así como la información que es procesada, almacenada y transportada a través de los sistemas de información interconectados (Ortega, 2021).

Kaspersky (2023) señala que “La Ciberseguridad es la práctica de proteger las computadoras, los servidores, dispositivos electrónicos, dispositivos móviles, las redes y los datos de ataques maliciosos”.

La ciberseguridad puede dividirse en las siguientes categorías:

- La Seguridad de red.
- La seguridad de las aplicaciones.
- La seguridad de la información.
- La recuperación ante desastres y la continuidad del negocio.
- La capacitación del usuario final.

Según Cisco (2023), refiere cuatro tipos de amenazas a la ciberseguridad entre los que se encuentran:

- **Suplantación de identidad (phishing)**

Es la práctica de enviar correos electrónicos fraudulentos que parecen correos electrónicos de fuentes confiables, con el objetivo de robar información

sensible como números de tarjetas de crédito, contraseñas de inicio de sesión, entre otros.

- **Ransomware**

Es un tipo de software malicioso diseñado para extorsionar bloqueando el acceso a los sistemas informáticos y archivos hasta que se pague un rescate.

- **Malware**

Es un Software diseñado para obtener acceso no autorizado, realizando funciones perjudiciales para el usuario y los sistemas informáticos.

- **Ingeniería Social**

Es un conjunto de técnicas que utilizan los cibercriminales para engañar a los usuarios con el fin de que revelen datos confidenciales, La ingeniería social se puede combinar con cualquiera de las amenazas mencionadas anteriormente para aumentar la posibilidad de descargar malware o confiar en fuentes maliciosas.

1.2.9. Software de virtualización Virtual Box

Oracle VM VirtualBox, es un potente software de virtualización multiplataforma de código abierto más popular del mundo, permite a los desarrolladores entregar código más rápido al ejecutar múltiples sistemas operativos en un solo dispositivo. Virtual box se está desarrollando activamente, incluyendo la integración de Infraestructura cloud (OCI), soporte 3D mejorado, un generador de máquinas virtuales (VM) automatizado y cifrado completo de VM. Las nuevas funciones ayudarán a las organizaciones a simplificar la administración de sus máquinas virtuales y ayudarán a acelerar la implementación de aplicaciones en la nube y en las instalaciones. (Oracle VM VirtualBox, 2022)

Figura 3

Virtual Box



Fuente: (Metric Software Developers, 2018)

1.2.10. Sistema Operativo Kali Linux

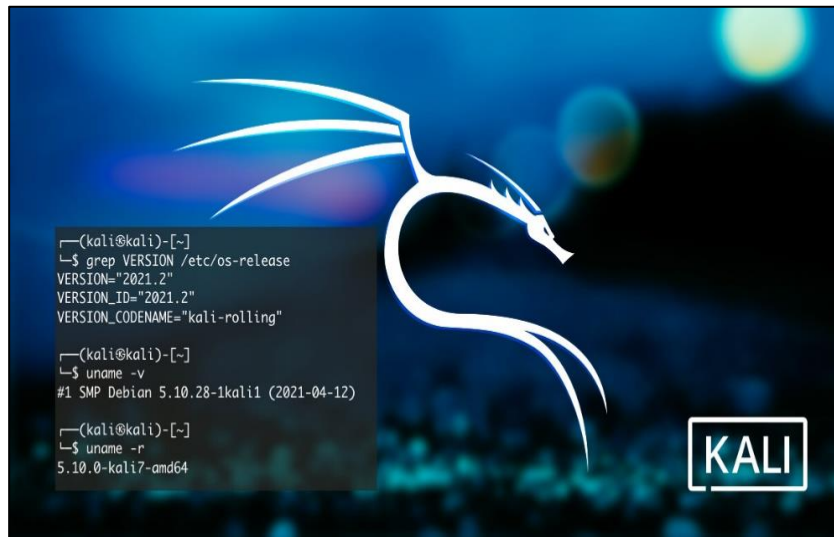
Kali Linux es una distribución de Linux de código abierto basada en Debian y diseñada para una variedad de tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, análisis forense informático e ingeniería inversa. Además de ser considerada una solución multiplataforma y de libre acceso para profesionales y aficionados a la seguridad de la información. (Kali, 2023)

Principales características de Kali Linux teniendo en cuenta a Kali (2023) son:

- Kali Linux incluye más de 600 herramientas de pruebas de penetración.
- Al ser código abierto está disponible para personas que deseen realizar alguna modificación de acuerdo a sus necesidades específicas.
- Compatibilidad con varios dispositivos inalámbricos.
- Personalizable a gusto de cada usuario.
- Herramientas y sistema operativo actualizados con las últimas versiones.

Figura 4

Kali Linux



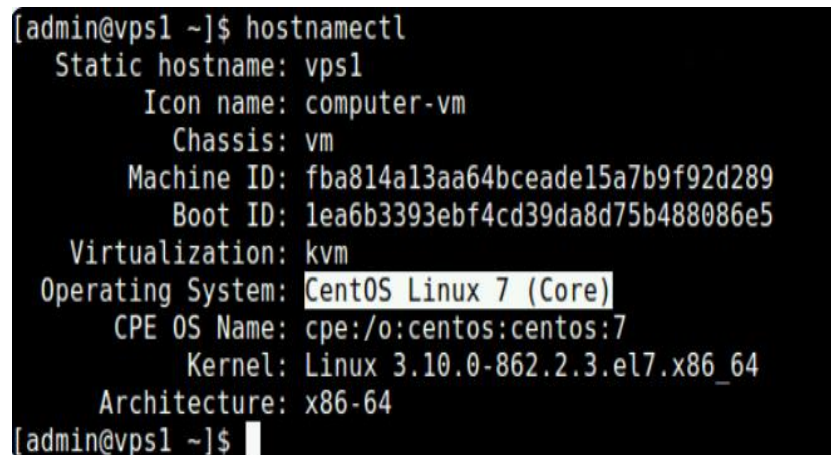
Fuente: (Kali, 2021).

1.2.11. Sistema Operativo Centos

Centos es un sistema operativo de código abierto, basado en la distribución Red Hat Enterprise Linux, funcionando de manera similar con RHEL y cuyo objetivo es ofrecer al usuario una plataforma consistente y manejable que se adapta a una amplia variedad de implementaciones.

Figura 5

CLI de Centos



Fuente: (tecmint, 2019).

1.2.12. Sistema Operativo Security Onion

Según Burks (2023) menciona que security onion es una distribución de Linux basada en Ubuntu, diseñada para la seguridad informática, permitiendo la detección de intrusiones, monitorización de la red y la gestión de eventos. Incorpora una serie de herramientas para auditar la seguridad a nivel de redes, sin tener que instalar apps adicionales.

Teniendo en cuenta a Fer (2019) señala algunas herramientas principales de security onion, entre ellas tenemos:

Para la detección de intrusos

- Snort
- Suricata

Para la gestión de eventos

- Squil
- Squert

Para las capturas de paquetes o PCAP

- Wireshark
- NetworkMiner

Análisis Forense

- Bro
- Xplico

Todas estas herramientas se encuentran integradas y configuradas para realizar sus funciones de manera automática.

Figura 6

Sistema Operativo Security Onion



Fuente: (SorceForget, 2016).

1.3. Bases conceptuales

1.3.1. Operacionalización de Variables

Tabla 1

Operacionalización de variables

	Variable	Definición	Dimensión	Indicadores	Técnica de Recolección de Información	Instrumento de recolección de información	Instrumento de medición
Variable Independiente	Software Siem	Herramienta principal de un centro de operaciones de seguridad SOC que permite gestionar los eventos de un sistema de información.	Administración de eventos	Registros de eventos	Observación	Ficha de observación	Software de análisis de eventos
			Sistema de detección de Intrusiones	Alertas de intrusos	Interfaz del software siem	Reporte del software siem	
			Análisis de paquetes	Paquetes analizados			
Variable Dependiente	Detección de ataques y mitigación de vulnerabilidades de los servicios web	Acción que permite detectar un fallo perjudicial en el sistema para reducir el impacto del ataque.	Detección de Ataques	Cantidad de Ataques detectados Frecuencia de Ataques	Análisis de documentos	Guía de Análisis de documentos	VM Kali Linux
			Mitigación de Vulnerabilidades	Cantidad de Vulnerabilidades			
				Nivel de Riesgo	Análisis de documentos	Guía de Análisis de documentos	
				Nivel de Impacto			

Fuente: Elaboración Propia.

CAPÍTULO II. MÉTODOS Y MATERIALES

2.1. Tipo de Investigación

La presente investigación según su objetivo y la manipulación de las variables es de tipo aplicada tecnológica - experimental, porque nos permitió demostrar de manera real la implementación de un sistema de gestión de eventos e información de seguridad – SIEM.

2.2. Diseño de contrastación de hipótesis

Para poder determinar el nivel de afectación de cada uno de los ataques informáticos detectados en los servicios web de la municipalidad provincial de Chiclayo, se utilizará la siguiente escala tipo Likert:

Tabla 2

Escala para la valoración de los niveles de afectación

Afectación	Valor	Porcentaje
No Aplica	0	--
Muy Bajo	1	0-20
Bajo	2	21-40
Medio	3	41-60
Alto	4	61-80
Muy Alto	5	81-100

Fuente: Elaboración Propia.

Para determinar la cantidad, nivel de riesgo e impacto de las vulnerabilidades de cada uno de los servicios web de la Municipalidad Provincial de Chiclayo, se utilizará la siguiente escala tipo Likert:

Tabla 3

Escala para la valoración de los niveles de riesgo

Nivel de Riesgo	Valor	Porcentaje
No Aplica	0	--
Bajo	1	21-40
Medio	2	41-60
Alto	3	61-80

Fuente: Elaboración Propia.

Tabla 4

Escala para la valoración de los niveles de impacto

Nivel de Impacto	Valor	Porcentaje
No Aplica	0	--
Bajo	1	0-30
Medio	2	31-60
Alto	3	61-100

Fuente: Elaboración Propia

2.3. Población y muestra

La población utilizada en la presente investigación está conformada por los servicios web de la municipalidad provincial de Chiclayo, y como muestra de la investigación se tomará el servicio web sisgedo, siendo este uno de los servicios más relevantes en cuanto a la sistematización de procesos de las unidades orgánicas de la municipalidad.

Tabla 5

Servicios web de la municipalidad provincial de Chiclayo.

Servicio web N°	Descripción
1	Portal web municipal
2	Sisgedo municipal
3	Correo electrónico zimbra
4	Tarjeta circulación
5	Licencia de conducir
6	Sistema de registro civil
7	Sistema de licencias de edificación

Fuente: Elaboración Propia.

2.4. Técnicas, instrumentos, equipos y materiales

Técnicas e Instrumentos de recolección

En la presente investigación se empleó como técnicas de recolección de datos la observación y el análisis de documentos siendo esenciales para analizar el funcionamiento y la situación actual de los sistemas de seguridad informática que cuenta la municipalidad provincial de Chiclayo. Así mismo, se consideró como instrumentos de recolección de datos la guía de observación y la guía de análisis de documentos con el fin de recolectar información de distintas fuentes.

Equipos

Dentro de los equipos utilizados para el desarrollo del presente trabajo de investigación tenemos:

- **02 equipos portátiles (Laptop)**

- **Laptop 1**

- Sistema Operativo: Windows 11

- Memoria RAM: 8GB

- **Laptop 2**

- Sistema Operativo: Windows 10

- Memoria RAM: 8GB

- **Software de virtualización**

- Virtual Box 7.0.4

- **03 máquinas virtuales**

- **VM 1**

- Sistemas Operativo: Kali Linux

RAM virtual: 1.5 GB

VM 2

Sistemas Operativo: Security Onion

RAM virtual: 2GB

VM3

Sistemas Operativo: CentOS 7

RAM virtual: 1GB

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1. Implementación del sistema de gestión de eventos e información de seguridad -SIEM

Como resultados de la implementación del sistema de gestión de eventos e información de seguridad – SIEM, se logró monitorear el tráfico de la red, detectar y alertarnos de posibles ataques en tiempo real y sobre todo tener una visión centralizada de la seguridad de la red, con el fin de garantizar la protección de los activos digitales de la institución.

Se realizó la implementación del sistema SIEM utilizando el software de virtualización virtual box v.7.0.4, el cual se utilizó para importar y ejecutar la máquina virtual security onion con las siguientes características: memoria base 2 GB y almacenamiento 20 GB. prueba de ello se anexa la importación de la máquina virtual de manera detallada.

Herramienta security onion

Figura 7

Interfaz de Virtual Box



Fuente: Elaboración propia.

Figura 8

Características de la máquina virtual security onion



Fuente: Elaboración propia.

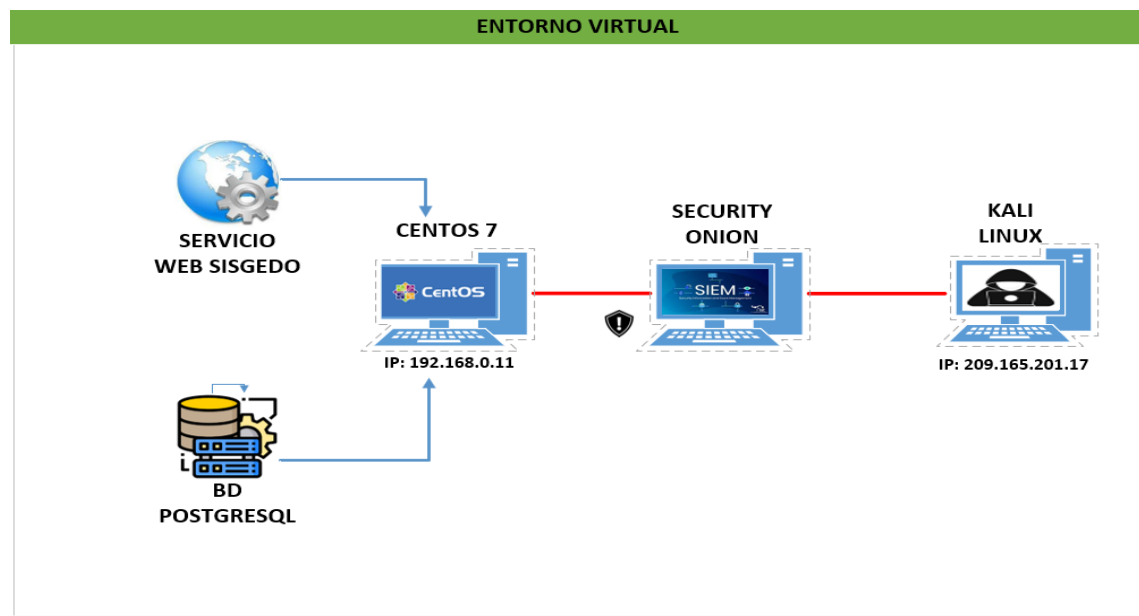
3.2. Detección de ataques en la aplicación web sisgedo

Como parte del desarrollo de esta investigación, se llevó a cabo la detección de ataques del servicio web sisgedo, implementando un entorno virtual con los siguientes sistemas operativos: Kali Linux, security onion y centos, en este último se desplegó una réplica exacta de la aplicación web sisgedo v.2.0 de la municipalidad provincial de Chiclayo, con el fin de detectar los ataques ejecutados.

En primer lugar, se realizó un análisis de vulnerabilidades para posteriormente ejecutar los ataques y al mismo tiempo detectarlos con la herramienta security onion (SIEM).

Figura 9

Diagrama del entorno Virtual



Fuente: Elaboración propia.

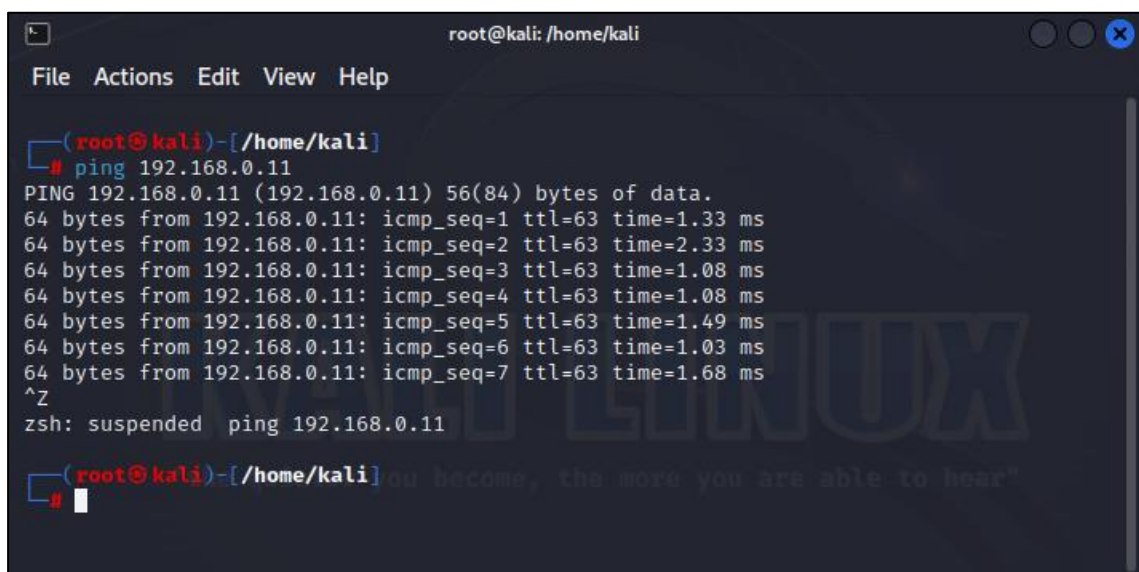
3.2.1. Análisis de vulnerabilidades de la aplicación web sisgedo v.2.0

Para el respectivo análisis de vulnerabilidades de la aplicación web sisgedo v.2.0 se realizaron las siguientes acciones:

- En esta primera parte, mediante el comando **ping** realizamos pruebas de conexión entre la máquina virtual con el rol de atacante (Kali Linux) y la máquina virtual con el rol de objetivo (centos).

Figura 10

Prueba de conexión con la máquina objetivo



```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# ping 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=63 time=1.33 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=63 time=2.33 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=63 time=1.08 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=63 time=1.08 ms
64 bytes from 192.168.0.11: icmp_seq=5 ttl=63 time=1.49 ms
64 bytes from 192.168.0.11: icmp_seq=6 ttl=63 time=1.03 ms
64 bytes from 192.168.0.11: icmp_seq=7 ttl=63 time=1.68 ms
^Z
zsh: suspended ping 192.168.0.11
(root@kali)-[/home/kali]
#
```

Fuente: Elaboración propia.

En este caso podemos observar que se han enviado 7 paquetes de 64 bytes con un total de 63 saltos hacia la máquina objetivo y se recibió la misma cantidad en un tiempo de 2 ms, lo que quiere decir que no hubo pérdida de paquetes y que la conexión con la máquina objetivo es exitosa.

- Desde la terminal de la máquina virtual objetivo (centos) iniciamos el servidor Zend. Para administrar los distintos procesos de zend server, ejecutamos el siguiente script.

```
cd /usr/local/zend/bin/zendctl.sh start
```

Figura 11

Iniciando zend server desde centos

```
[root@Srv-Apli ~]# cd /usr/local/zend/bin
[root@Srv-Apli bin]# ./zendctl.sh start
Starting Zend Server 5.1.0 ..

/usr/local/zend/bin/apachectl start [OK]
spawn-fcgi: child spawned successfully: PID: 1177
Starting Zend Server GUI [Lighttpd] [OK]
[ 08.06.2023 08:05:28 SYSTEM] watchdog for lighttpd is running.
[ 08.06.2023 08:05:28 SYSTEM] lighttpd is not running.

Zend Server started...
[root@Srv-Apli bin]# _
```

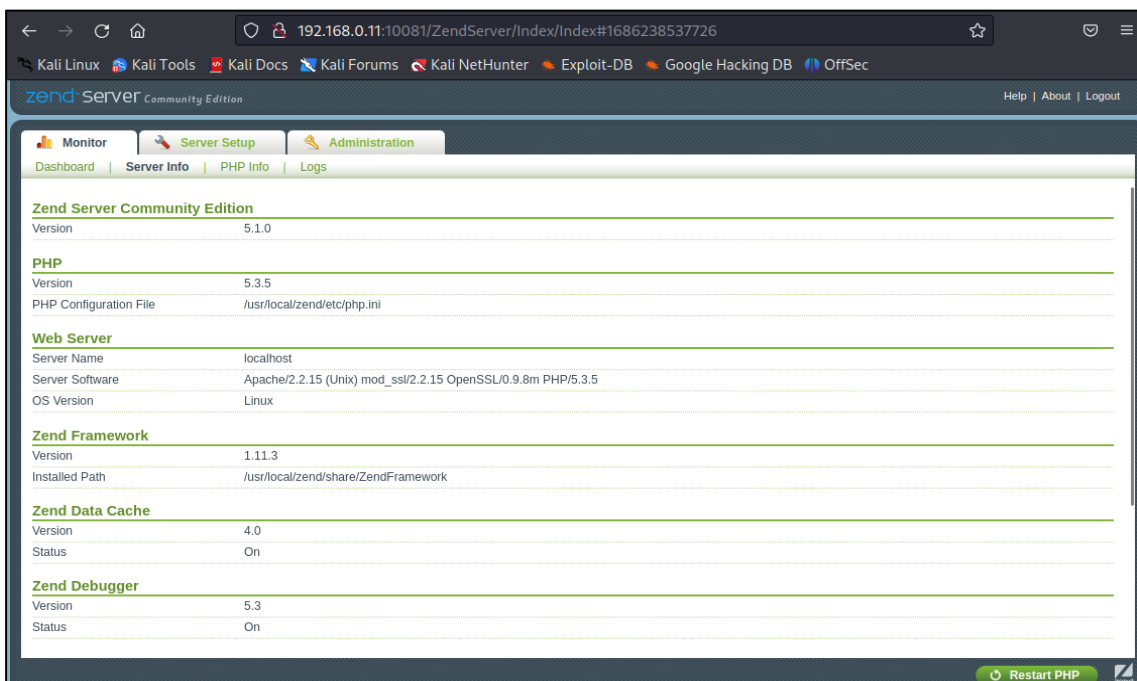
Fuente: Elaboración propia

- Una vez iniciado el servidor zend, accedemos a la interfaz de administración y al servicio web sisgedo municipal desde el navegador de la máquina kali linux (atacante) para comprobar que dicho servicio se esté ejecutando correctamente.

Enlace para acceder a la administración del servidor zend: **<http://192.168.0.11:10081>**

Figura 12

Interfaz de administración de zen server



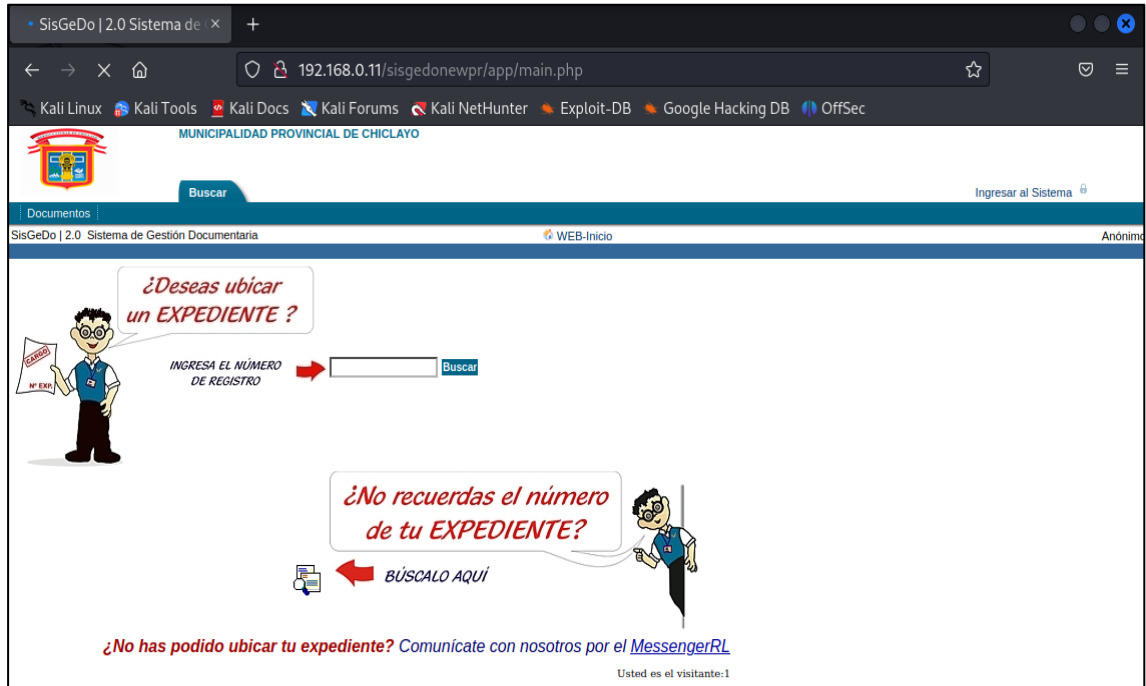
Fuente: Elaboración propia

Ingresamos al siguiente enlace para acceder al servicio web sisgedo municipal:

<http://192.168.0.11/sisgedonewpr/app/mai.php>

Figura 13

Interfaz del servicio web Sisgedo.



Fuente: Elaboración propia

Nmap

Nmap es una herramienta desarrollada en python con el objetivo de escanear distintas redes, puertos y servicios. Según Shivanandhan (2023), refiere que nmap es una herramienta de línea de comandos de linux de código abierto que se utiliza para escanear direcciones IP, encontrar qué dispositivos se están ejecutando en su red, descubrir puertos, servicios abiertos y detectar vulnerabilidades. Algunas características que incluye la herramienta nmap son:

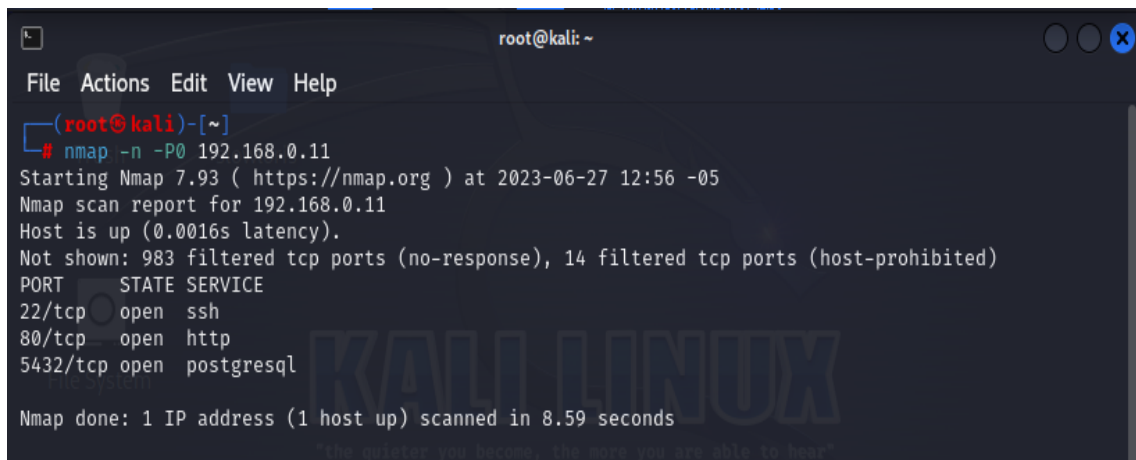
- Capacidad para reconocer cualquier dispositivo de red.
- Permite identificar qué servicios se están ejecutando en un sistema, incluidos servidores web y dns.

- Identificar el sistema operativo que se está ejecutando en los dispositivos.
- Permite utilizar distintos scripts para el escaneo de puertos y de vulnerabilidades durante la auditoría de seguridad.
- Con la herramienta nmap realizamos el escaneo de todos los puertos abiertos que se encuentran en nuestra máquina objetivo (centOS) con la **ip: 192.168.0.11**, Ejecutando el siguiente script desde la terminal de la máquina atacante (kali linux):

nmap -n -P0 192.168.0.11

Figura 14

Escaneo de puertos con nmap



```

root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# nmap -n -P0 192.168.0.11
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-27 12:56 -05
Nmap scan report for 192.168.0.11
Host is up (0.0016s latency).
Not shown: 983 filtered tcp ports (no-response), 14 filtered tcp ports (host-prohibited)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
5432/tcp  open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 8.59 seconds

```

Fuente: Elaboración propia

De los resultados obtenidos podemos observar cuatro puertos abiertos y el servicio que se ejecuta en cada puerto.

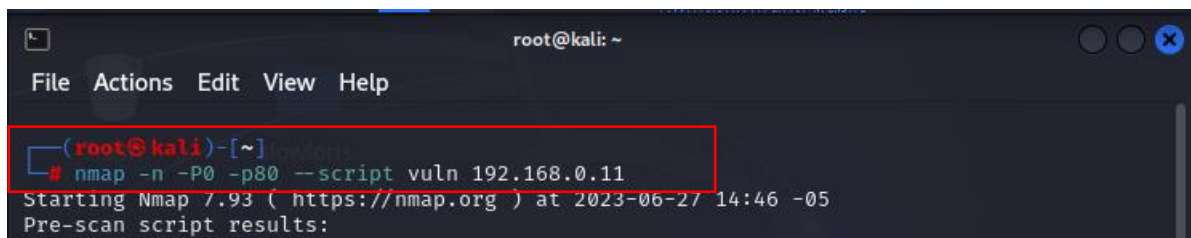
- P22/tcp: ejecuta el servicio (SSH), el protocolo secure shell (SSH) permite acceder a equipos de forma remota en la red y administrar el sistema a través de un intérprete de comandos.
- P80/tcp: ejecuta el servicio (HTTP),
- P5432/tcp: ejecuta el servicio (POSTGRESQL),

- A partir de los resultados obtenidos del escaneo de puertos, se realizó el escaneo de vulnerabilidades específicamente en los puertos 80 y 5432, ya que ejecutan los servicios que utiliza la aplicación web sisgedo v.2.0. Utilizamos el siguiente script de la herramienta nmap teniendo en cuenta los siguientes parámetros:
 - n: deshabilita resoluciones DNS inversas.
 - P0: evita enviar mensajes ICMP.
 - p: especifica el puerto a escanear.
 - script vuln: detecta vulnerabilidades conocidas.

Nmap -n -P0 -p80 --script vuln 192.168.0.11

Figura 15

Script para el escaneo de vulnerabilidades con nmap



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# nmap -n -P0 -p80 --script vuln 192.168.0.11  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-27 14:46 -05  
Pre-scan script results:
```

Fuente: Elaboración propia

- Del escaneo de vulnerabilidades en el puerto 80, se obtuvieron los siguientes resultados:

Vulnerabilidad 01

Slowloris DOS attack

Cve: CVE-2007-6750

Descripción: Permite a los atacantes remotos provocar un ataque de denegación de servicio, a través de solicitudes HTTP con la finalidad de sobrecargar el servidor web.

Figura 16

Escaneo de vulnerabilidades I del puerto 80 con nmap

```
PORT      STATE SERVICE
80/tcp    open  http
| http-slowloris-check: "the quieter you become, the more you are able to hear"
|   VULNERABLE:
|     Slowloris DOS attack
|       State: LIKELY VULNERABLE
|       IDs:   CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible. It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
```

Fuente: Elaboración propia

Vulnerabilidad 02:

SQL Injection

Descripción: Permite a los atacantes realizar consultas de base de datos con la finalidad de comprometer todo el sistema.

Figura 17

Escaneo de vulnerabilidades II del puerto 80 con nmap

```
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.0.11:80/sisgedonewpr/?C=S%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=M%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=N%3B0%3DD%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=D%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=M%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=N%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=S%3B0%3DD%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=D%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=S%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=N%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=M%3B0%3DD%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=D%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=S%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=M%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=N%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/?C=D%3B0%3DA%27%20OR%20sqlspider
|     http://192.168.0.11:80/sisgedonewpr/mislibs/?C=N%3B0%3DD%27%20OR%20sqlspider
```

Fuente: Elaboración propia

Vulnerabilidad 03:

http-enum:

Descripción: Muestra los directorios utilizados en las aplicaciones web, permitiendo la copia de estos mismos.

Figura 18

Escaneo de vulnerabilidades III del puerto 80 con nmap

```
|_ http-enum:
|   /: Root directory w/ directory listing
|   /icons/: Potentially interesting folder w/ directory listing
|_ http-trace: TRACE is enabled
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.

Nmap done: 1 IP address (1 host up) scanned in 344.64 seconds

(root@kali)~#
```

Fuente: Elaboración propia

Vulnerabilidad 04:

TRACE is enable

Descripción: Este método de petición al encontrarse habilitado, permite a los atacantes obtener información confidencial sobre los encabezados de autenticación internos que son agregados por proxies inversos.

Figura 19

Escaneo de vulnerabilidades IV del puerto 80 con nmap

```
|_ http-enum:
|   /: Root directory w/ directory listing
|   /icons/: Potentially interesting folder w/ directory listing
|_ http-trace: TRACE is enabled
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.

Nmap done: 1 IP address (1 host up) scanned in 344.64 seconds

(root@kali)~#
```

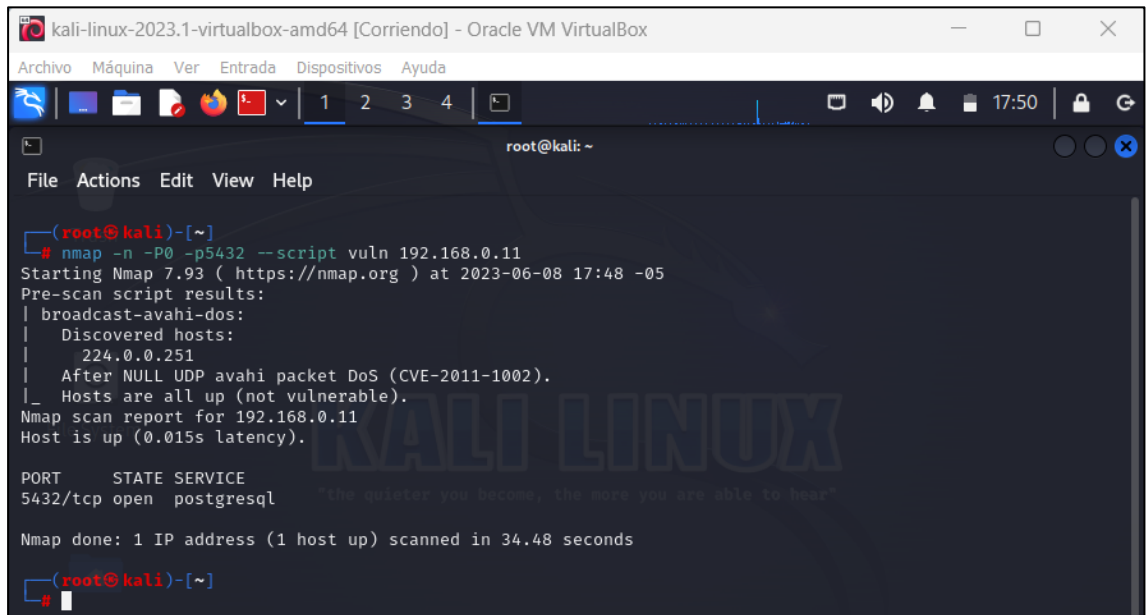
Fuente: Elaboración propia

- Se realizó el escaneo de vulnerabilidades en el puerto 5432 ejecutando el siguiente script:

```
nmap -n -P0 -p80 --script vuln 192.168.0.11
```

Figura 20

Escaneo de vulnerabilidades del puerto 5432 con nmap



```
kali-linux-2023.1-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
1 2 3 4
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# nmap -n -P0 -p5432 --script vuln 192.168.0.11
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-08 17:48 -05
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.11
Host is up (0.015s latency).

PORT      STATE SERVICE
5432/tcp  open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 34.48 seconds

(root@kali)-[~]
#
```

Fuente: Elaboración propia

De los resultados obtenido sobre el escaneo de vulnerabilidades hacia el el puerto 5432 se pudo observar que no se encontró vulnerabilidad alguna.

3.2.2. Ejecución y detección de ataques

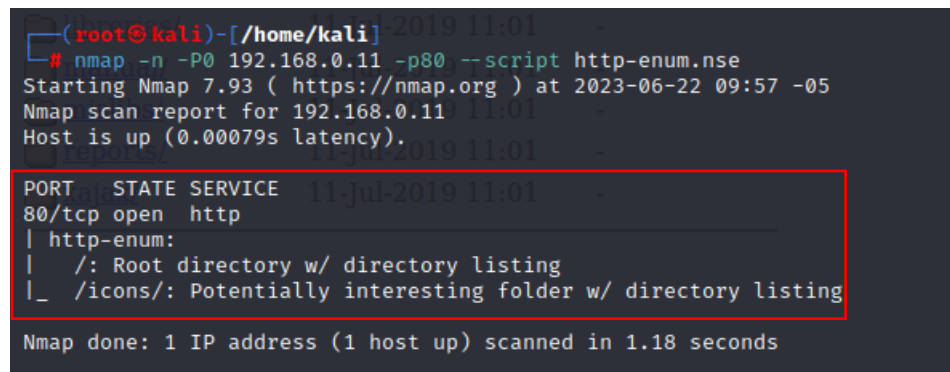
Ataque 01

- En esta primera prueba se realizó un ataque de reconocimiento sobre la vulnerabilidad http-enum.nse dirigida hacia el puerto 80, tratando de explorar que carpetas o directorios de la aplicación web sisgedo v.2.0 se están listando con la finalidad de acceder a archivos con información relevante, copiar el contenido de la aplicación o clonación de la misma. Utilizamos la herramienta nmap ejecutando el siguiente script.

```
nmap -n -P0 192.168.0.11 -p80 --script http-enum.nse
```

Figura 21

Ejecución de ataque 01 con nmap



```
(root@kali)-[/home/kali] 2019 11:01
# nmap -n -P0 192.168.0.11 -p80 --script http-enum.nse
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 09:57 -05
Nmap scan report for 192.168.0.11
Host is up (0.00079s latency).
PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|   /: Root directory w/ directory listing
|_  /icons/: Potentially interesting folder w/ directory listing
Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
```

Fuente: Elaboración propia

Detección del ataque

- Para la detección del ataque se utilizó la herramienta security onion (SIEM), logrando detectar el ataque hacia el servidor web en tiempo real. Utilizamos la suite de herramientas de security onion para la detección de ataques.

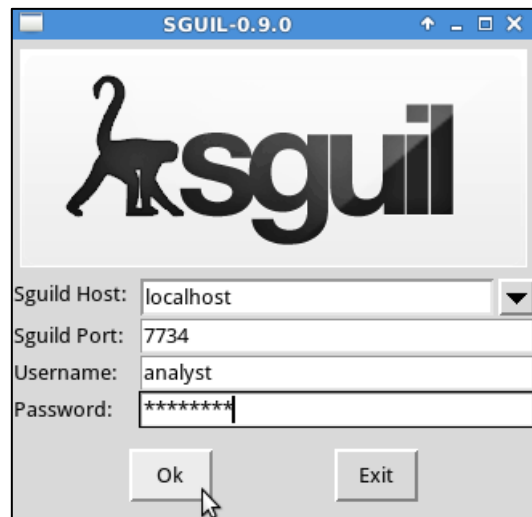
Sguil

Teniendo en cuenta a Brisa (2018) describe a sguil como una herramienta de análisis de eventos de red desarrollada por analistas de seguridad de redes, esta herramienta consta de varios sistemas que trabajan de manera integrada para ayudarnos a monitorear la seguridad de nuestras redes informáticas en tiempo real. Además, proporciona funciones de gestión y clasificación de eventos e información sobre los datos de sesión y alcances de paquetes de red.

- Utilizamos la herramienta sguil para monitorear la red durante la detección de los ataques ejecutados, por lo que accederemos a esta herramienta ingresando las siguientes credenciales: **analyst- cyberops**, posteriormente seleccionamos todas las interfaces de red e iniciamos la herramienta.

Figura 22

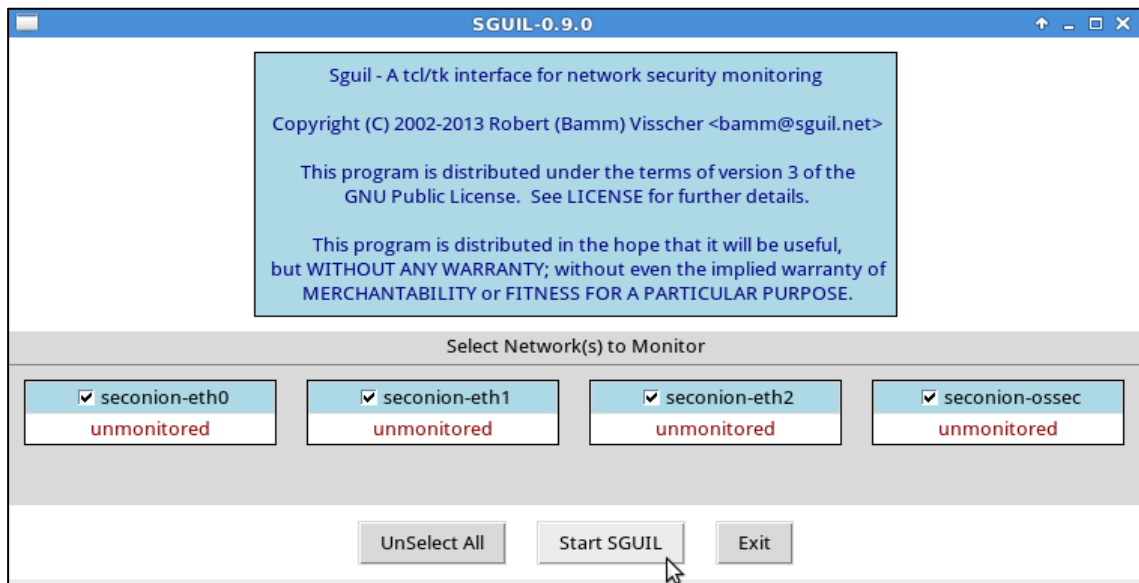
Interfaz de inicio de sesión de la herramienta sguil



Fuente: Elaboración propia

Figura 23

Interfaz de selección de interfaces de red



Fuente: Elaboración propia

- En la consola de la herramienta sguil podemos observar lo siguiente: la cantidad de eventos registrados en tiempo real durante la ejecución del ataque, el sensor de security onion, id de la alerta, fecha y hora en que se registraron los eventos, las ip de origen y destino, también observamos los puertos de origen y destino, finalmente en la última columna observamos el mensaje del evento. Por otra parte, utilizamos tecnologías integradas a la herramienta sguil para generar y examinar el contenido de paquetes de red capturados.

Figura 24

Eventos registrados durante el ataque 01 con sgul I

File

Query

Reports

Sound: Off

ServerName: localhost

UserName: analyst

UserID: 2

2023-07-12 02:12:50 GMT

RealTime Events

Escalated Events

..	/	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT		7	seconio...	7.13146	2023-07-12 01:26:29	209.165.201.17	47922	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
RT		7	seconio...	7.13147	2023-07-12 01:26:29	209.165.201.17	47922	192.168.0.11	80	6	ET SCAN Possible Nmap User-Agent Observed
RT		7	seconio...	3.7896	2023-07-12 01:26:29	209.165.201.17	47922	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
RT		7	seconio...	3.7897	2023-07-12 01:26:29	209.165.201.17	47922	192.168.0.11	80	6	ET SCAN Possible Nmap User-Agent Observed

IP Resolution

Agent Status

Short Statistics

System Msgs

User Msgs

☒ Reverse DNS

☒ Enable External DNS

Src IP:

209.165.201.17

Src Name:

209-165-201-17.got.net

Dst IP:

192.168.0.11

Dst Name:

Unknown

☐ Show Packet Data

☒ Show Rule

alert tcp \$EXTERNAL_NET any -> \$HOME_NET \$HTTP_PORTS (msg:"ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)"; flow:to_server,established; content:"User-Agent [3a] Mozilla/5.0 (compatible [3b] Nmap Scripting Engine"; fast_pattern:38,20; http_header; nocase; reference:url,doc.emergingthreats.net/2009358; classtype:web-application-attack; sid:2009358; rev:5;)/nsm/server_data/securityonion/rules/seconion-eth2-1/downloaded.rules: Line 11345

Fuente: Elaboración propia

Figura 25

Eventos registrados durante el ataque 01 con sgul II

SGUIL-0.9.0 - Connected To localhost

FileQueryReports

Sound: Off

ServerName: localhost

UserName: analyst

UserID: 2

2023-07-12 02:15:21 GMT

RealTime EventsEscalated Events7.13146

CloseExport

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-...	7.13146	2023-07-12 01:26:29	209.165.201.17	47922	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting E...
RT	1	seconion-...	7.13148	2023-07-12 01:26:29	209.165.201.17	47934	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting E...
RT	1	seconion-...	7.13150	2023-07-12 01:26:29	209.165.201.17	47948	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting E...
RT	1	seconion-...	7.13152	2023-07-12 01:26:29	209.165.201.17	47964	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting E...
RT	1	seconion-...	7.13154	2023-07-12 01:26:29	209.165.201.17	47980	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting E...
RT	1	seconion-...	7.13156	2023-07-12 01:26:29	209.165.201.17	47990	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting E...
RT	1	seconion-...	7.13158	2023-07-12 01:26:30	209.165.201.17	48112	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting E...

IP ResolutionAgent StatusShort StatisticsSystem MsgsUser Msgs

☒ Reverse DNS☒ Enable External DNS

Src IP: 209.165.201.17

Src Name: 209-165-201-17.got.net

Dst IP: 192.168.0.11

Dst Name: Unknown

Show Packet DataShow Rule

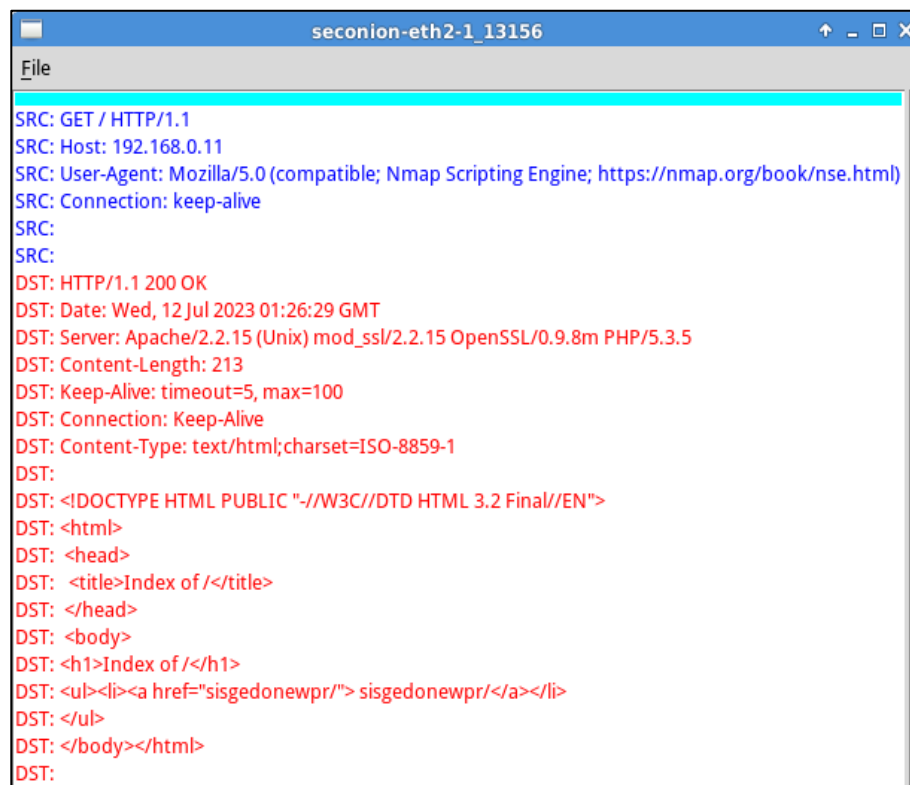
alert tcp \$EXTERNAL_NET any -> \$HOME_NET \$HTTP_PORTS (msg:"ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)"; flow:to_server,established; content:"User-Agent [3a] Mozilla/5.0 (compatible [3b] Nmap Scripting Engine"; fast_pattern:38,20; http_header; nocase; reference:url,doc.emergingthreats.net/2009358; classtype:web-application-attack; sid:2009358; rev:5;)/nsm/server_data/securityonion/rules/seconion-eth2-1/downloaded.rules: Line 11345

Fuente: Elaboración propia

De las siguientes interfaces observamos que se han detectado eventos indicando un escaneo con la herramienta nmap, así mismo podemos visualizar las direcciones ips de donde provienen y hacia donde van dirigidos estos ataques de reconocimiento.

Figura 26

Transcripción de paquetes de red capturado



```
seconion-eth2-1_13156
File
SRC: GET / HTTP/1.1
SRC: Host: 192.168.0.11
SRC: User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
SRC: Connection: keep-alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Wed, 12 Jul 2023 01:26:29 GMT
DST: Server: Apache/2.2.15 (Unix) mod_ssl/2.2.15 OpenSSL/0.9.8m PHP/5.3.5
DST: Content-Length: 213
DST: Keep-Alive: timeout=5, max=100
DST: Connection: Keep-Alive
DST: Content-Type: text/html; charset=ISO-8859-1
DST:
DST: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
DST: <html>
DST: <head>
DST: <title>Index of /</title>
DST: </head>
DST: <body>
DST: <h1>Index of /</h1>
DST: <ul><li><a href="sisgedonewpr/">sisgedonewpr</a></li>
DST: </ul>
DST: </body></html>
DST:
```

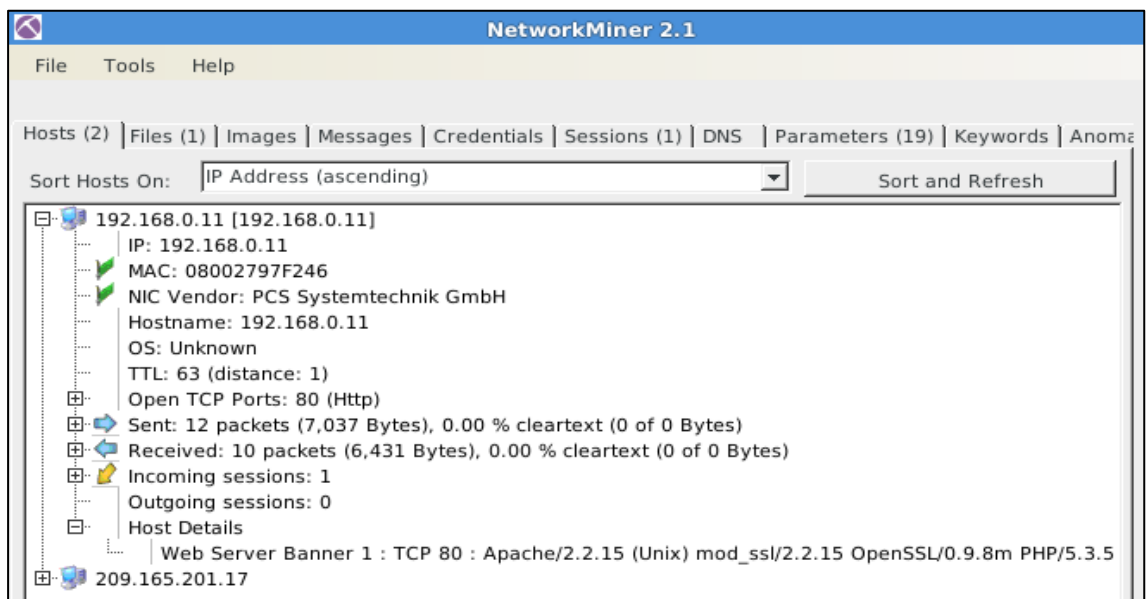
Fuente: Elaboración propia

Networkminer

Networkminer es una herramienta forense de código abierto, utilizada para análisis de seguridad de red, permitiendo extraer información de logs, archivos, credenciales, imágenes y correos electrónicos de los paquetes de red capturados en archivos de tipo pcap, así mismo poder reconocer a detalle todos los dispositivos que están conectados a la red. (NETRESEC, 2023)

Figura 27

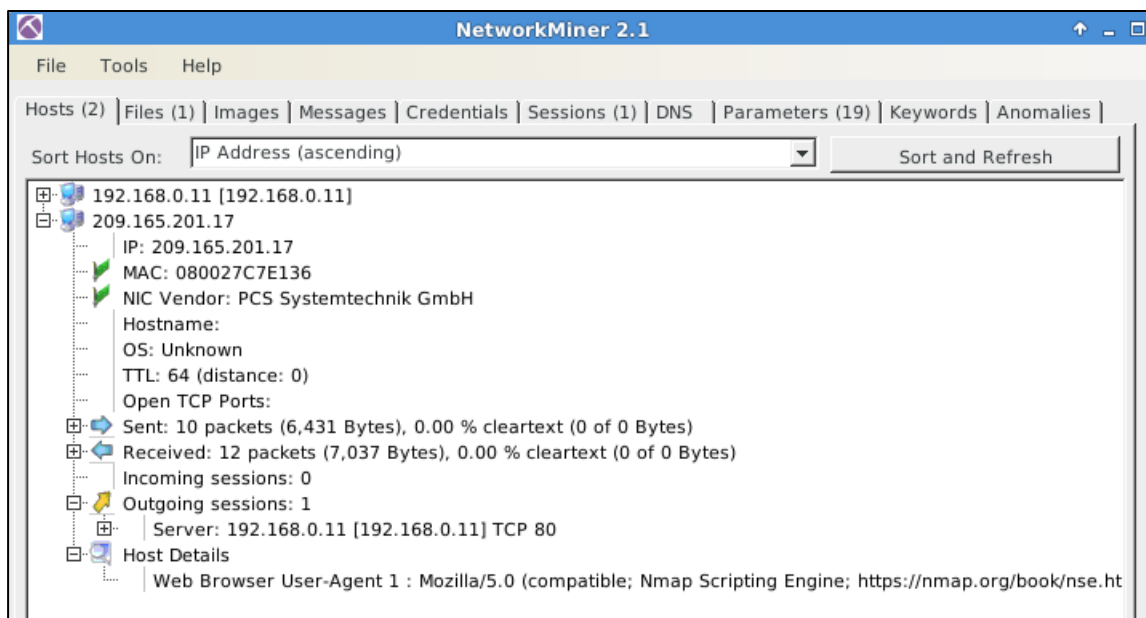
Información de los hosts conectados I en la red con networkminer



Fuente: Elaboración propia

Figura 28

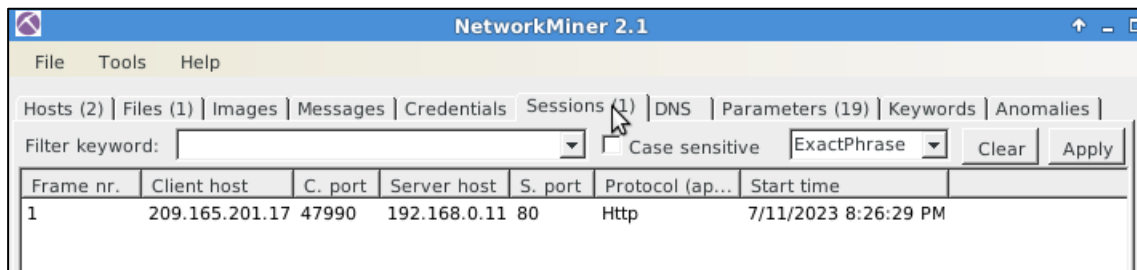
Información de los hosts conectados I en la red con networkminer



Fuente: Elaboración propia

Figura 29

Información de la sesión activa con networkminer



The screenshot shows the NetworkMiner 2.1 application window. The 'Sessions' tab is selected in the top menu. Below the menu, there is a filter keyword field and a 'Case sensitive' checkbox. The main table displays session information for frame 1.

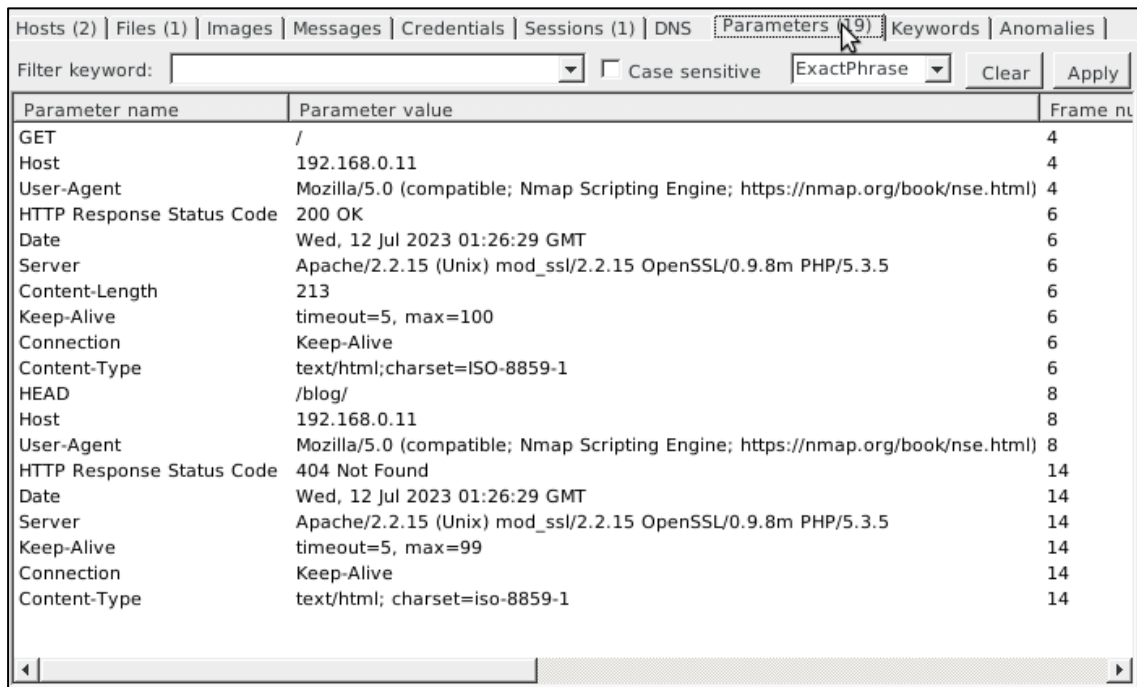
Frame nr.	Client host	C. port	Server host	S. port	Protocol (ap...	Start time
1	209.165.201.17	47990	192.168.0.11	80	Http	7/11/2023 8:26:29 PM

Fuente: Elaboración propia

En las siguientes interfaces de la herramienta networkminer podemos observar información detallada de los hosts descubiertos durante el monitoreo de la red como su dirección ip, dirección mac, sesiones establecidas, cantidad de paquetes enviados y recibidos de los hosts que se encuentran en la red.

Figura 30

Detalle de los parámetros del tráfico de red con networkminer



The screenshot shows the NetworkMiner 2.1 application window with the 'Parameters' tab selected. The table displays detailed parameters for two frames (4 and 14).

Parameter name	Parameter value	Frame nr
GET	/	4
Host	192.168.0.11	4
User-Agent	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	4
HTTP Response Status Code	200 OK	6
Date	Wed, 12 Jul 2023 01:26:29 GMT	6
Server	Apache/2.2.15 (Unix) mod_ssl/2.2.15 OpenSSL/0.9.8m PHP/5.3.5	6
Content-Length	213	6
Keep-Alive	timeout=5, max=100	6
Connection	Keep-Alive	6
Content-Type	text/html; charset=ISO-8859-1	6
HEAD	/blog/	8
Host	192.168.0.11	8
User-Agent	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	8
HTTP Response Status Code	404 Not Found	14
Date	Wed, 12 Jul 2023 01:26:29 GMT	14
Server	Apache/2.2.15 (Unix) mod_ssl/2.2.15 OpenSSL/0.9.8m PHP/5.3.5	14
Keep-Alive	timeout=5, max=99	14
Connection	Keep-Alive	14
Content-Type	text/html; charset=iso-8859-1	14

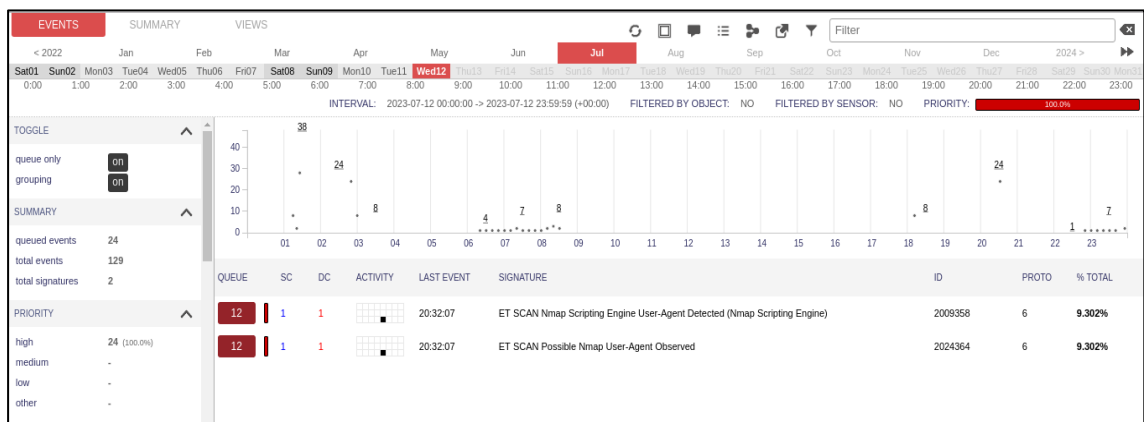
Fuente: Elaboración propia

Squert

Según Ortega (2020) describe que squert es una de las aplicaciones web de security onion la cual posibilita visualizar y realizar consultas de los eventos almacenados en la base de datos de Sguil a través de una interfaz intuitiva, como son representaciones de series de tiempo, resultados ponderados y en grupos lógicamente, además te permite visualizar los datos mediante el mapeo de geo-IP.

Figura 31

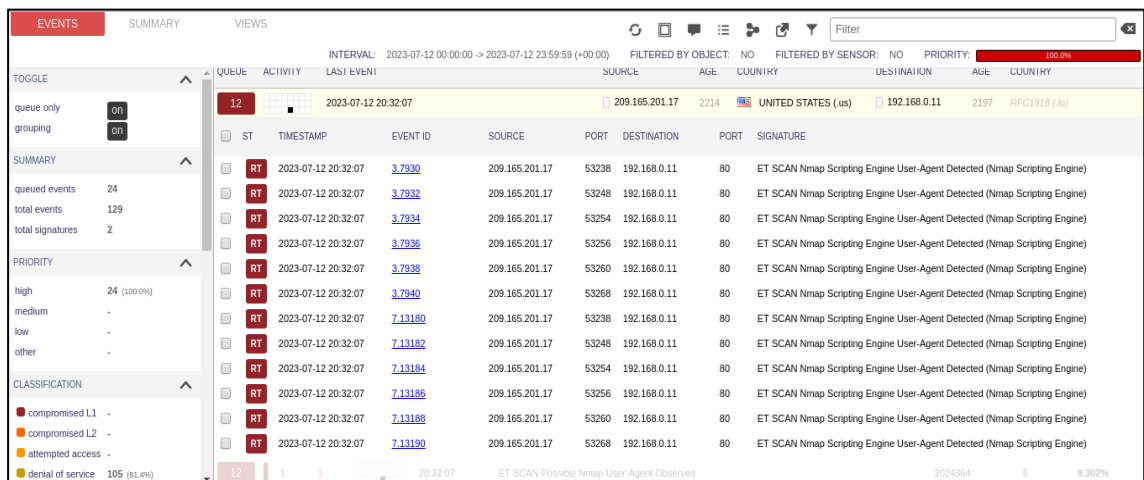
Eventos registrados de manera agrupada con squert



Fuente: Elaboración propia

Figura 32

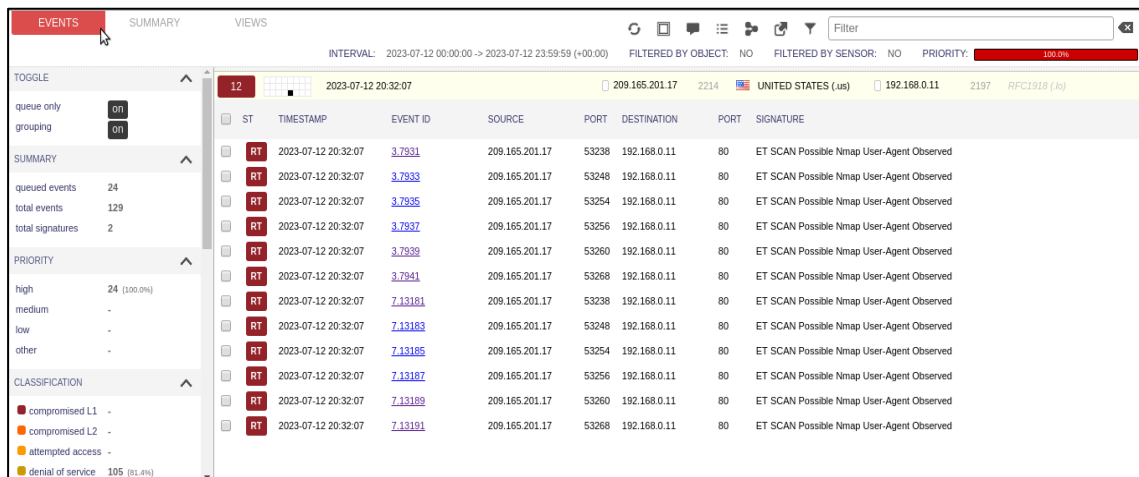
Eventos correlacionados con squert



Fuente: Elaboración propia

Figura 33

Eventos correlacionados con squert II

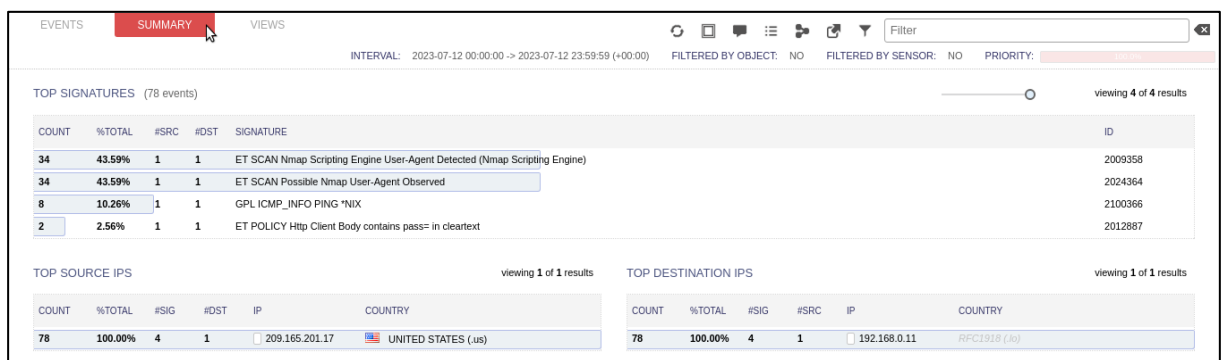


Fuente: Elaboración propia

En las siguientes interfaces de la herramienta squert se visualizan los eventos de manera agrupada, cargados desde la base de datos de Sguil. Estas interfaces ayudan a identificar sesiones o comportamientos sospechosos.

Figura 34

Interfaz de Resumen de la herramienta squert



Fuente: Elaboración propia

De la siguiente interfaz observamos que existe una actividad de escaneo con la herramienta nmap desde la ip 209.165.201.17 hacia la ip 192.168.0.11 dónde se encuentra alojado la aplicación web sisgedo, podemos deducir que el servidor está recibiendo ataques de reconocimiento.

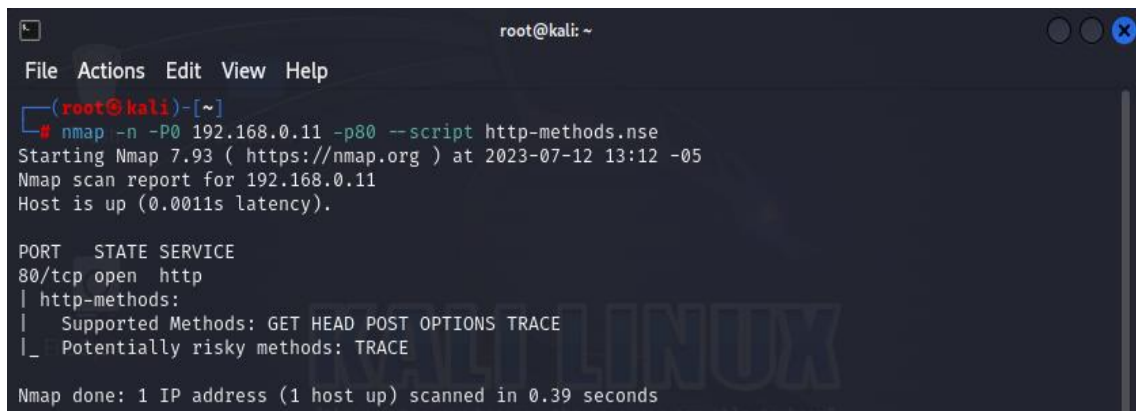
Ataque 02

- Para esta prueba se ejecutó un segundo ataque de reconocimiento con el fin de obtener información sobre los métodos de petición http que soporta el servidor web donde se encuentra alojado la aplicación web sisgedo v.2.0. Se ejecutó el siguiente script utilizando la herramienta nmap.

```
nmap -n -P0 192.168.0.11 -p80 --script http-methods.nse
```

Figura 35

Ejecución de ataque 02 con nmap



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# nmap -n -P0 192.168.0.11 -p80 --script http-methods.nse  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-12 13:12 -05  
Nmap scan report for 192.168.0.11  
Host is up (0.0011s latency).  
  
PORT      STATE SERVICE  
80/tcp    open  http  
| http-methods:  
|   Supported Methods: GET HEAD POST OPTIONS TRACE  
|_  Potentially risky methods: TRACE  
  
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

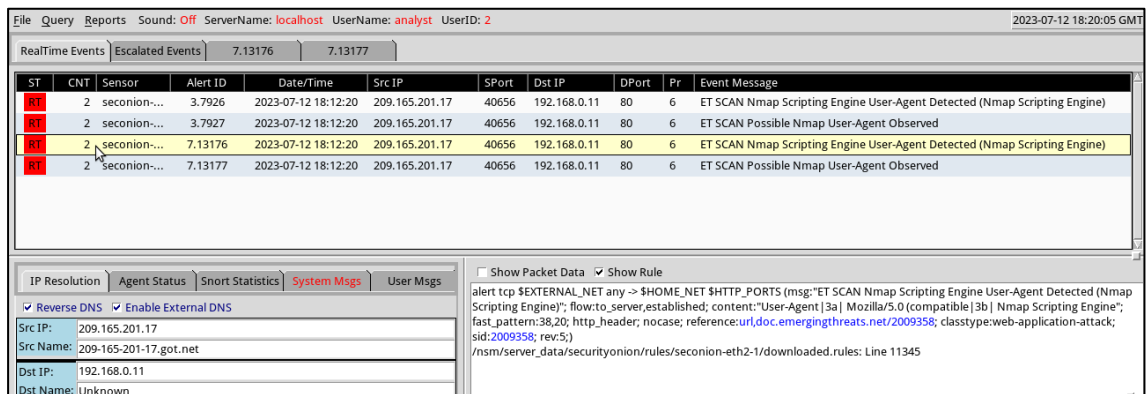
Fuente: Elaboración propia

Detección del Ataque

- Para la detección del ataque continuamos utilizando la herramienta security onion (SIEM), logrando detectar el escaneo de métodos de petición hacia el servidor web en tiempo real.

Figura 36

Eventos registrados durante el ataque 02 con sgul I

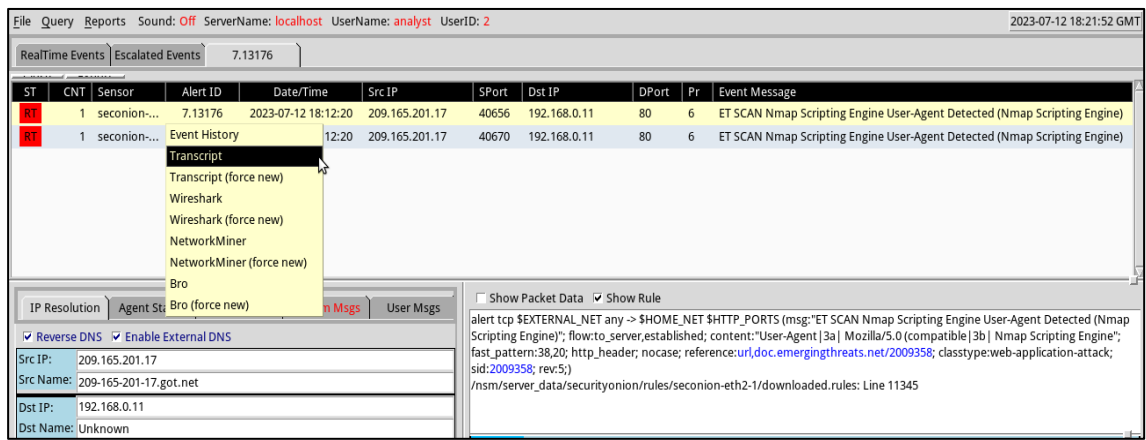


ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	seconion-...	3.7926	2023-07-12 18:12:20	209.165.201.17	40656	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
RT	2	seconion-...	3.7927	2023-07-12 18:12:20	209.165.201.17	40656	192.168.0.11	80	6	ET SCAN Possible Nmap User-Agent Observed
RT	2	seconion-...	7.13176	2023-07-12 18:12:20	209.165.201.17	40656	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
RT	2	seconion-...	7.13177	2023-07-12 18:12:20	209.165.201.17	40656	192.168.0.11	80	6	ET SCAN Possible Nmap User-Agent Observed

Fuente: Elaboración propia

Figura 37

Eventos registrados durante el ataque 02 con sgul II



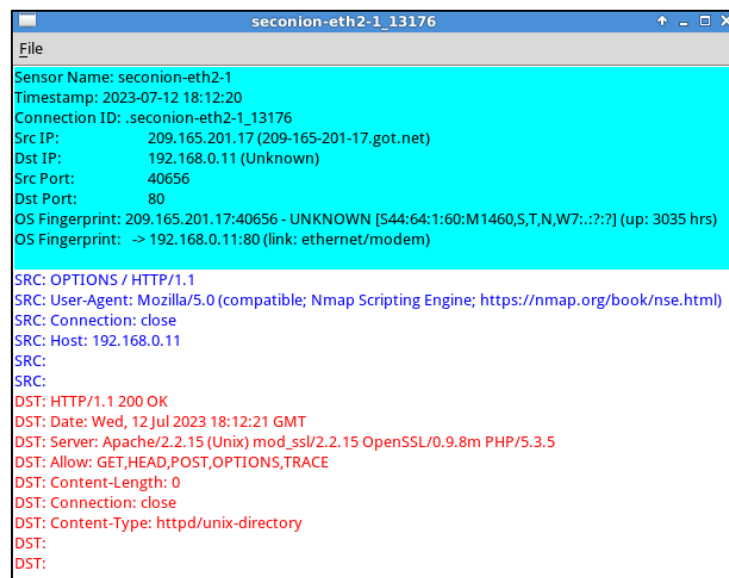
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-...	7.13176	2023-07-12 18:12:20	209.165.201.17	40656	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
RT	1	seconion-...	7.13176	2023-07-12 18:12:20	209.165.201.17	40670	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)

Fuente: Elaboración propia

De las siguientes interfaces observamos que se han detectado eventos indicando un escaneo con la herramienta nmap, así mismo podemos visualizar las direcciones ips de donde provienen y hacia donde van dirigidos estos ataques de reconocimiento. Generamos el contenido de los paquetes de red capturados durante el monitoreo con la opción transcrip y networkminer.

Figura 38

Transcripción de paquetes de red capturado

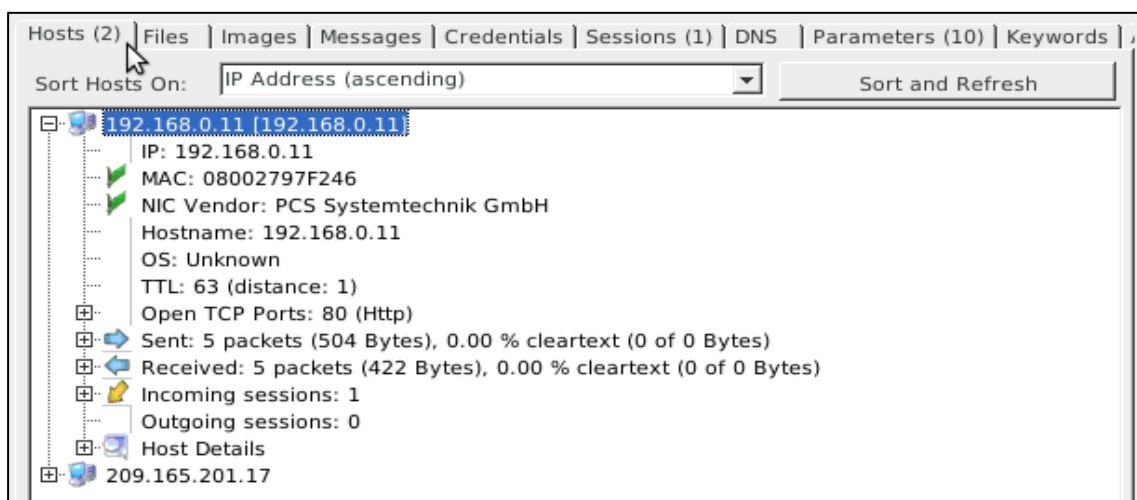


Fuente: Elaboración propia

En la siguiente interfaz podemos visualizar una solicitud para comprobar que métodos de petición están permitidos teniendo como respuesta información del servidor y una lista de métodos http habilitados entre ellos el método trace, considerado como riesgo potencial.

Figura 39

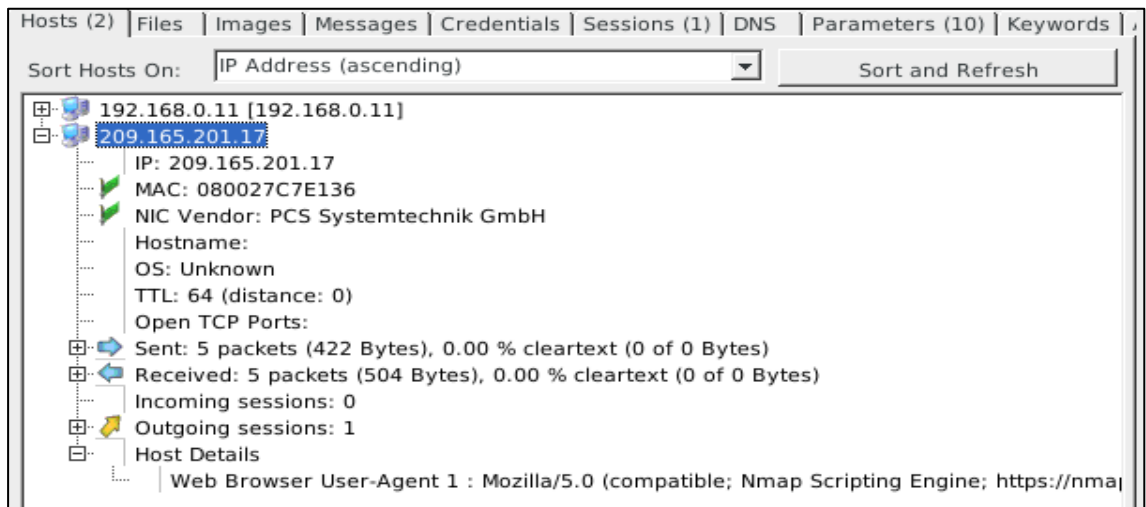
Información de los hosts conectados I en la red con networkminer



Fuente: Elaboración propia

Figura 40

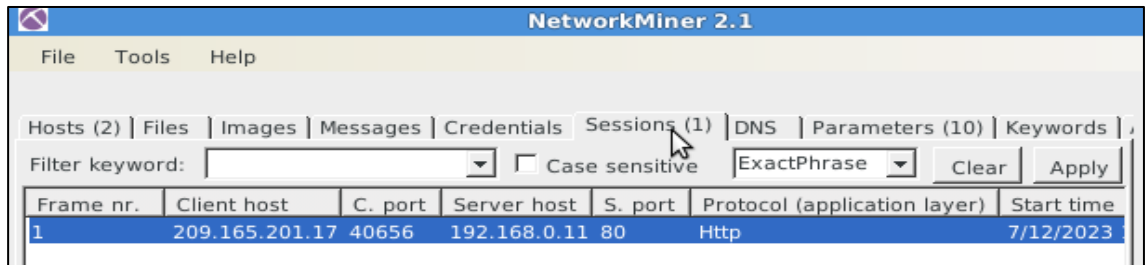
Información de los hosts conectados II en la red con networkminer



Fuente: Elaboración propia

Figura 41

Información de las sesiones activas del tráfico de red con networkminer



Fuente: Elaboración propia

En las siguientes interfaces de la herramienta networkminer podemos observar información detallada de los hosts descubiertos durante el monitoreo de la red como su dirección ip, dirección mac, sesiones establecidas, cantidad de paquetes enviados y recibidos de los hosts que se encuentran en la red.

Figura 42

Información de los parámetros del tráfico de red con networkminer

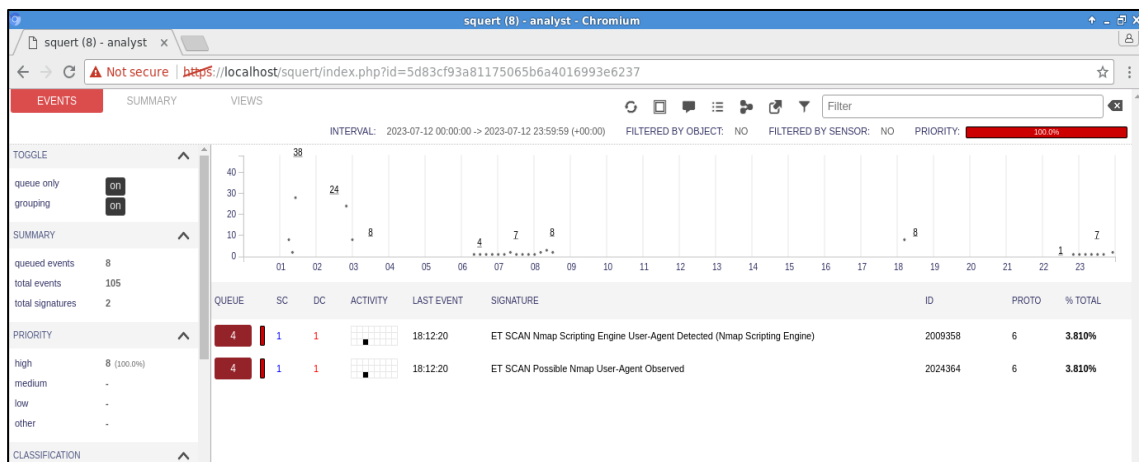
Hosts (2) Files Images Messages Credentials Sessions (1) DNS Parameters (10) Keywords	
Filter keyword:	<input type="text"/> <input type="checkbox"/> Case sensitive <input type="button" value="ExactPhrase"/> <input type="button" value="Clear"/> <input type="button" value="Apply"/>
Parameter name	Parameter value
OPTIONS	/
User-Agent	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/n..
Host	192.168.0.11
HTTP Response Status Code	200 OK
Date	Wed, 12 Jul 2023 18:12:21 GMT
Server	Apache/2.2.15 (Unix) mod_ssl/2.2.15 OpenSSL/0.9.8m PHP/5.3.5
Allow	GET,HEAD,POST,OPTIONS,TRACE
Content-Length	0
Connection	close
Content-Type	httpd/unix-directory

Fuente: Elaboración propia

En la siguiente interfaz observamos que se realizó un ataque de reconocimiento consultando los métodos http permitidos desde la herramienta nmap, teniendo una respuesta exitosa por parte del servidor y listando los métodos de petición permitidos, entre ellos el se encontró el método de riesgo potencial trace.

Figura 43

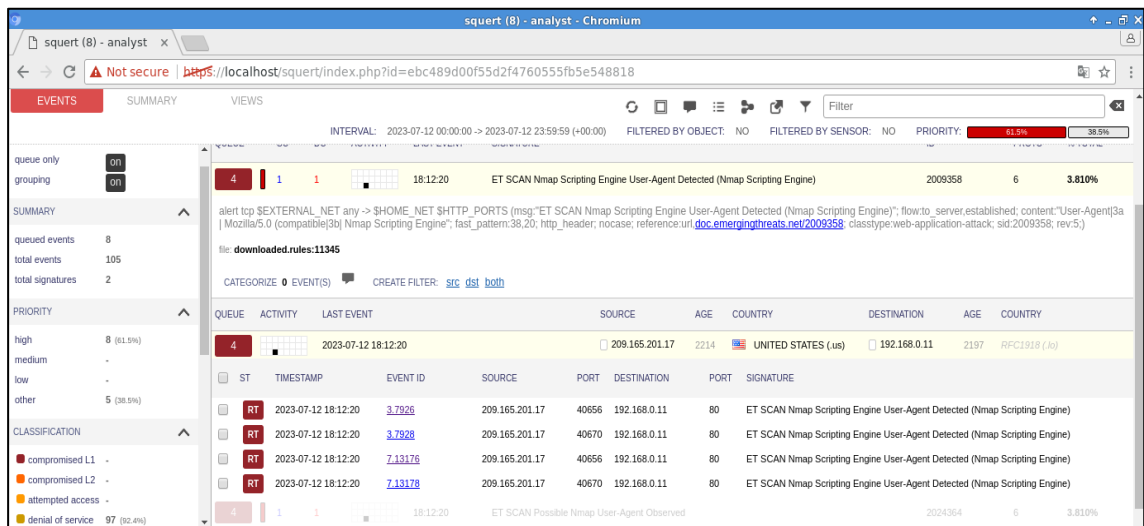
Eventos registrados de manera agrupada con squert



Fuente: Elaboración propia

Figura 44

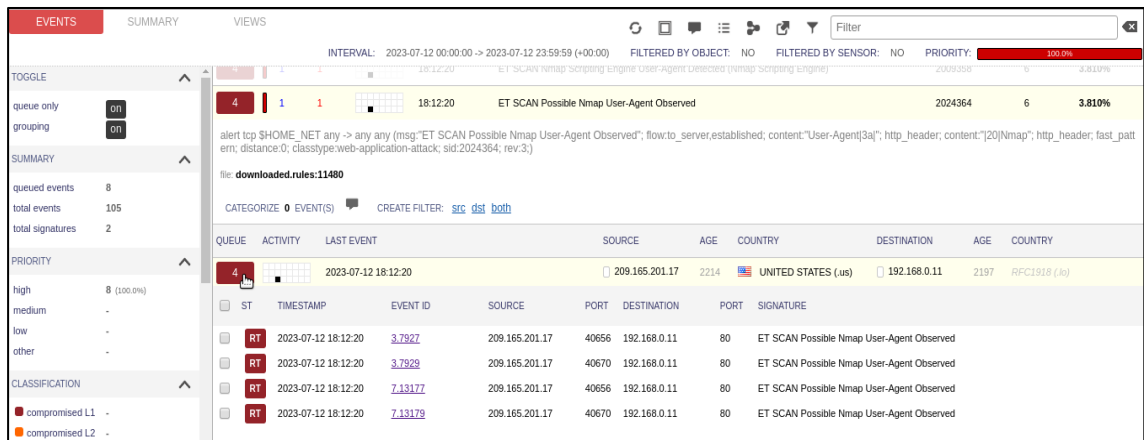
Eventos correlacionados con squert I



Fuente: Elaboración propia

Figura 45

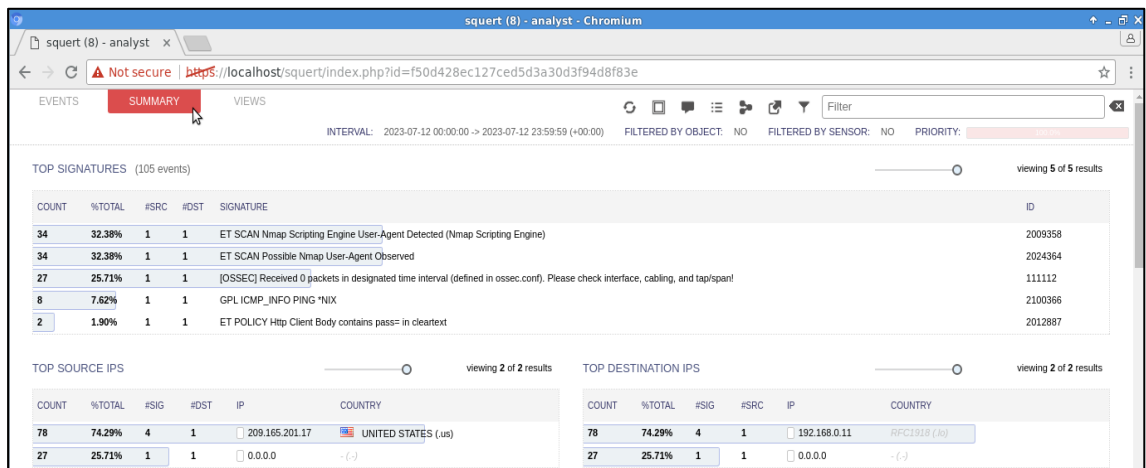
Eventos correlacionados con squert II



Fuente: Elaboración propia

Figura 46

Interfaz de Resumen de la herramienta squert

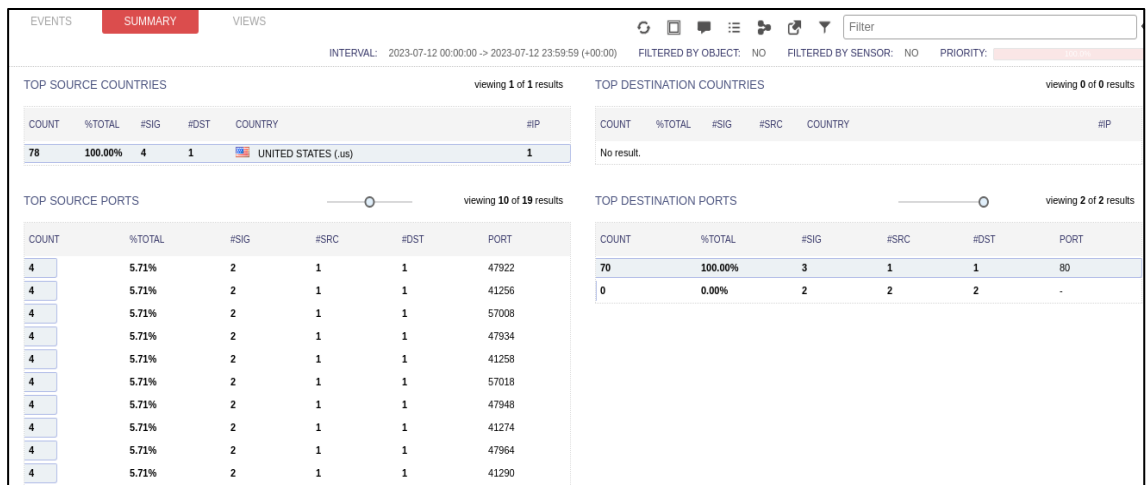


Fuente: Elaboración propia

De la siguientes interfaz observamos que existe una actividad de escaneo con la herramienta nmap desde la ip 209.165.201.17 hacia la ip del servidor 192.168.0.11 dónde se encuentra alojado la aplicación web sisgedo, podemos deducir que el servidor está recibiendo ataques de reconocimiento.

Figura 47

Interfaz de Resumen de la herramienta squert II

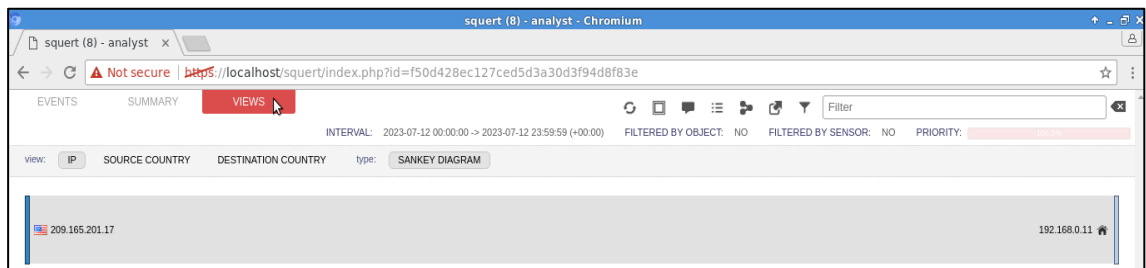


Fuente: Elaboración propia

En esta interfaz observamos que este tipo de escaneos con nmap mayormente van dirigidos hacia el puerto 80 que ejecuta el servicio http.

Figura 48

Vista de geolocalización con Squert



Fuente: Elaboración propia

En esta vista podemos observar la relación que existe entre las ips 209.165.201.17 y 192.168.0.11, y así mismo su geolocalización.

3.3. Mitigación de vulnerabilidades

- Como propuesta de mitigación del ataque 01 de reconocimiento ejecutado se editó la directiva **DirectoryIndex** en el archivo de configuración del servidor web apache **httpd.conf**, deshabilitando los índices de directorio.

Figura 49

Eventos registrados durante el escaneo de vulnerabilidades del puerto 80 con sgul II

```
<Directory "/var/www/html">
#
# Possible values for the Options directive are "None", "All",
# or any combination of:
#   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
#
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
#
# The Options directive is both complicated and important. Please see
# http://httpd.apache.org/docs/2.2/mod/core.html#options
# for more information.
#
Options -Indexes FollowSymLinks

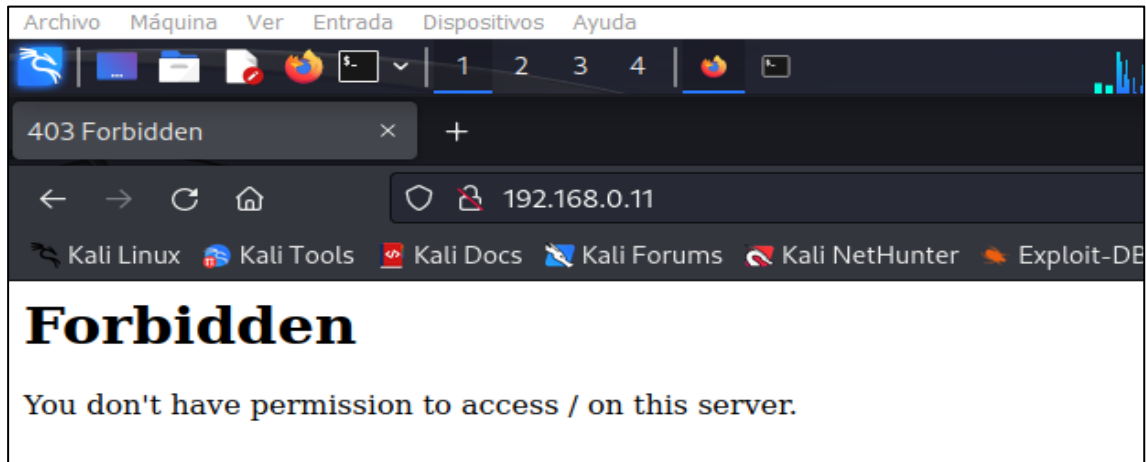
#
# AllowOverride controls what directives may be placed in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
147,35 32%
```

Fuente: Elaboración propia

- Se intentó explorar nuevamente el listado de directorios obteniendo como respuesta el error 403, restringiendo el acceso al sitio web y de esta manera evitar que los atacantes puedan acceder a información relevante.

Figura 50

Eventos registrados durante el escaneo de vulnerabilidades del puerto 80 con sguil II



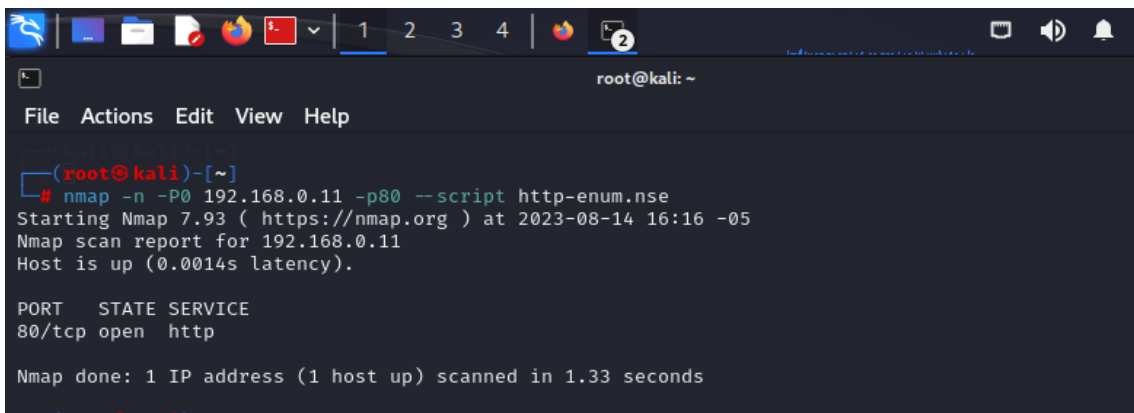
Fuente: Elaboración propia

- Finalmente se logró comprobar que la vulnerabilidad fue mitigada con éxito utilizando la herramienta nmap y ejecutando el siguiente script:

• `nmap -n -P0 192.168.0.11 -p80 --script http-enum.nse`

Figura 51

Escaneo de vulnerabilidades después de la mitigación 01



Fuente: Elaboración propia

Figura 52

Eventos registrados con sgul después de la mitigación.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
ET	1	seconion...	3.7958	2023-08-14 21:15:58	209.165.201.17	51416	192.168.0.11	80	6	ET POLICY Http Client Body contains pass= in cleartext
ET	1	seconion...	7.13208	2023-08-14 21:15:58	209.165.201.17	51416	192.168.0.11	80	6	ET POLICY Http Client Body contains pass= in cleartext
ET	8	seconion...	3.7959	2023-08-14 21:16:18	209.165.201.17	42446	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
ET	8	seconion...	3.7960	2023-08-14 21:16:18	209.165.201.17	42446	192.168.0.11	80	6	ET SCAN Possible Nmap User-Agent Observed
ET	1	seconion...	3.7971	2023-08-14 21:16:18	192.168.0.11	80	209.165.201.17	42480	6	GPL WEB_SERVER 403 Forbidden
ET	8	seconion...	7.13209	2023-08-14 21:16:18	209.165.201.17	42446	192.168.0.11	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
ET	8	seconion...	7.13210	2023-08-14 21:16:18	209.165.201.17	42446	192.168.0.11	80	6	ET SCAN Possible Nmap User-Agent Observed
ET	1	seconion...	7.13221	2023-08-14 21:16:18	192.168.0.11	80	209.165.201.17	42480	6	GPL WEB_SERVER 403 Forbidden
ET	1	seconion...	1.5804	2023-08-15 02:18:28	0.0.0.0	0.0.0.0	0.0.0.0			[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf)...

Fuente: Elaboración propia

- Como propuesta de mitigación del ataque 02 de reconocimiento ejecutado se editó el archivo de configuración del servidor web apache **httpd.conf**, insertando una línea de código para desactivar el método de riesgo potencial TRACE.

Figura 53

Eventos registrados durante el escaneo de vulnerabilidades del puerto 80 con sgul II

```

Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
# at a local disk. If you wish to share the same ServerRoot for multiple
# httpd daemons, you will need to change at least LockFile and PidFile.
#
ServerRoot "/usr/local/zend/apache2"
TraceEnable off
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80

```

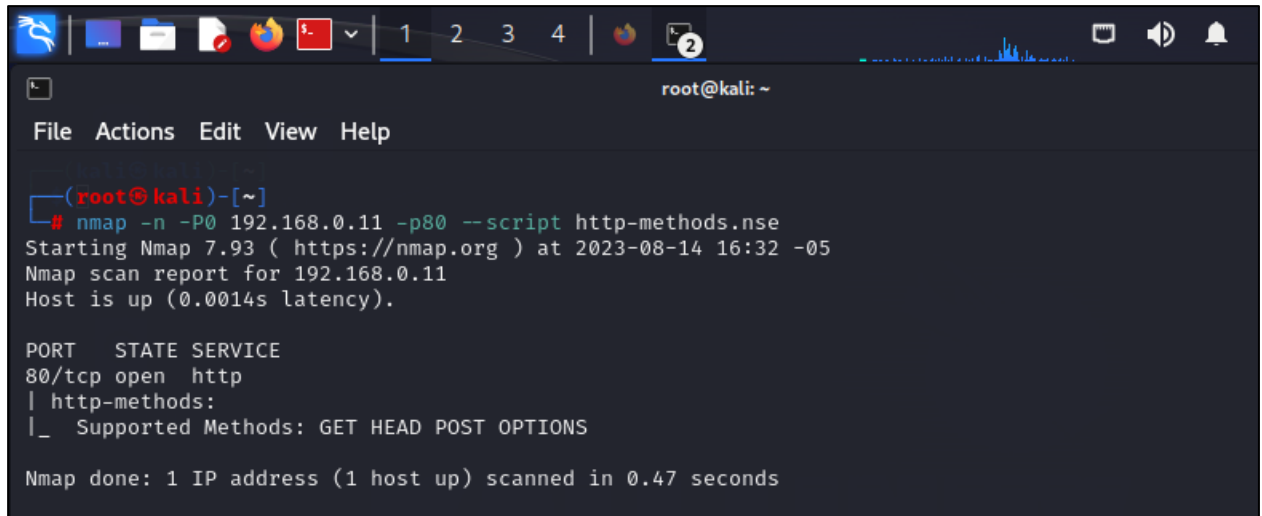
Fuente: Elaboración propia

- Finalmente se logró comprobar que la vulnerabilidad fue mitigada con éxito utilizando la herramienta nmap y ejecutando el siguiente script:

• **`nmap -n -P0 192.168.0.11 -p80 --script http-methods.nse`**

Figura 54

Escaneo de vulnerabilidades después de la mitigación 02



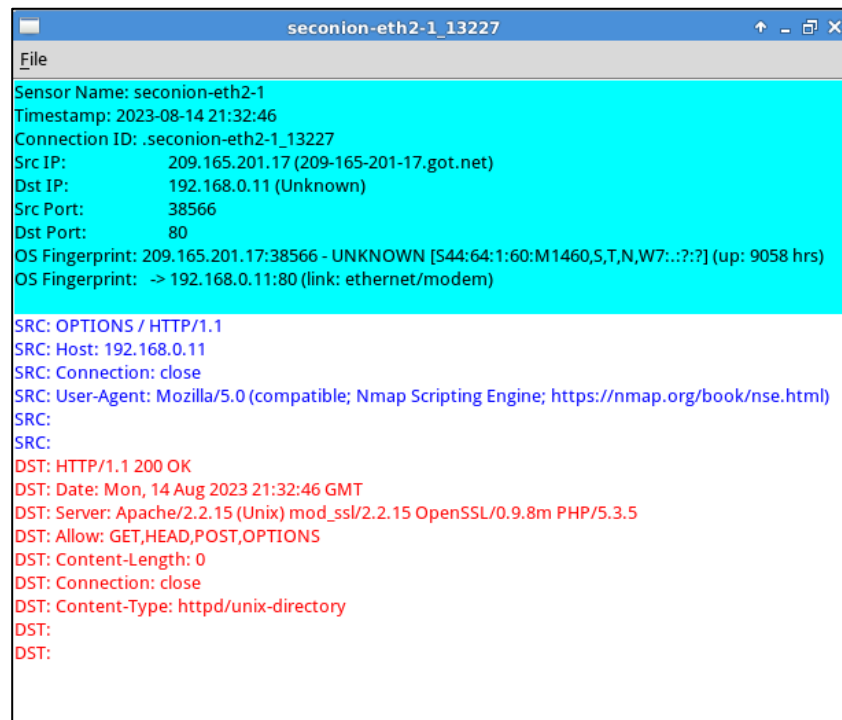
```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# nmap -n -P0 192.168.0.11 -p80 --script http-methods.nse  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-14 16:32 -05  
Nmap scan report for 192.168.0.11  
Host is up (0.0014s latency).  
  
PORT      STATE SERVICE  
80/tcp    open  http  
| http-methods:  
|_ Supported Methods: GET HEAD POST OPTIONS  
  
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

Fuente: Elaboración propia

- En la siguiente captura se muestra la transcripción de paquetes de los eventos registrados durante la comprobación de la mitigación de vulnerabilidades, logrando apreciar los métodos de petición mostrados en la figura 38 excepto el método trace ya que fue inhabilitado con el fin de mitigar el riesgo potencial según el escaneo de vulnerabilidades que nos muestra la figura 35.

Figura 55

Transcripción de los eventos registrados después de la mitigación 02



```
seconion-eth2-1_13227
File
Sensor Name: seconion-eth2-1
Timestamp: 2023-08-14 21:32:46
Connection ID: .seconion-eth2-1_13227
Src IP: 209.165.201.17 (209-165-201-17.got.net)
Dst IP: 192.168.0.11 (Unknown)
Src Port: 38566
Dst Port: 80
OS Fingerprint: 209.165.201.17:38566 - UNKNOWN [S44:64:1:60:M1460,S,T,N,W7:::?:?] (up: 9058 hrs)
OS Fingerprint: -> 192.168.0.11:80 (link: ethernet/modem)

SRC: OPTIONS / HTTP/1.1
SRC: Host: 192.168.0.11
SRC: Connection: close
SRC: User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Mon, 14 Aug 2023 21:32:46 GMT
DST: Server: Apache/2.2.15 (Unix) mod_ssl/2.2.15 OpenSSL/0.9.8m PHP/5.3.5
DST: Allow: GET,HEAD,POST,OPTIONS
DST: Content-Length: 0
DST: Connection: close
DST: Content-Type: httpd/unix-directory
DST:
DST:
```

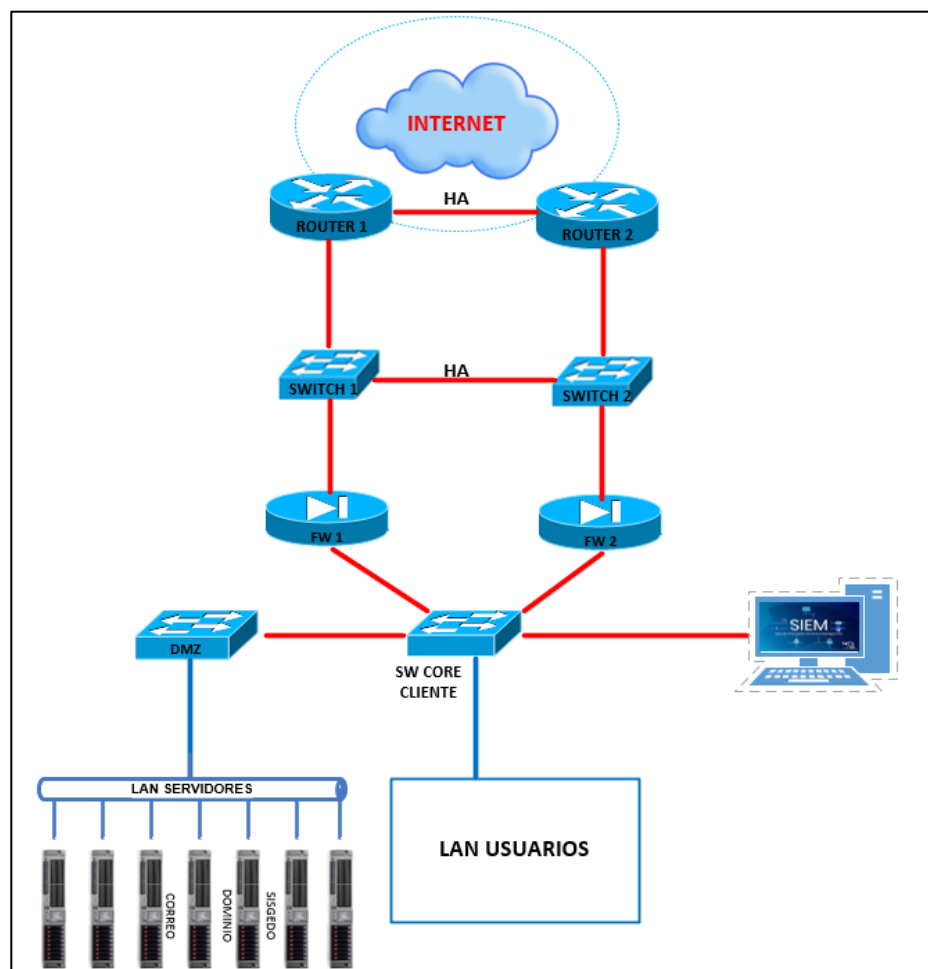
Fuente: Elaboración propia

3.4. Seguimiento y control con la herramienta SIEM

La herramienta de gestión de eventos y seguridad de la información SIEM se ha implementado de acuerdo a la siguiente topología en un lugar estratégico, conectándolo directamente al switch core cliente y configurando el puerto port mirroring con el fin de capturar todo el tráfico que pasa por la red troncal o los puertos troncales, el cual se encargará de recibir toda la información de los eventos que suceden de manera continua para así poder controlar y realizar el seguimiento de toda la red tanto interna como externa de la municipalidad provincial de Chiclayo.

Figura 56

Topología de la Propuesta a implementar



Fuente: Elaboración propia

CAPÍTULO IV. CONCLUSIONES

- Se implementó el sistema de gestión de eventos e información de seguridad-SIEM utilizando software de virtualización y sobre ello se instaló la herramienta security onion.
- La herramienta security onion demostró efectividad al realizar la detección de ataques y gestión de eventos de seguridad en tiempo real sobre el servicio web sisgedo v.2.0 de la municipalidad provincial de Chiclayo.
- Se realizó la mitigación de vulnerabilidades del servicio web sisgedo v.2.0 editando políticas en los archivos de configuración del servicio web y ejecutando la herramienta nmap para comprobar el éxito sobre la mitigación de dichas vulnerabilidades.
- Con la implementación de la herramienta security onion (SIEM) y el conjunto de herramientas que vienen integradas se realizó el seguimiento y control de los eventos de seguridad en tiempo real.

CAPÍTULO V. RECOMENDACIONES

- Implementar un centro de operaciones de seguridad SOC en entidades públicas y privadas con la finalidad de monitorear, detectar y responder incidentes ante posibles ataques informáticos en la red, de manera que puedan proteger sus activos digitales, además capacitar a un equipo de trabajo para la administración eficiente del mismo.
- Contar con herramientas de gestión de eventos e información de seguridad-SIEM para detectar oportunamente los ataques informáticos.
- Considerar la aplicación de las normas internacionales ISO NTP/IEC 27001 según resolución ministerial 004-2016-PCM para la implementación de un sistema de gestión de seguridad de la información, ISO/IEC 22320 para establecer un plan de continuidad de los servicios ante incidentes, específicamente en seguridad de la información.
- Se recomienda realizar proceso de análisis de vulnerabilidades de manera continua con el fin de identificarlas a tiempo y poder reducir o eliminar la superficie de ataque que un atacante podría utilizar para controlar algún sistema o servicio web.
- Se recomienda realizar campañas de concientización en ciberseguridad a todos los trabajadores de la municipalidad provincial de Chiclayo con el propósito de proteger los activos digitales y evitar que sean expuestos.

REFERENCIAS

Ambit. (10 de noviembre de 2020). *Tipos de Vulnerabilidades y Amenazas informáticas*. ambit:

<https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas>

Ariganello, E. (2020). *Redes Cisco, Guía de estudio para la certificación CCNA 200-301*. España: RA-MA

S.A. Editorial y Publicaciones.

https://www.google.com.pe/books/edition/Redes_Cisco_Gu%C3%ADa_de_estudio_para_la_certificaci%C3%B3n_CCNA_200-301/5c-4EAAQBAJ?hl=es-419&gbpv=1

Astudillo, K. (2018). *Kacking Ético* (3ª Edición ed.). España: RA-MA S.A. Editorial y Publicaciones.

Benavides, E., Fuertes, W., & Sanchez, S. (2020). Caracterización de los ataques de phishing y técnicas

para mitigarlos. Ataques: una revisión sistemática de la literatura. *Revista Ciencia y Tecnología*

OJS, 97-104. <https://doi.org/https://doi.org/10.18779/cyt.v13i1.357>

Brisa, S. (07 de julio de 2018). *Squert - Security Art Work*. Security Art Work:

<https://www.securityartwork.es/?s=SQUERT>

Burks, D. (01 de junio de 2023). *Security Onion*. <https://blog.securityonion.net/>

Castillo, J. (5 de noviembre de 2018). *Qué es la virtualización y para qué sirve*. Profesional review:

<https://www.profesionalreview.com/2018/11/05/que-es-virtualizacion/>

Chávez, C. (29 de julio de 2021). *Hacking ético: qué es, fases, informes y análisis*. Segurilatam:

https://www.segurilatam.com/tecnologias-y-servicios/ciberseguridad/hacking-etico-que-es-fases-informes-y-analisis_20210729.html

Cisco. (2023). *¿Qué es la ciberseguridad?* Retrieved 2023 de febrero de 9, from Cisco:

https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~how-cybersecurity-works

Clavo, C. (2022). *Análisis Comparativo De Técnicas De Mitigación De Ataque De DDOS En Cloud*

Computing [Tesis de Título, Universidad Señor de Sipán]. Repositorio Institucional, Pimentel.

<https://hdl.handle.net/20.500.12802/9185>

El Español. (27 de enero de 2023). Los hackers se ceban con la administración pública española: un

45.5% más de ataques en 2022. *El Español*.

Espinoza Peche, M. (2022). *Mitigación de Vulnerabilidades informáticas utilizando un Firewall de*

Software libre con Pfsense en las empresas de revisiones Técnicas de la Ciudad de Tacna en el

año 2021 [Tesis de Título, Universidad Privada de Tacna]. Repositorio Universidad Privada de

Tacna. <http://hdl.handle.net/20.500.12969/2575>

Estela, M. (2020). *Implementación de un security information and event management (SIEM) para*

detectar vulnerabilidades y amenazas expuestas en las plataformas informáticas y redes de una

entidad financiera [Tesis de Título, Universidad Tecnológica del Perú]. Universidad Tecnológica

del Perú, Lima. <https://hdl.handle.net/20.500.12867/3375>

Fer. (24 de noviembre de 2019). *Security Onion – Detección de intrusos*. Caminosdigitales.es:

<https://caminosdigitales.es/security-onion-deteccion-de-intrusos/>

IBM. (13 de diciembre de 2022). *Introducción: servicios Web*. [https://www.ibm.com/docs/es/was-](https://www.ibm.com/docs/es/was-nd/9.0.5?topic=overview-introduction-web-services)

[nd/9.0.5?topic=overview-introduction-web-services](https://www.ibm.com/docs/es/was-nd/9.0.5?topic=overview-introduction-web-services)

incibe. (21 de agosto de 2018). *Qué son los ataques DoS y DDoS*. incibe:

<https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos>

Jotta. (2020). *Hacking: Iníciate en el increíble mundo de la seguridad ofensiva*.

<https://www.google.com.pe/books/edition/Hacking/2UILEAAQBAJ?hl=es-419&gbpv=0>

Kali. (01 de junio de 2021). *Lanzamiento de Kali Linux 2021.2 (Kaboxer, Kali-Tweaks, Bleeding-Edge y puertos privilegiados)*. <https://www.kali.org/blog/kali-linux-2021-2-release/>

Kali. (04 de febrero de 2023). *¿Qué es KaliLinux?* Kali: <https://www.kali.org/docs/introduction/what-is-kali-linux/>

Kaspersky. (2023). *¿Qué es la ciberseguridad?* Retrieved 8 de febrero de 2023, from Kaspersky:

<https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>

Lázaro, D. (2018). *Introducción a los Web Services*. diego: <https://diego.com.es/introduccion-a-los-web-services>

Metric Software Developers. (26 de agosto de 2018). *Virtual Box y Ubuntu Server [Fotografía]*. Metric Software Developers: <https://metric.com.ec/virtual-box-y-ubuntu-server/>

NETRESEC. (2023). *NetworkMiner*. NETRESEC: <https://www.netresec.com/?page=NetworkMiner>

Olivares, J., & Oncins, A. (2018). *Seguridad informática: ethical hacking : conocer el ataque para una mejor defensa*. España: Ediciones ENI.

Optical Networks. (27 de Diciembre de 2021). *Ataques informáticos: Causas, Tipos, Consecuencias y Prevenciones*. Optical Networks: <https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/>

Oracle VM VirtualBox. (12 de octubre de 2022). *Oracle VM VirtualBox*. Oracle:

<https://www.oracle.com/pe/virtualization/virtualbox/>

Ortega, A. (20 de marzo de 2020). *Linkedin*. Descubre todas las capas de tu red empresarial con Security Onion y haz que los hackers e insiders lo piensen dos veces:

<https://www.linkedin.com/pulse/security-onion-introducci%C3%B3n-al-network-monitor-con-de-ortega-s%C3%A1enz/?originalSubdomain=es>

Ortega, J. (2021). *Ciberseguridad. Manual Práctico*. Paraninfo.

<https://books.google.com.pe/books?id=QsROEAAAQBAJ&pg=PA293&dq=CENTRO+DE+OPERACIONES+DE+SEGURIDAD&hl=es-419&sa=X&ved=2ahUKEwi844CW9o39AhUDFLkGHWzIDMYQ6wF6BAgJEAE#v=onepage&q=CENTRO%20DE%20OPERACIONES%20DE%20SEGURIDAD&f=false>

Perú recibió 5,2 mil millones de intentos de ciberataques en la primera mitad de 2022. (24 de agosto de 2022). *El Comercio*. <https://elcomercio.pe/tecnologia/actualidad/ciberseguridad-peru-recibio-52-mil-millones-de-intentos-de-ciberataques-en-la-primera-mitad-de-2022-cibercriminales-espana-mexico-colombia-argentina-noticia/?ref=ecr>

Postigo, A. (2020). *Seguridad Informática* (2020 ed.). España, España: Ediciones Paraninfo, S.A.

https://www.google.com.pe/books/edition/Seguridad_inform%C3%A1tica_Edici%C3%B3n_2020/UCjnDwAAQBAJ?hl=es-419&gbpv=0

Ramos, A. (01 de julio de 2021). *SIEM, gestión de eventos e información de seguridad*. mytra:

<https://www.mytra.es/blog-post/siem-gestion-de-eventos-e-informacion-de-seguridad>

Roa, J. (2018). *Seguridad informática*. McGraw-Hill.

https://profesorezequielruizgarcia.files.wordpress.com/2016/08/seguridad_informatica_mc_graw-hill_2013-2.pdf

- Rodríguez Aburto, W., & Castellón Mena, P. (2019). *Propuesta de detección y mitigación de ataques de denegación de servicios en las redes institucionales DGI [Tesis de Maestría, Universidad Nacional de Ingeniería]*. Repositorio Centroamericano SIIDCA-CSUCA, Nicaragua.
<http://ribuni.uni.edu.ni/3490/1/94803.pdf>
- Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., . . . Castillo, M. (2018). *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades*. Área de Innovación y Desarrollo.
<https://doi.org/>: <http://dx.doi.org/10.17993/IngyTec.2018.46>
- Rosero, J. (2020). *Detección y mitigación de ataques de ingeniería social tipo Phishing utilizando minería de datos [Tesis de Título, Universidad de las Fuerzas Armadas]*. Repositorio Institucional.
<http://repositorio.espe.edu.ec/handle/21000/23409>
- Rouse, M. (agosto de 2017). *Gestión de eventos e información de seguridad (SIEM)*. Retrieved 11 de febrero de 2023, from ComputerWeekly:
<https://www.computerweekly.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM>
- Santos, J. (29 de setiembre de 2022). *Vulnerabilidad informática: Qué es y cómo protegerse*. Delta Protect: <https://www.deltaprotect.com/blog/vulnerabilidad-informatica>
- Santos, J. (16 de febrero de 2023). *¿Qué es el Pentesting? Tipos y cómo utilizarlo para prevenir ciberataques*. Delta Protect: <https://www.deltaprotect.com/blog/que-es-pentesting>
- Shivanandhan, M. (23 de abril de 2023). *Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos*. Freecodecamp:
<https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/>

SorceForget. (07 de Junio de 2016). *Security Onion*. <https://sourceforge.net/projects/security-onion/>

tecmint. (4 de octubre de 2019). *30 cosas que hacer después de una instalación mínima de RHEL/CentOS*

7. tecmint: <https://www.tecmint.com/things-to-do-after-minimal-rhel-centos-7-installation/#C1>

Yesquen, R. (2018). *Prototipo de Detección y Mitigación de Ataques de Denegación de Servicios (DoS), en Servidores Web [Tesis de Título, Universidad Nacional Pedro Ruíz Gallo]*. Repositorio

Institucional. <https://hdl.handle.net/20.500.12893/10405>

ANEXOS

ANEXO 01: GUÍA DE IMPLEMENTACIÓN DEL ENTORNO VIRTUAL

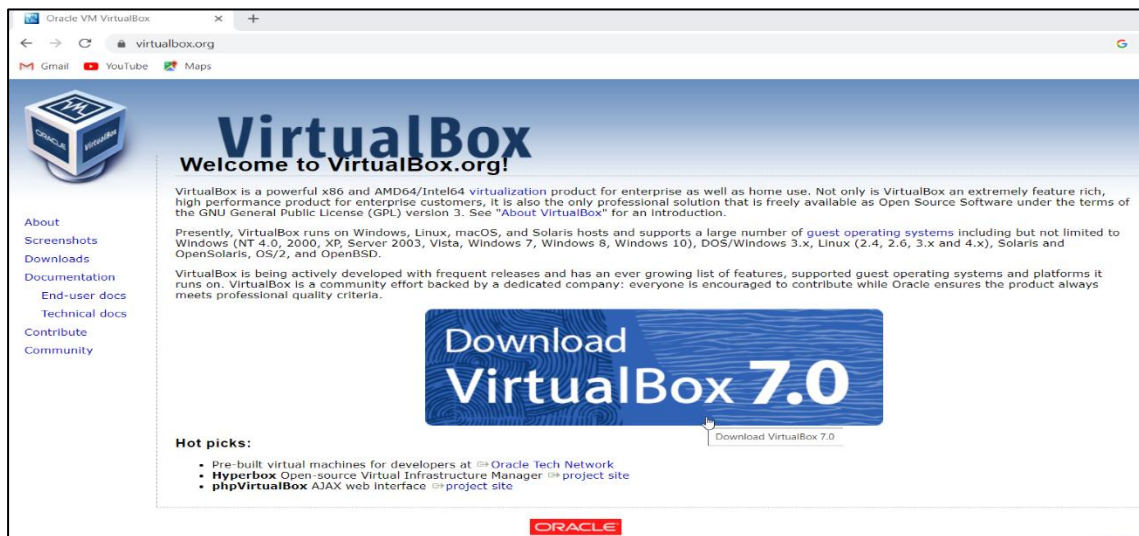
Para la implementación de nuestro entorno virtual se realizó la instalación del software virtual box y la instalación de tres máquinas virtuales con los siguientes sistemas operativos: kali linux, security onion y centos. En esta última se instaló el framework zend server que permitirá administrar aplicaciones php. Por otra parte se instaló el servicio web sisgedo utilizando una réplica exacta al que utiliza la municipalidad provincial de Chiclayo, con el fin de no alterar dicho servicio y a su vez se instaló el sistema gestor de base de datos postgresql.

INSTALACIÓN DE SOFTWARE DE VIRTUALIZACIÓN

- Descargamos el software de virtualización Virtual Box desde su página principal. Link de la página <https://www.virtualbox.org/>.

Figura 57

Página Oficial del Software de Virtualización Virtual Box

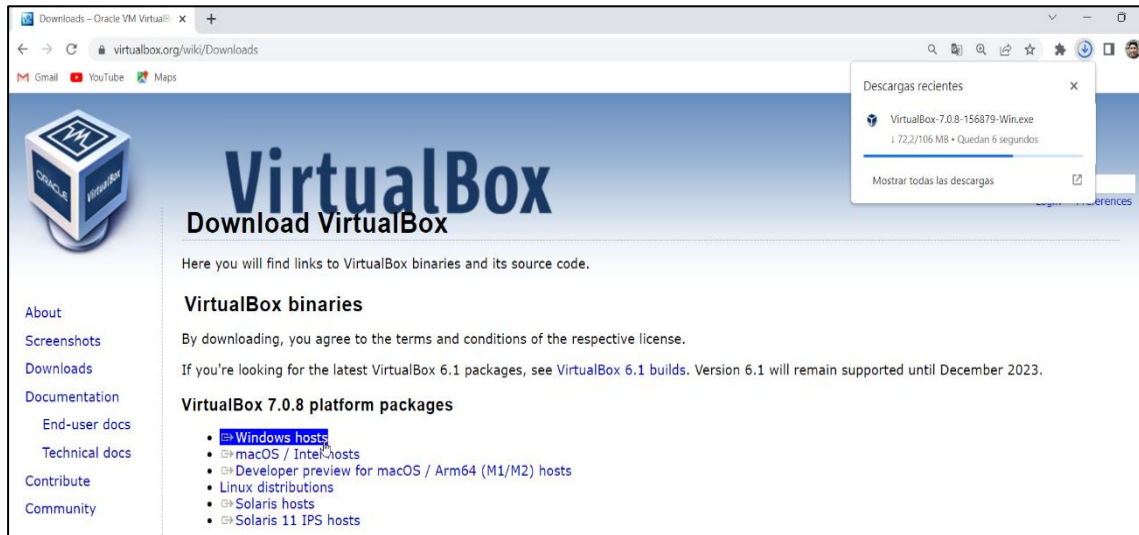


Fuente: Elaboración Propia

- Seleccionamos el paquete de plataforma de acuerdo a nuestro sistema operativo en este caso windows hosts e iniciamos la descarga.

Figura 58

Instaladores Virtual Box



Fuente: Elaboración Propia

- A continuación, ejecutaremos el archivo descargado y empezaremos con el proceso de instalación de Virtual Box.

Figura 59

Proceso de Instalación de Virtual Box



Fuente: Elaboración Propia

- Una vez finalizado el proceso de instalación del software Virtual Box, nos aparecerá una Interfaz de bienvenida.

Figura 60

Interfaz principal de Virtual Box



Fuente: Elaboración Propia

INSTALACIÓN DEL SISTEMA OPERATIVO KALI LINUX EN VIRTUALBOX

- Para la realización de este paso es necesario tener previamente descargado el servicio virtualizado de kali linux, nos ubicamos en la interfaz principal de Virtual Box y seguidamente damos clic en la opción añadir.

Figura 61

Interfaz principal de Virtual Box

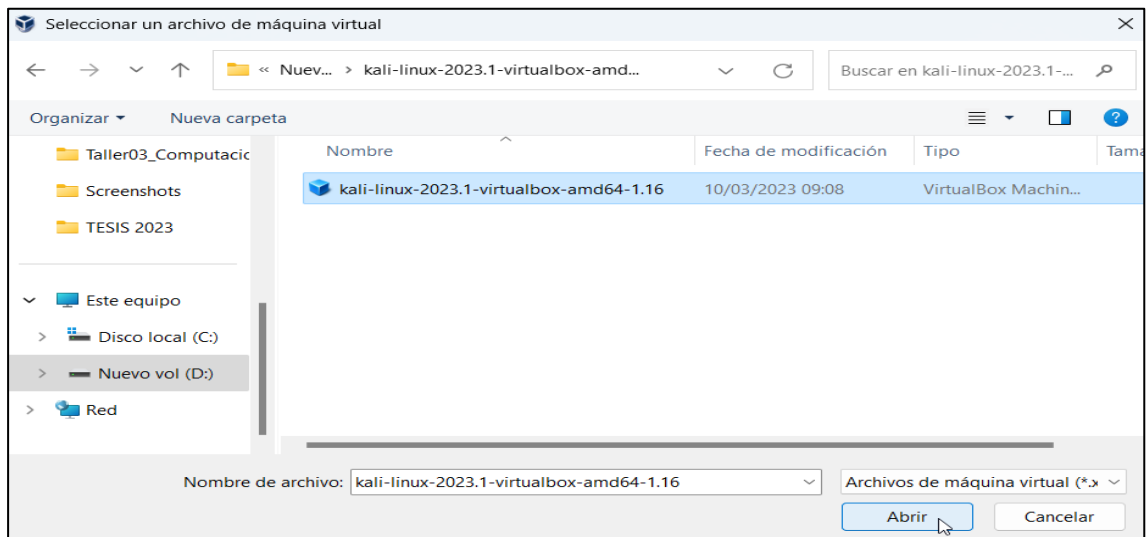


Fuente: Elaboración Propia

- En la siguiente interfaz seleccionaremos el archivo de kali linux descargado y presionamos el botón abrir.

Figura 62

Interfaz del sistema de archivos local

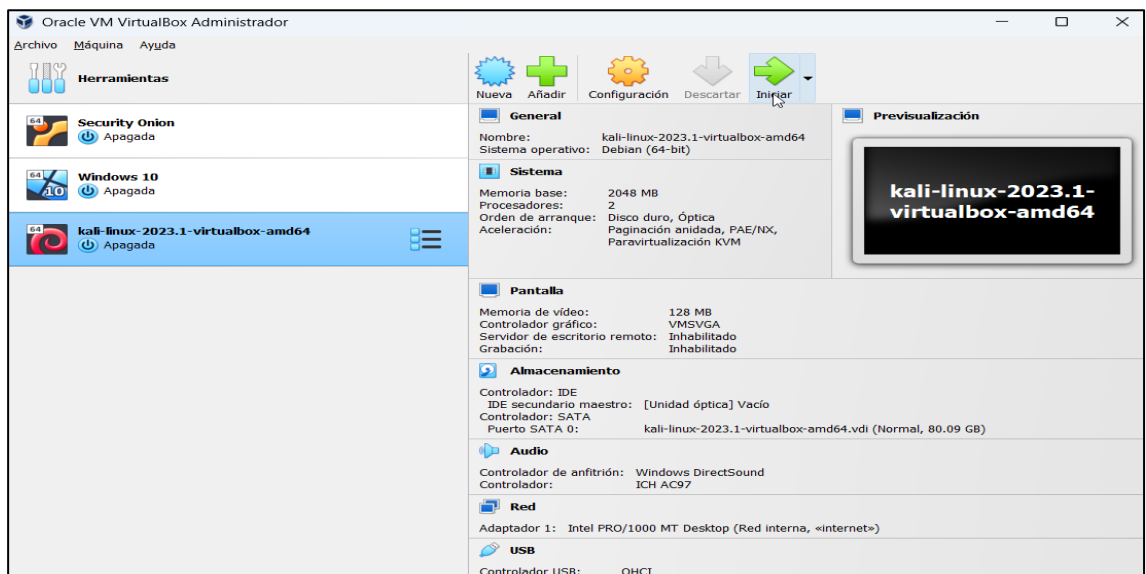


Fuente: Elaboración Propia

- Una vez seleccionado el archivo de kali linux, se visualizará la máquina virtual en la interfaz del software de virtualización Virtual Box, seguidamente damos clic en iniciar para completar la instalación del sistema operativo.

Figura 63

Interfaz del sistema de archivos local

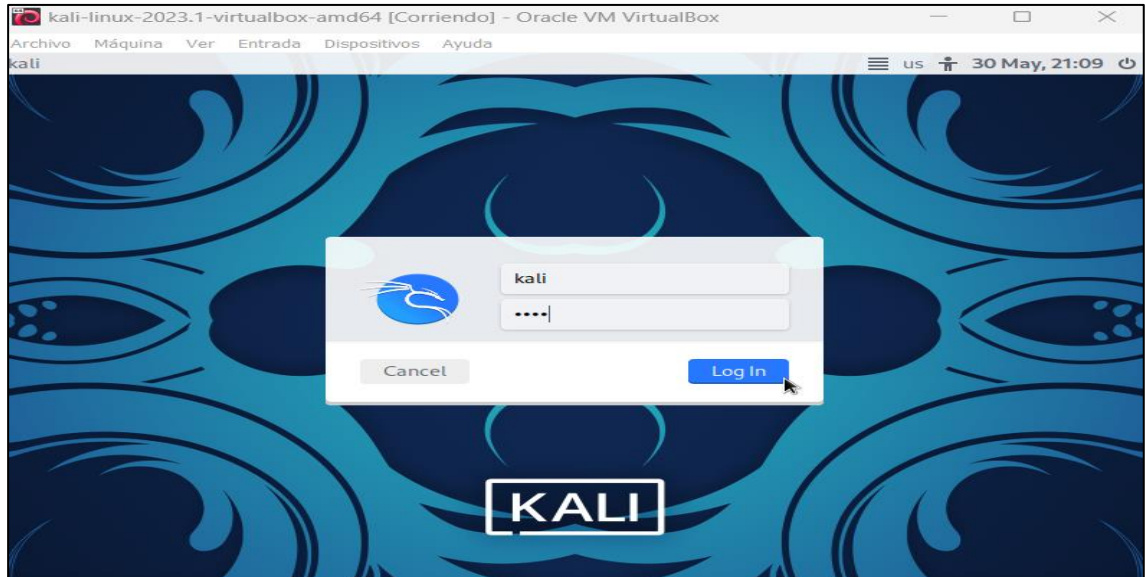


Fuente: Elaboración Propia

- Finalizada la instalación de kali linux, nos aparecerá la interfaz de inicio de sesión para poder utilizar el sistema operativo, en usuario y password colocaremos las siguientes credenciales:
usuario: **kali** y en password: **kali**

Figura 64

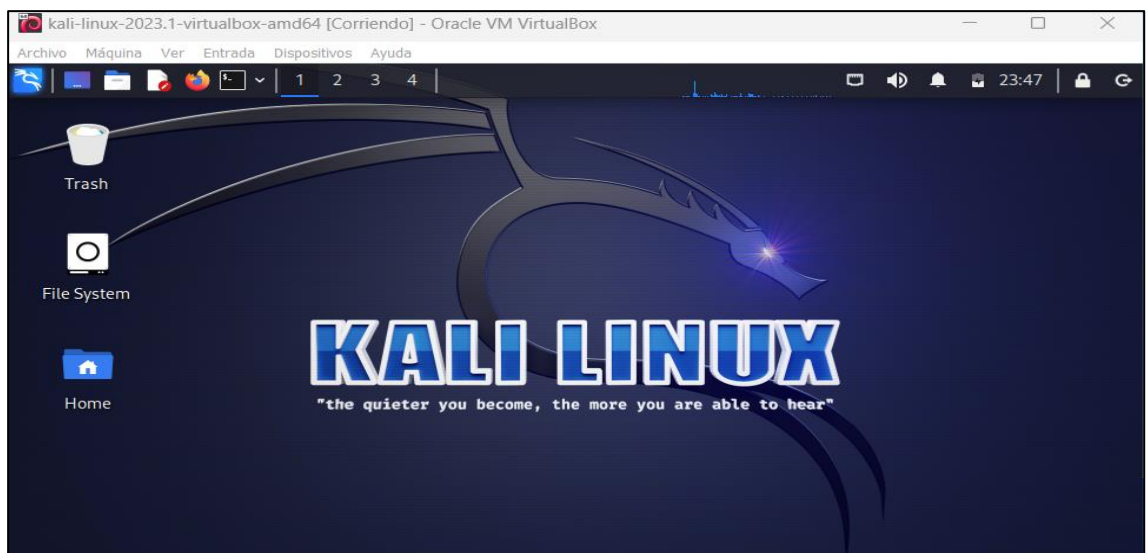
Interfaz de inicio de sesión



Fuente: Elaboración Propia

Figura 65

Interfaz de escritorio de Kali linux



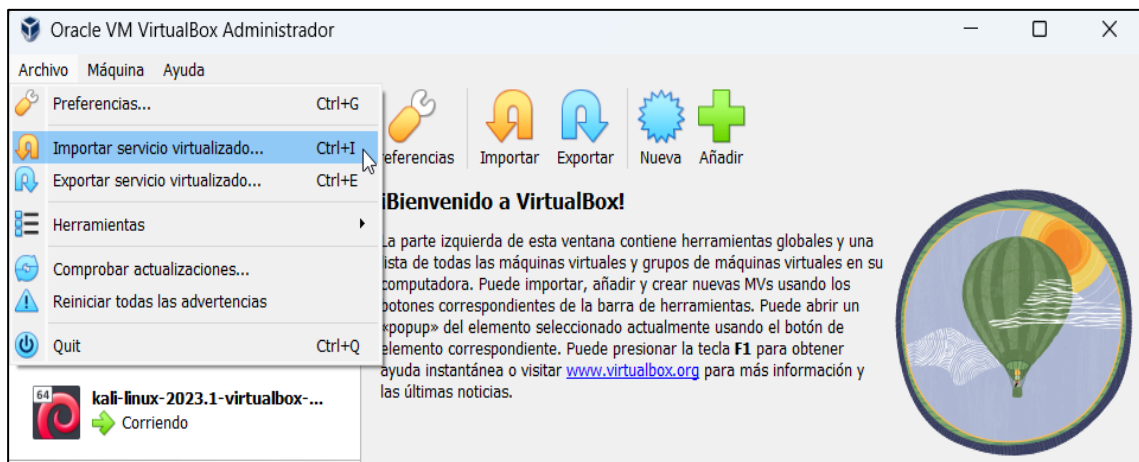
Fuente: Elaboración Propia

IMPORTACIÓN DE LA MÁQUINA VIRTUAL SECURITY ONION DESDE VIRTUAL BOX

- Como primer paso nos ubicamos en el software de virtualización Virtual Box, posteriormente seleccionamos la opción archivo y seguidamente importar servicio virtualizado.

Figura 66

Importación de Servicio virtualizado



Fuente: Elaboración Propia

- En la siguiente interfaz seleccionamos sistemas de archivos local en la opción fuente, luego seleccionamos el archivo con extensión. OVA de la máquina virtual security onion y damos clic en next.

Figura 67

Importación de Servicio virtualizado II



Fuente: Elaboración Propia

- A continuación nos aparecerá la siguiente interfaz mostrando las preferencias del servicio, damos clic en terminar.

Figura 68

Interfaz de preferencias de servicio

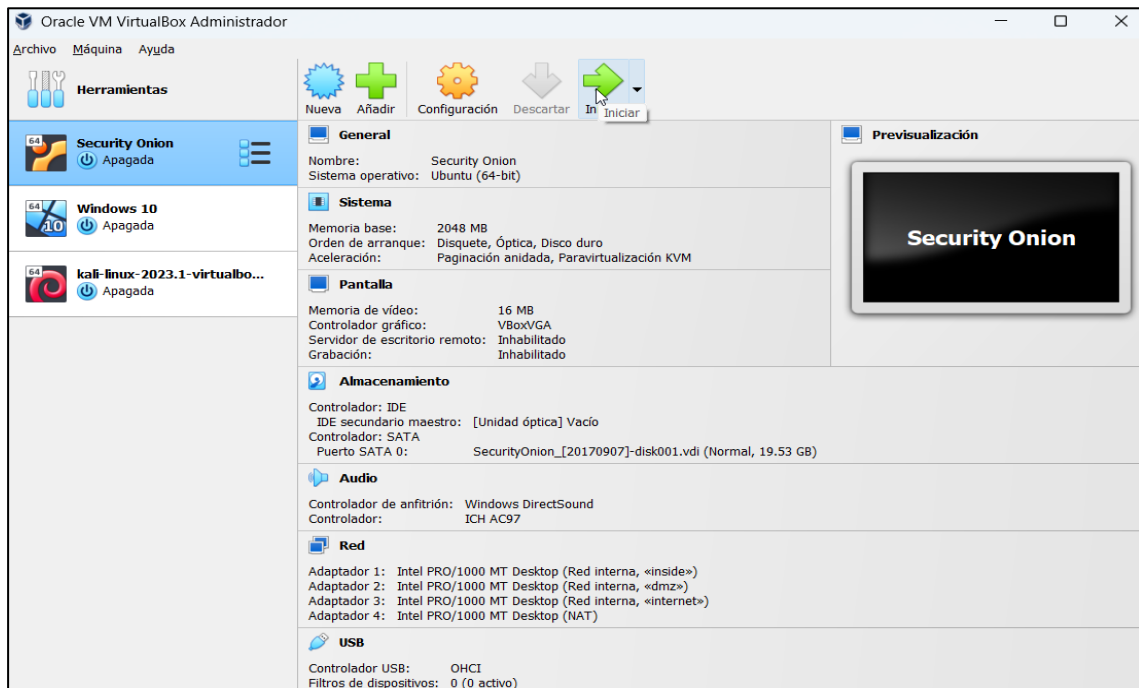


Fuente: Elaboración Propia

- Una vez terminada la importación de la máquina virtual security onion, procederemos a iniciar la máquina virtual.

Figura 69

Interfaz de inicialización de la máquina virtual security onion

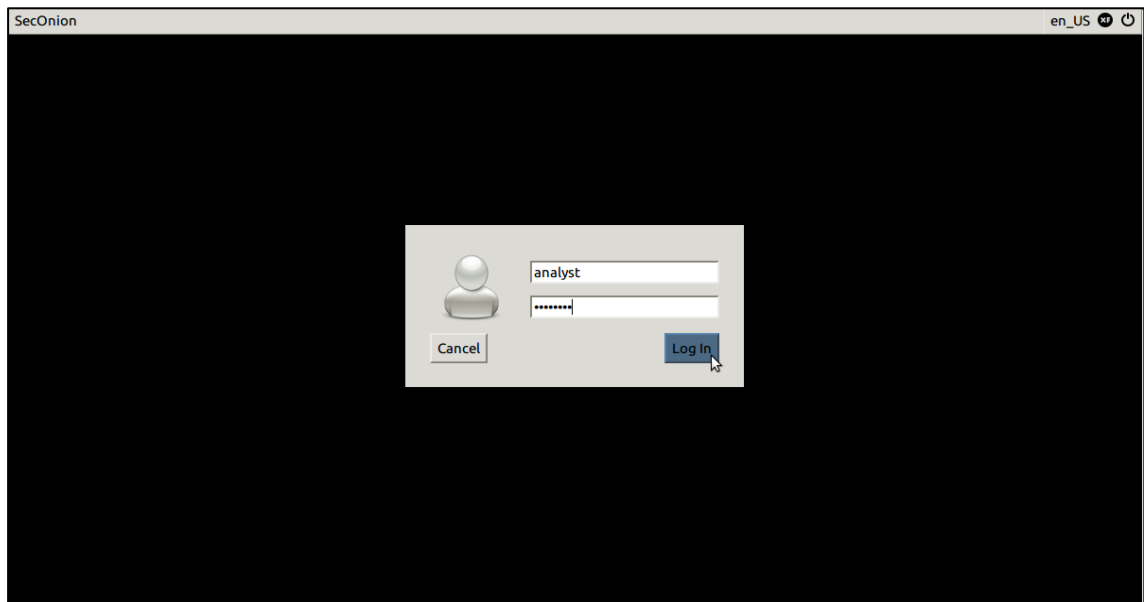


Fuente: Elaboración Propia

- Finalmente aparecerá la interfaz de inicio de sesión para poder utilizar el sistema operativo, en usuario colocaremos **analyst** y en password **cyberops**.

Figura 70

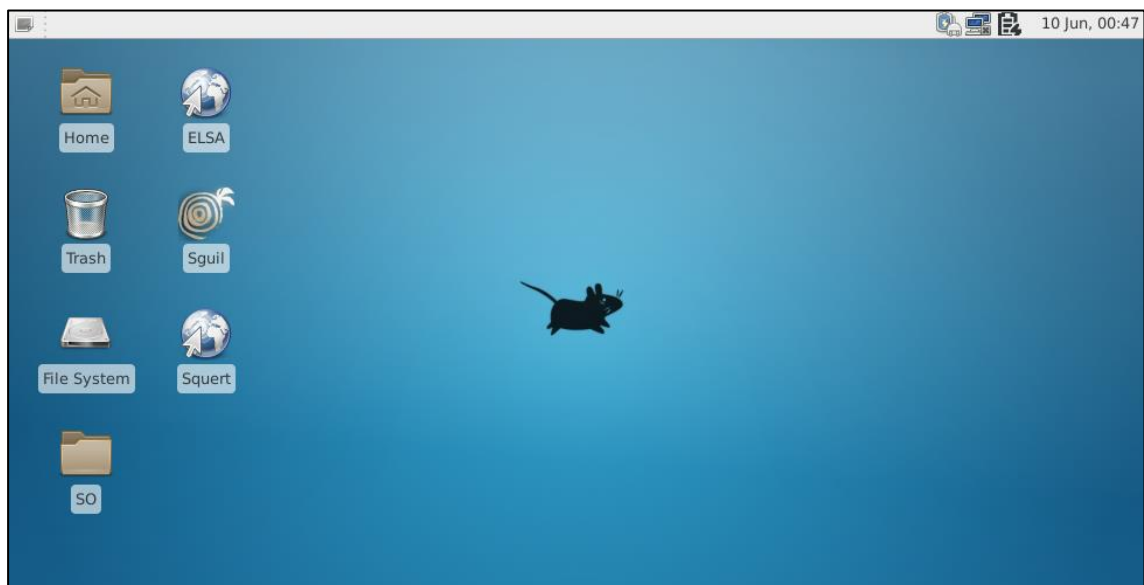
Interfaz de inicio de sesión



Fuente: Elaboración Propia

Figura 71

Interfaz del escritorio del Security Onion



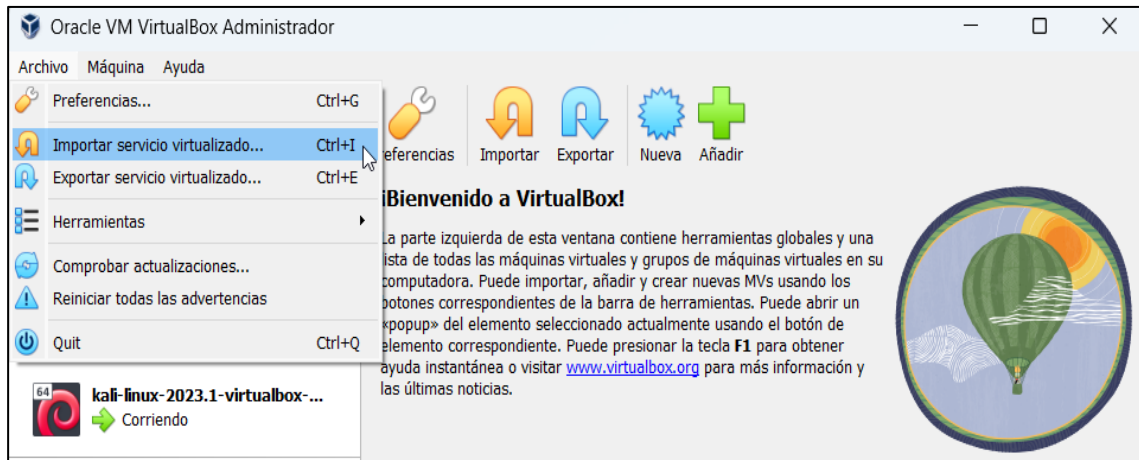
Fuente: Elaboración Propia

IMPORTACIÓN DE LA MÁQUINA VIRTUAL SRV-APLI

- Desde el software de virtualización Virtual Box, seleccionamos la opción archivo y seguidamente importar servicio virtualizado.

Figura 72

Importación de servicio virtualizado



Fuente: Elaboración Propia

- En la siguiente interfaz seleccionamos sistemas de archivos local en la opción fuente, luego seleccionamos el archivo con extensión .OVA de la máquina virtual SRV-APLI y damos clic en next.

Figura 73

Interfaz del servicio a importar



Fuente: Elaboración Propia

- A continuación nos aparecerá la siguiente interfaz mostrando las preferencias del servicio, damos clic en terminar.

Figura 74

Interfaz de Preferencias de servicio

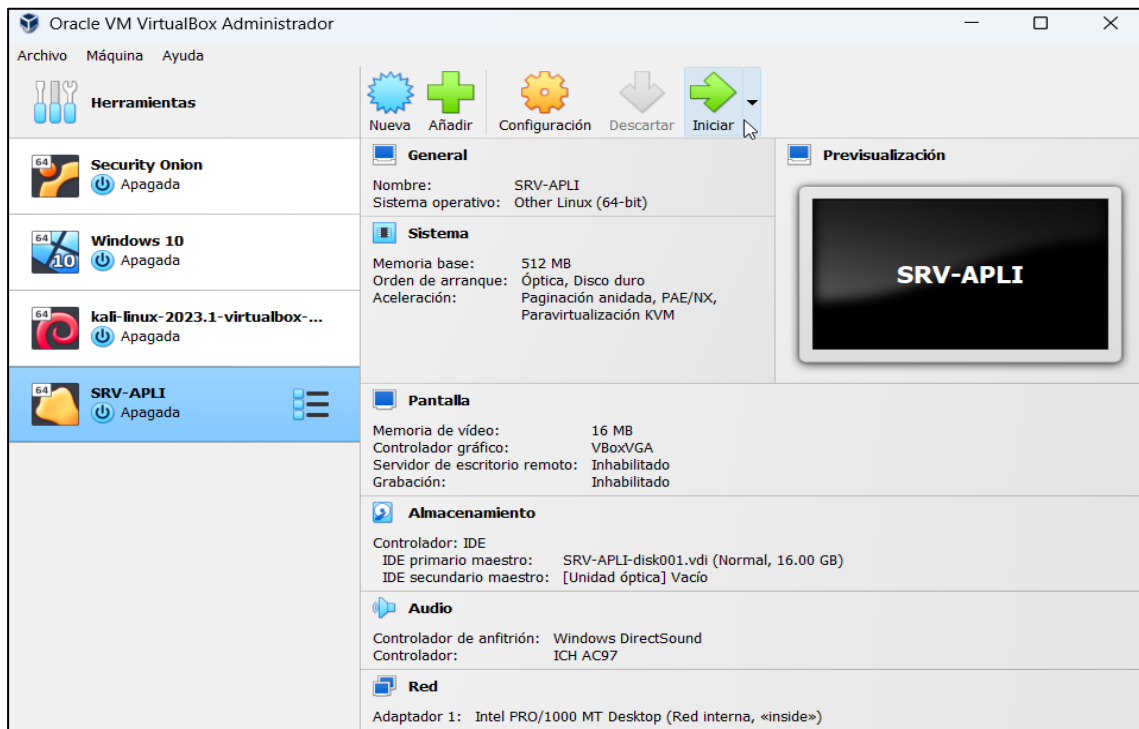


Fuente: Elaboración Propia

- Una vez terminada la importación de la máquina virtual SRV-APLI, procederemos a iniciar la máquina virtual.

Figura 75

Interfaz de inicialización de Centos 7

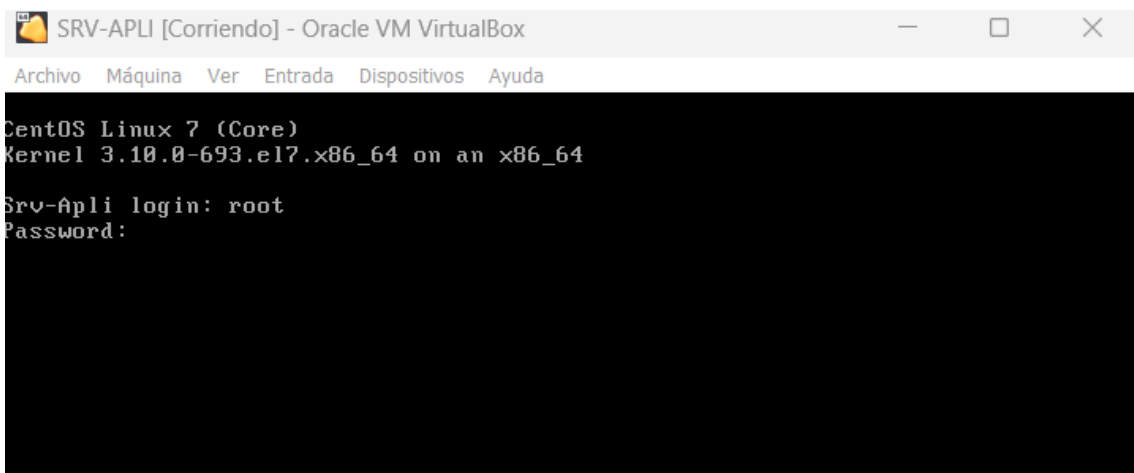


Fuente: Elaboración Propia

- Finalmente aparecerá la interfaz de inicio de sesión para poder utilizar el sistema operativo, en login colocaremos **root** y en password colocaremos **123456**.

Figura 76

Interfaz de Inicio de Sesión Centos 7

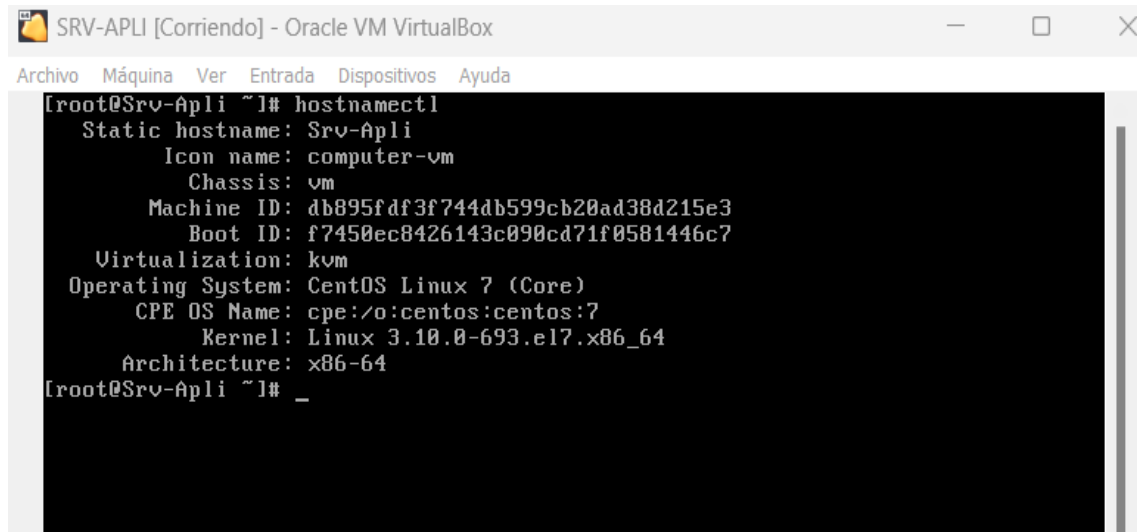


Fuente: Elaboración Propia

- Ejecutamos el script **hostnamectl** para que nos muestre información detallada sobre la máquina virtual instalada.

Figura 77

Información del servidor centos 7



```
SRV-APLI [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli ~]# hostnamectl
  Static hostname: Srv-Apli
            Icon name: computer-vm
            Chassis: vm
      Machine ID: db895fdf3f744db599cb20ad38d215e3
        Boot ID: f7450ec8426143c090cd71f0581446c7
    Virtualization: kvm
  Operating System: CentOS Linux 7 (Core)
      CPE OS Name: cpe:/o:centos:centos:7
        Kernel: Linux 3.10.0-693.el7.x86_64
    Architecture: x86-64
[root@Srv-Apli ~]# _
```

Fuente: Elaboración Propia

CONFIGURACIONES DE RED DE LAS MÁQUINAS VIRTUALES

En esta parte realizaremos la configuración de red entre las máquinas virtuales creadas según nuestro diagrama de entorno virtual. Para nuestro caso hemos realizado la siguiente:

- En la configuración de red de la máquina virtual security onion podemos observar que consta de cuatro adaptadores de red, los tres primeros utilizan el modo de red interna y en el último adaptador utiliza el modo nat, en este modo de configuración la máquina virtual puede conectarse a internet. Security onion permite conectar a todas las máquinas virtuales con un adaptador de red en cada una de las redes vlan (inside, dmz, internet).

Figura 78

Interfaz de configuración de las Máquinas virtuales

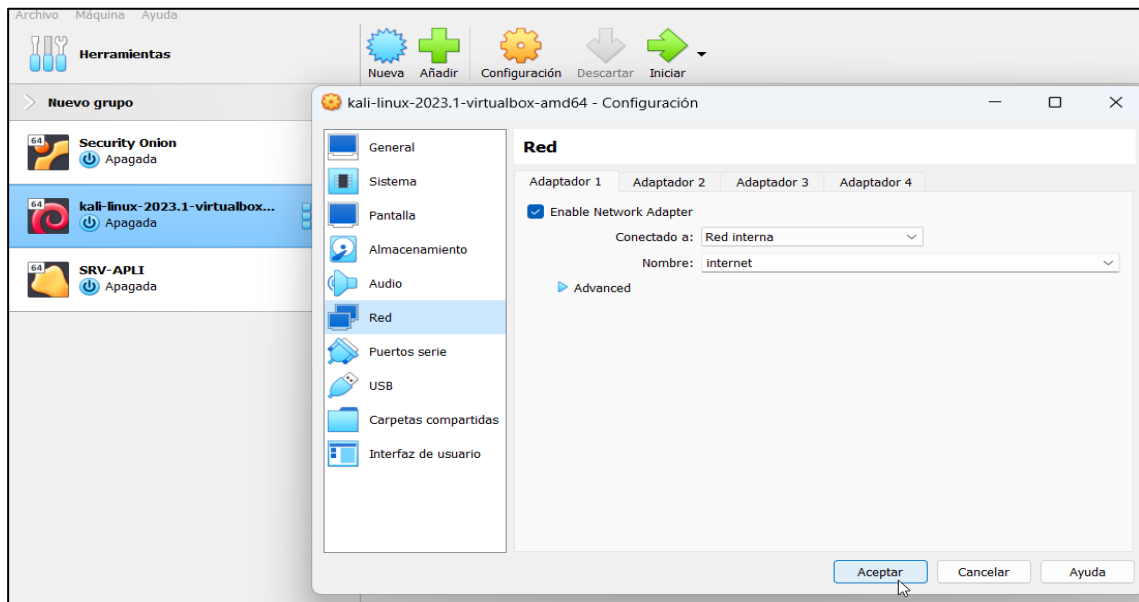


Fuente: Elaboración Propia

- Realizamos la siguiente configuración de red en la máquina virtual kali linux, seleccionando el modo de red interna y la red vlan internet.

Figura 79

Interfaz de configuración de la máquina virtual Kali Linux

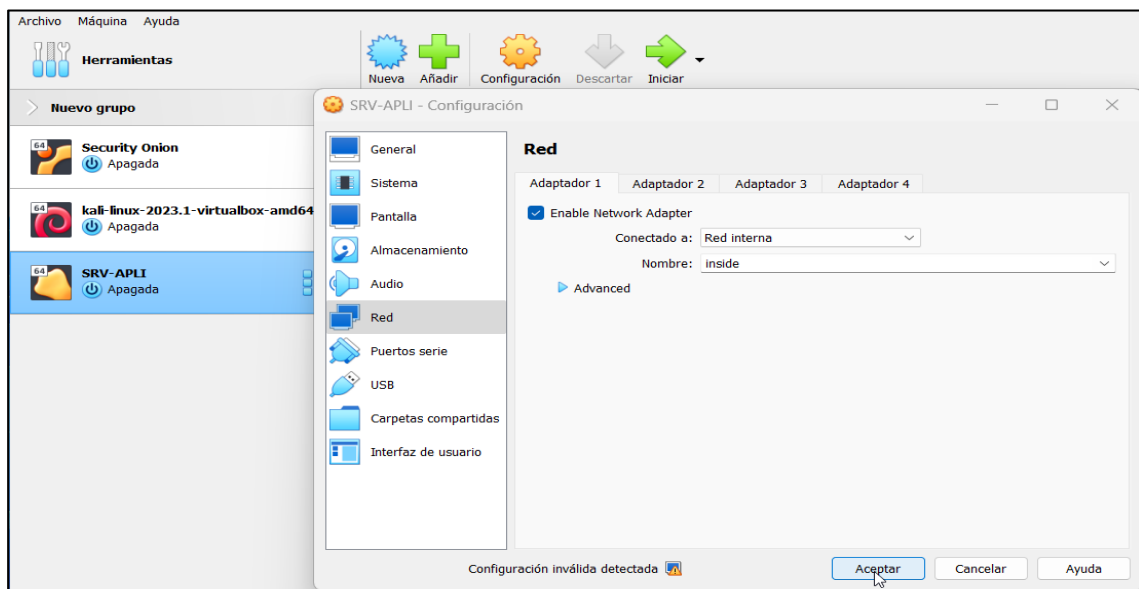


Fuente: Elaboración Propia

- Para la maquina virtual CentOS se realizó la siguiente configuración de red, se conecto en modo de red interna y en la red vlan como inside.

Figura 80

Interfaz de configuración de la máquina virtual centos 7



Fuente: Elaboración Propia

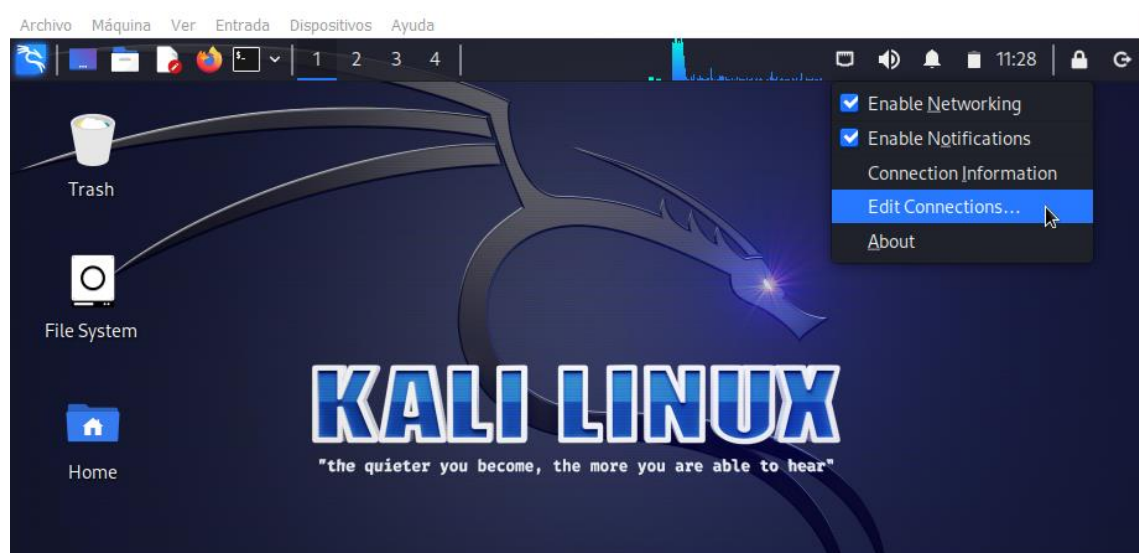
CONFIGURACIONES DE LAS DIRECCIONES IP DE LAS MÁQUINAS VIRTUALES.

Una vez configurado los modos de conexión de las máquinas virtuales, procederemos a configurar las direcciones IP de manera estática o manual, tanto de la máquina atacante (kali linux) como de la máquina objetivo (centOS) para ello realizamos lo siguiente.

- Nos dirigimos a la interfaz gráfica de nuestra máquina virtual kali linux, damos clic derecho en el icono de red que se encuentra en la superior derecha y seguidamente seleccionamos editar conexiones.

Figura 81

Interfaz gráfica de la máquina virtual Kali linux

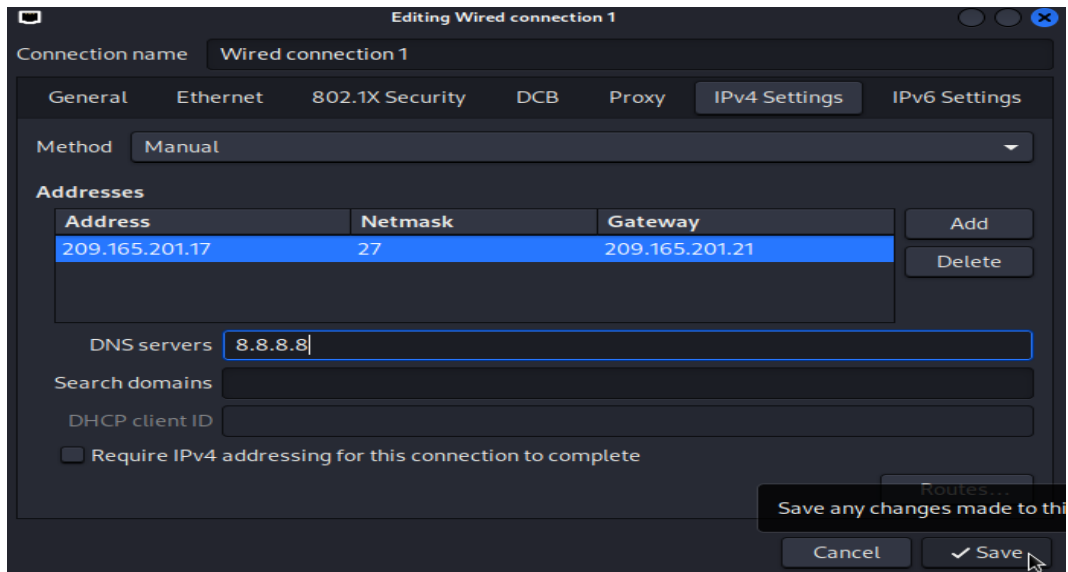


Fuente: Elaboración Propia

- Nos aparecerá la interfaz de edición de red, damos clic en ajustes de IPv4 y seleccionamos método manual, seguidamente añadimos la dirección ip **209.165.201.17** y guardamos los cambios.

Figura 82

Interfaz de configuración de red Kali linux

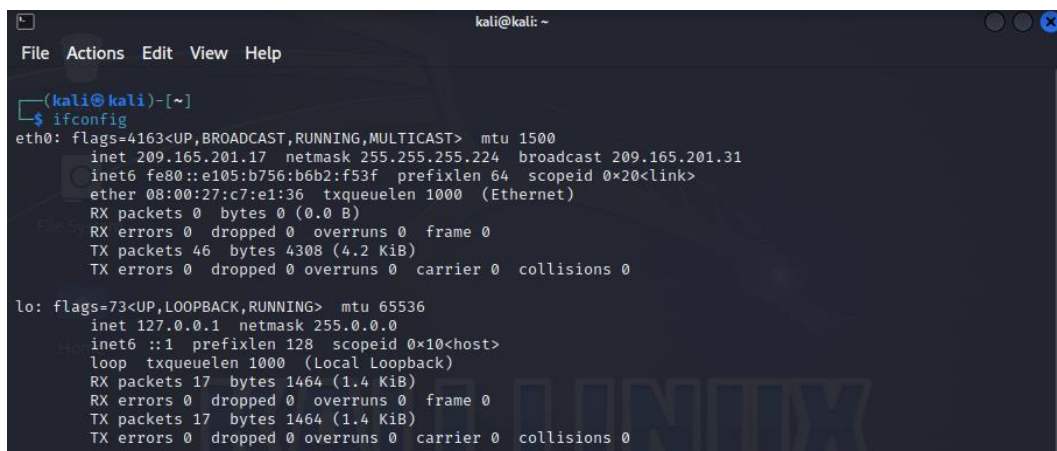


Fuente: Elaboración Propia

- Para verificar que se haya guardado correctamente la dirección ip asignada, desde la terminal de la máquina virtual realizamos una consulta con el siguiente comando **ifconfig** y nos mostrará información como: el nombre de la interfaz, la dirección ip, la máscara de red y la dirección de broadcast. De esta manera corroboramos que dichos cambios han sido guardados con éxito.

Figura 83

Interfaz de información de la interfaz de red



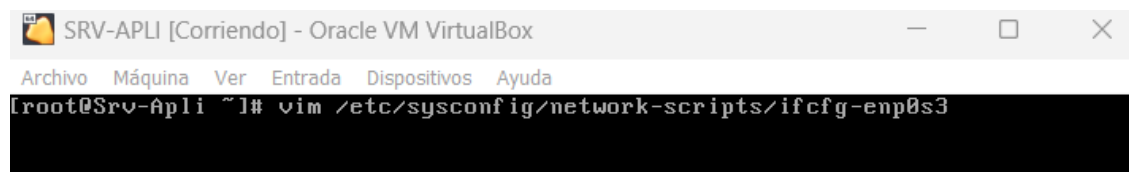
Fuente: Elaboración Propia

- Para configurar la dirección ip de manera estática en la máquina objetivo (centOS), procedemos a editar el archivo “ifcfg-enp0s3” , ejecutando el siguiente script..

vim /etc/sysconfig/network-scripts/ifcfg-enp0s3

Figura 84

Script para editar archivo de configuración de red



```

[root@Srv-Apli ~]# vim /etc/sysconfig/network-scripts/ifcfg-enp0s3

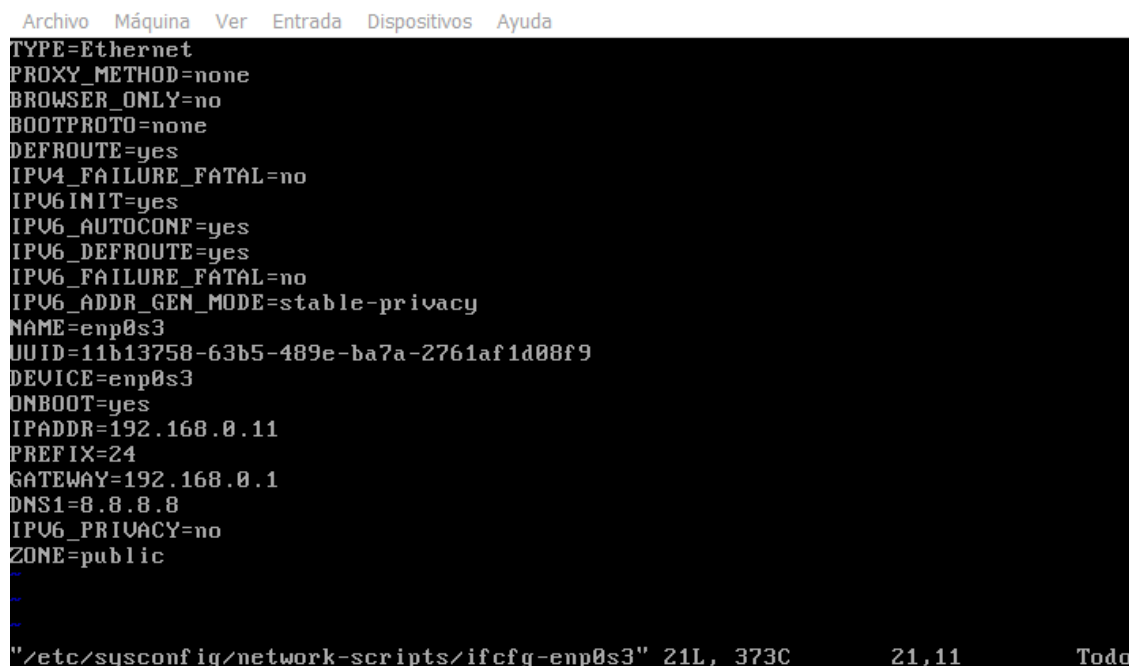
```

Fuente: Elaboración Propia

- Del archivo “ifcfg-enp0s3” editaremos los parámetros **ipaddr**, **gateway**, **dns1** y guardaremos los cambios.

Figura 85

Parámetros del archivo de configuración de red



```

TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp0s3
UUID=11b13758-63b5-489e-ba7a-2761af1d08f9
DEVICE=enp0s3
ONBOOT=yes
IPADDR=192.168.0.11
PREFIX=24
GATEWAY=192.168.0.1
DNS1=8.8.8.8
IPV6_PRIVACY=no
ZONE=public

"/etc/sysconfig/network-scripts/ifcfg-enp0s3" 21L, 373C      21,11      Todo

```

Fuente: Elaboración Propia

- Para verificar que los cambios se hayan guardado con éxito, ejecutaremos el script **ip a**, que nos mostrará información como: el nombre de la interfaz, dirección MAC, la dirección ip, la máscara de red y la dirección de broadcast.

Figura 86

Parámetros del archivo de configuración de red

```

Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli ~]# systemctl restart network
[root@Srv-Apli ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
   qlen 1000
    link/ether 08:00:27:5f:73:1e brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.11/24 brd 192.168.0.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::6224:700f:8ae5:c2ff/64 scope link
        valid_lft forever preferred_lft forever
[root@Srv-Apli ~]#

```

Fuente: Elaboración Propia

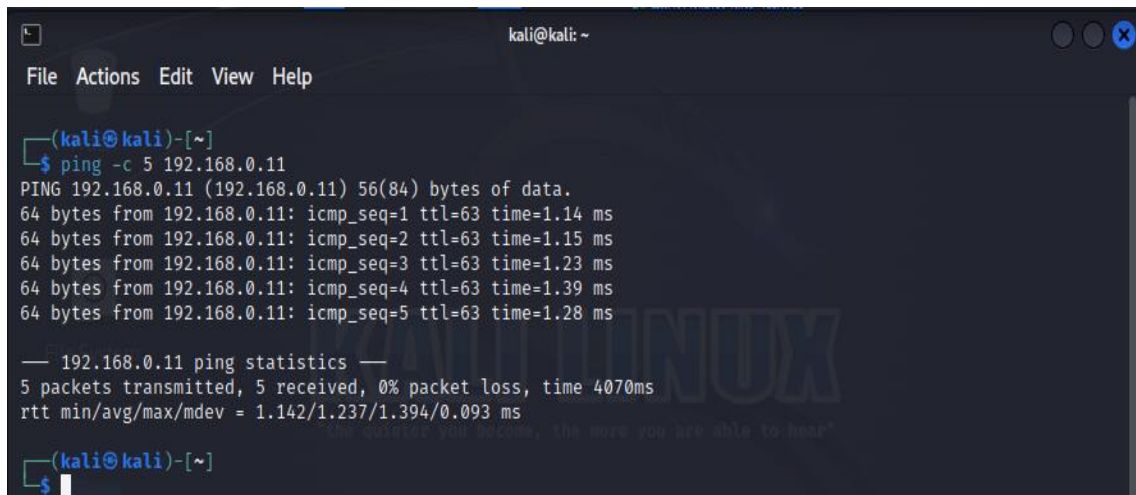
PRUEBAS DE CONEXIÓN DE RED ENTRE LAS MÁQUINAS VIRTUALES

- Una vez culminada la configuración de direcciones ip, realizamos pruebas de conexión de red desde la máquina virtual atacante (kali linux) hacia la máquina objetivo (centOS), en la terminal de la máquina atacante ejecutamos el comando **ping** especificando el número con el parámetro **-c** y seguidamente la dirección ip de destino.

```
ping -c 5 192.168.0.11
```

Figura 87

Pruebas de conexión I



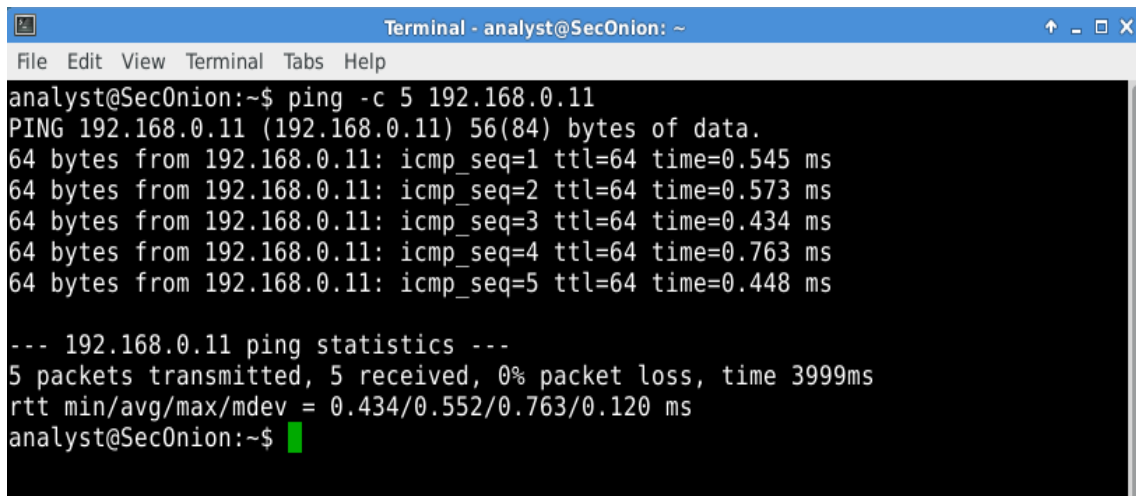
```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ping -c 5 192.168.0.11  
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.  
64 bytes from 192.168.0.11: icmp_seq=1 ttl=63 time=1.14 ms  
64 bytes from 192.168.0.11: icmp_seq=2 ttl=63 time=1.15 ms  
64 bytes from 192.168.0.11: icmp_seq=3 ttl=63 time=1.23 ms  
64 bytes from 192.168.0.11: icmp_seq=4 ttl=63 time=1.39 ms  
64 bytes from 192.168.0.11: icmp_seq=5 ttl=63 time=1.28 ms  
  
— 192.168.0.11 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4070ms  
rtt min/avg/max/mdev = 1.142/1.237/1.394/0.093 ms  
  
(kali@kali)-[~]  
$
```

Fuente: Elaboración Propia

- Así mismo se realizó pruebas de conexión entre la máquina virtual security onion con la máquina virtual atacante (kali linux) y la máquina objetivo (centOS).

Figura 88

Pruebas de conexión II

A terminal window titled "Terminal - analyst@SecOnion: ~" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows a ping command being executed: `analyst@SecOnion:~$ ping -c 5 192.168.0.11`. The output displays five successful ping responses with varying times (0.545 ms to 0.763 ms). Below the responses, it shows the ping statistics: 5 packets transmitted, 5 received, 0% packet loss, and a total time of 3999ms. The round-trip times (rtt) are listed as min/avg/max/mdev = 0.434/0.552/0.763/0.120 ms. The prompt returns to `analyst@SecOnion:~$` with a green cursor.

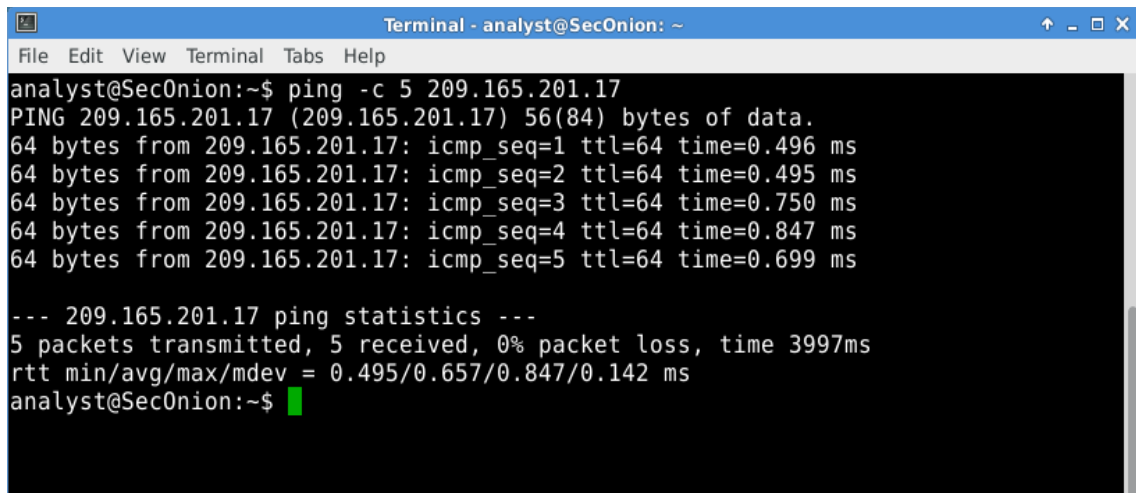
```
analyst@SecOnion:~$ ping -c 5 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=64 time=0.545 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=64 time=0.573 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=64 time=0.434 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=64 time=0.763 ms
64 bytes from 192.168.0.11: icmp_seq=5 ttl=64 time=0.448 ms

--- 192.168.0.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.434/0.552/0.763/0.120 ms
analyst@SecOnion:~$
```

Fuente: Elaboración Propia

Figura 89

Pruebas de conexión III

A terminal window titled "Terminal - analyst@SecOnion: ~" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows a ping command being executed: `analyst@SecOnion:~$ ping -c 5 209.165.201.17`. The output displays five successful ping responses with varying times (0.496 ms to 0.847 ms). Below the responses, it shows the ping statistics: 5 packets transmitted, 5 received, 0% packet loss, and a total time of 3997ms. The round-trip times (rtt) are listed as min/avg/max/mdev = 0.495/0.657/0.847/0.142 ms. The prompt returns to `analyst@SecOnion:~$` with a green cursor.

```
analyst@SecOnion:~$ ping -c 5 209.165.201.17
PING 209.165.201.17 (209.165.201.17) 56(84) bytes of data.
64 bytes from 209.165.201.17: icmp_seq=1 ttl=64 time=0.496 ms
64 bytes from 209.165.201.17: icmp_seq=2 ttl=64 time=0.495 ms
64 bytes from 209.165.201.17: icmp_seq=3 ttl=64 time=0.750 ms
64 bytes from 209.165.201.17: icmp_seq=4 ttl=64 time=0.847 ms
64 bytes from 209.165.201.17: icmp_seq=5 ttl=64 time=0.699 ms

--- 209.165.201.17 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.495/0.657/0.847/0.142 ms
analyst@SecOnion:~$
```

Fuente: Elaboración Propia

DESPLIEGUE DE LA APLICACIÓN WEB SISGEDO V.2.0 EN LA MÁQUINA VIRTUAL CENTOS.

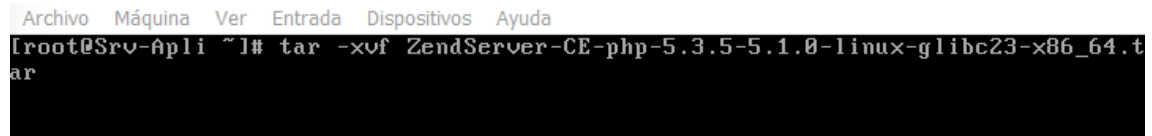
INSTALACIÓN DEL FRAMEWORK ZEND SERVER

- Ubicamos y extraemos el archivo de instalación del framework zend server previamente descargado con el siguiente script.

```
tar -xvf ZendServer-CE-php-5.3.5-5.1.0-linux-glibc23-x86.64.tar
```

Figura 90

Script para extraer el framework zendserver



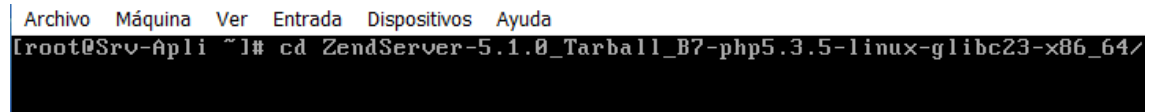
```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli ~]# tar -xvf ZendServer-CE-php-5.3.5-5.1.0-linux-glibc23-x86_64.t
ar
```

Fuente: Elaboración Propia

- Una vez extraído el archivo **.tar**, nos dirigimos a la carpeta de zend server y abrimos el archivo ejecutable **./install.sh**.

Figura 91

Ruta de la carpeta del Zend Server

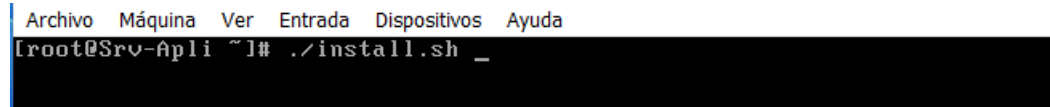


```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli ~]# cd ZendServer-5.1.0_Tarball_B7-php5.3.5-linux-glibc23-x86_64/
```

Fuente: Elaboración Propia

Figura 92

Archivo ejecutable de Zend Server



```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli ~]# ./install.sh _
```

Fuente: Elaboración Propia

- Finalizada la instalación ubicamos el archivo de configuración del framework zend server y añadimos la línea `ServerName` seguida de la **ip** de la máquina ejecutando el siguiente script.

Ruta: `cd/usr/local/apache2/conf`

Edición: `vim httpd.conf`

Figura 93

Ruta del archivo de configuración de Zend Server

```

Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli conf]# cd /usr/local/zend/apache2/conf
[root@Srv-Apli conf]# ll
total 96
drwxr-xr-x 2 root root  290 jul 11  2019 extra
-rw-r--r-- 1 root root 13384 jul 11  2019 httpd.conf
-rw-r--r-- 1 root root 14364 mar 18  2010 httpd.conf.bak
-rw-r--r-- 1 root root 12958 mar 18  2010 magic
-rw-r--r-- 1 root root 45472 mar 18  2010 mime.types
drwxr-xr-x 3 root root   37 mar 18  2010 original
[root@Srv-Apli conf]# vim httpd.conf

```

Fuente: Elaboración Propia

Figura 94

Edición del archivo de configuración de Zend Server

```

# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName 192.168.0.11

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"

#
# Each directory to which Apache has access can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
#
# First, we configure the "default" to be a very restrictive set of

```

Fuente: Elaboración Propia

- Iniciamos el servidor zend server mediante la ejecución del siguiente script.

```
cd /usr/local/zend/bin/zendctl.sh start
```

Figura 95

Framework Zend Server iniciado

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli ~]# cd /usr/local/zend/bin/
[root@Srv-Apli bin]# ./zendctl.sh start
Starting Zend Server 5.1.0 ..

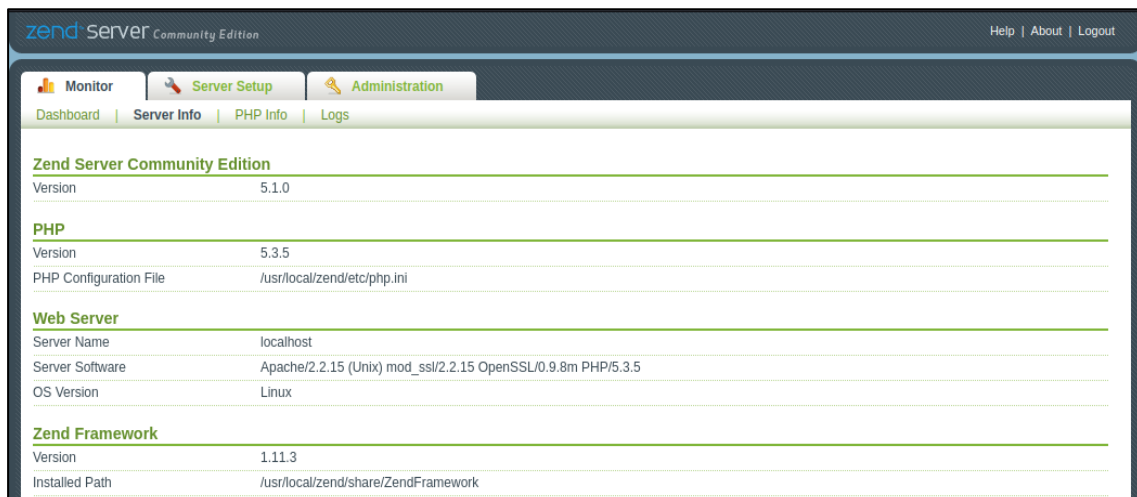
httpd (pid 1629) already running
/usr/local/zend/bin/apachectl start [OK]
spawn-fcgi: socket is already in use, can't spawn
lighttpd watchdog is up and running.. [OK]
[ 20.06.2023 20:15:03 SYSTEM] watchdog for lighttpd is running.
[ 20.06.2023 20:15:03 SYSTEM] lighttpd is running.

Zend Server started...
[root@Srv-Apli bin]#
```

Fuente: Elaboración Propia

Figura 96

Interfaz de administración de Zend Server



Fuente: Elaboración Propia

INSTALACIÓN DEL SISTEMA GESTOR DE BASE DE DATOS POSTGRESQL

- Para instalar el sgbd postgresql debemos tener descargado el archivo ejecutable previamente y ejecutar el siguiente script.

```
yum install -y postgresql-9.6.24-1linux-x64.run
```

Figura 97

Instalación del SGBD PostgreSQL

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli conf]# yum install -y postgresql-9.6.24-1-linux-x64.run _
```

Fuente: Elaboración Propia

- Añadimos la **ip** de la máquina en el archivo de configuración de la base de datos **pg_hba.conf** mediante el siguiente script.

```
vim/opt/PostgreSQL/9.6/data/pg_hba.conf
```

Figura 98

Ruta del archivo de configuración del SGBD PostgreSQL

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli conf]# vim /opt/PostgreSQL/9.6/data/pg_hba.conf
```

Fuente: Elaboración Propia

Figura 99

Edición del archivo de configuración del SGBD PostgreSQL

```
# TYPE      DATABASE      USER      ADDRESS      METHOD
# "local" is for Unix domain socket connections only
local      all          all              md5
# IPv4 local connections:
host      all          all          127.0.0.1/32      md5
host      all          all          192.168.0.11/32    md5
host      all          all          192.168.1.3/32     md5
# IPv6 local connections:
host      all          all          ::1/128          md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
#local      replication  postgres     md5
#host      replication  postgres     127.0.0.1/32      md5
#host      replication  postgres     ::1/128          md5
```

Fuente: Elaboración Propia

- Después de editar el archivo de configuración, reiniciamos postgresql utilizando el siguiente script.

```
systemctl restart postgresql-9.6
```

Figura 100

Reinicio del SGBD PostgreSQL

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli conf]# systemctl restart postgresql-9.6_
```

Fuente: Elaboración Propia

- Una vez reiniciado el sgbd postgresql, configuramos el firewall habilitando el puerto predeterminado para el servicio de postgresql **5432/tcp**.

```
firewall-cmd --zone=public --add-port=5432/tcp --permanent
firewall-cmd --reload
```

Figura 101

Configuración de regla en el firewall

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli conf]# firewall-cmd --zone=public --add-port=5432/tcp --permanent
```

Fuente: Elaboración Propia

Figura 102

Actualización de configuraciones del firewall

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli conf]# firewall-cmd --reload_
```

Fuente: Elaboración Propia

- Finalmente con el comando **status postgresql** corroboramos que el servicio postgresql se está ejecutando correctamente.

systemctl status postgresql-9.6

Figura 103

Estado del servicio PostgreSQL

```
[root@Srv-Apli ~]# systemctl status postgresql-9.6
■ postgresql-9.6.service - PostgreSQL 9.6 database server
   Loaded: loaded (/usr/lib/systemd/system/postgresql-9.6.service; enabled; vendor preset: disabled)
   Active: active (running) since mié 2023-06-21 18:46:43 -05; 1h 55min ago
     Process: 945 ExecStart=/opt/PostgreSQL/9.6/bin/pg_ctl start -w -t ${TimeoutSec} -D /opt/PostgreSQL/9.6/data -l /opt/PostgreSQL/9.6/data/pg_log/startup.log (code=exited, status=0/SUCCESS)
    Main PID: 969 (postgres)
      CGroup: /system.slice/postgresql-9.6.service
              └─ 969 /opt/PostgreSQL/9.6/bin/postgres -D /opt/PostgreSQL/9.6/dat...
                 987 postgres: logger process
                 1032 postgres: checkpoint process
                 1033 postgres: writer process
                 1034 postgres: wal writer process
                 1035 postgres: autovacuum launcher process
                 1036 postgres: stats collector process
```

Fuente: Elaboración Propia

CONFIGURACIÓN DEL ARCHIVO DE CONEXIÓN DE LA APLICACIÓN WEB SIGEDO

- Verificamos datos de conexión de la aplicación web sigedo hacia la base de datos postgresql en el archivo **conexión.php** mediante el siguiente script.

```
vim /var/www/html/sisgedonewpr/app/conexión.php
```

Figura 104

Ruta del archivo de conexión de la aplicación web Sisgedo

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli bin]# vim /var/www/html/sisgedonewpr/app/conexion.php _
```

Fuente: Elaboración Propia

Figura 105

Parámetros del archivo de conexión de la aplicación web Sisgedo

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
<?
//Datos de conexión hacia la Base de Datos
$dbhost = '192.168.0.11:5432'; // host
$dbUsuario = 'postgres'; // usuario de conexión a la BD
$dbpassword = '123456'; // password de conexión a la BD
$dbName='sigedo'; // Nombre de la Base Datos
$dbtype = "postgres"; // Tipo de Bd

/* Servidor Smtip encargado de enviar correos. */
$ipSmtip = "172.16.0.4";
```

Fuente: Elaboración Propia

- Una vez verificado los datos de conexión, procedemos habilitar en el firewall el **puerto80/tcp** mediante el siguiente script.

```
firewall-cmd --zone=public --add-port=80/tcp --permanent
firewall-cmd --reload
```

Figura 106

Configuración de regla en el firewall

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli conf]# firewall-cmd --zone=public --add-port=80/tcp --permanent _
```

Fuente: Elaboración Propia

Figura 107

Actualización de configuraciones del firewall

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[root@Srv-Apli conf]# firewall-cmd --reload
```

Fuente: Elaboración Propia

- Finalmente abrimos un navegador y colocamos el siguiente link:
<http://192.168.0.11/sisgedonewpr/app/main.php>, con la finalidad de corroborar que la aplicación web sisgedo se ha desplegado de manera correcta.

Figura 108

Aplicación web Sisgedo



Fuente: Elaboración Propia

ANEXO 02: OFICIO DE AUTORIZACIÓN PARA REALIZAR EL PROYECTO



1311118
577242.

"AÑO DE LA UNIDAD, LA PAZ Y EL DESARROLLO"

Chiclayo, 16 de Mayo de 2023.

OFICIO N° 252 -2023-MPCH-GRR.HH.

Señora Dra.

GIULIANA FIORELLA LECCA ORREGO.

Directora de la Escuela Profesional de Ingeniería en Computación e Informática.
Universidad Nacional Pedro Ruiz Gallo.

Presente.-

REF.: Carta Virtual N° 017-2023-EPICI-FACyM.-
Reg. N° 570284-2022-SISGEDO.

De mi consideración:

Es grato dirigirme a usted, para expresarle mi saludo cordial a nombre de la Gerencia de Recursos Humanos de la Municipalidad Provincial de Chiclayo, y en atención al documento de la referencia, debo indicarle que, se autoriza a los Estudiantes **Sr. BRENIS FERNANDO TICONA TAPIA y Srta. ROSSMERY FLORES MIÑOPE**, para que realice su Proyecto de Tesis denominado "*Detección de ataques y mitigación de vulnerabilidades de los servicios web de la Municipalidad Provincial de Chiclayo*"; al respecto debo indicarle que, esta Gerencia autoriza la aplicación de encuestas y/o cuestionarios para su Proyecto de Investigación, siendo potestad del trabajador municipal colaborar con dicha encuesta. Asimismo, deberán informar respecto a los avances del referido Proyecto.

Es propicia la oportunidad para expresarle los sentimientos de mi consideración.

Atentamente



MUNICIPALIDAD PROVINCIAL DE CHICLAYO
GERENCIA DE RECURSOS HUMANOS

Abog. Jesús Alicia Fernández Palomino
GERENTE

Cc.
Archivo.

Detección de ataques y mitigación de vulnerabilidades de los servicios web de la municipalidad provincial de Chiclayo



INFORME DE ORIGINALIDAD

Dr. Ing. Gilberto Carrión Barco
DNI: 16720146
ASESOR

13%
INDICE DE SIMILITUD

13%
FUENTES DE INTERNET

1%
PUBLICACIONES

5%
TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1 hdl.handle.net
Fuente de Internet 3%

2 epage.pub
Fuente de Internet 2%

3 www.uacj.mx
Fuente de Internet 2%

4 revistas.uteq.edu.ec
Fuente de Internet 1%

5 repositorio.uide.edu.ec
Fuente de Internet 1%

6 repositorio.ug.edu.ec
Fuente de Internet 1%

7 repositorio.uta.edu.ec
Fuente de Internet 1%

8 repository.unad.edu.co
Fuente de Internet <1%

9 Submitted to Corporación Universitaria
Minuto de Dios, UNIMINUTO <1%



Trabajo del estudiante

Dr. Ing. Gilberto Carrión Barco
DNI: 16720146

ASESOR

10

Submitted to Universidad Tecnológica
Centroamericana UNITEC

Trabajo del estudiante

<1 %

11

Submitted to Universidad Tecnológica de
Honduras

Trabajo del estudiante

<1 %

12

repositorio.uisek.edu.ec

Fuente de Internet

<1 %

13

catalonica.bnc.cat

Fuente de Internet

<1 %

14

www.coursehero.com

Fuente de Internet

<1 %

15

Submitted to Pontificia Universidad Católica
del Perú

Trabajo del estudiante

<1 %

16

Submitted to Universidad Nacional Pedro Ruiz
Gallo

Trabajo del estudiante

<1 %

17

www.supertutoriales.com

Fuente de Internet

<1 %

18

Submitted to Ana G. Méndez University

Trabajo del estudiante

<1 %

19

Submitted to Universidad Anahuac México
Sur

Trabajo del estudiante

<1 %

20

ciberseguridad.blog

Fuente de Internet

<1 %

21

www.munichiclayo.gob.pe

Fuente de Internet

<1 %

22

Submitted to Universidad Internacional de la Rioja

Trabajo del estudiante

<1 %

23

repositorio.unprg.edu.pe

Fuente de Internet

<1 %

Excluir citas

Activo

Excluir coincidencias < 15 words

Excluir bibliografía

Activo



Dr. Ing. Gilberto Carrión Barco
DNI: 16720146
ASESOR



Recibo digital

Este recibo confirma que su trabajo ha sido recibido por **Turnitin**. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega: Rossmery & Brenis Flores Y Ticona
Título del ejercicio: Revisiones tesis EPICI
Título de la entrega: Informe3_tesis
Nombre del archivo: Informe_Parcial_03_TiconaTapia_FloresMi_ope_Turnitin.docx
Tamaño del archivo: 4.04M
Total páginas: 67
Total de palabras: 8,571
Total de caracteres: 48,511
Fecha de entrega: 28-ago.-2023 04:15p. m. (UTC-0500)
Identificador de la entrega... 2153007626

UNIVERSIDAD NACIONAL PEDRO RUÍZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE INGENIERÍA EN
COMPUTACIÓN E INFORMÁTICA



TESIS

"Detección de ataques y mitigación de vulnerabilidades de los servicios web
de la municipalidad provincial de Chiclayo"

INVESTIGADORES:

- Bach. Flores Miñope Rossmery
- Bach. Ticona Tapia Brenis Fernando

ASESOR:

- Dr. Ing. Carrión Barco Gilberto

LAMBAYEQUE, 2023

Dr. Ing. Gilberto Carrión Barco
DNI: 16720146